Information Operations

Joint Warfare Publication 3-80

JOINT WARFARE PUBLICATION 3-80

INFORMATION OPERATIONS

Joint Warfare Publication 3-80 (JWP 3-80) dated June 2002
is promulgated as directed by the Chiefs of Staff

Director General
Joint Doctrine and Concepts

AUTHORISATION

The Joint Doctrine & Concepts Centre (JDCC) is responsible for publishing Joint Warfare Publications (JWPs) and maintaining a hierarchy of such publications. Users wishing to quote JWPs as reference material in other work should confirm with the JDCC Doctrine Editor whether the particular publication and amendment state remains extant. Comments on factual accuracy or proposals for amendment should also be directed to the Doctrine Editor at:

The Joint Doctrine & Concepts Centre
Ministry of Defence
Shrivenham
SWINDON
Wilts SN6 8RF

Telephone number: 01793 787216/7
Facsimile number: 01793 787232
E-mail: doctrine@jdcc.mod.uk

DISTRIBUTION

Distribution of JWPs is managed by DSDC(L) Llangennech, Mwrwg Road, Llangennech, Llanelli, Carmarthenshire SA14 8YP. Requests for use of this publication, or amendments to its distribution, should be referred to DSDC(L).

Telephone number: 01554 822368
Facsimile number: 01554 822350

PREFACE

SCOPE

1.   **Purpose**. The purpose of Joint Warfare Publication (JWP) 3-80 '*Information Operations*', is to provide understanding, information and guidance to all involved in the planning and execution of Information Operations (Info Ops) on Joint and single Service operations. It is intended primarily for the Joint Task Force Commander (JTFC) and those of his staff with Info Ops responsibilities, as they will be the focus for Info Ops in the Joint Operations Area (JOA). It is, however, relevant to higher and lower commands and staffs as they will be directing and assisting, or conducting tasks in support of, the JTFC's Info Ops effort. It will also provide a valuable insight to other personnel with associated responsibilities. JWP 3-80 should also be of value to those attending the Joint Services Command and Staff College.

2.   **Context**. The fundamentals of Info Ops are enduring and JWP 3-80 is authoritative in this respect. However, Info Ops is a rapidly evolving field and processes will inevitably adapt to meet developments. Readers should therefore familiarise themselves with the latest practices and procedures for Info Ops in their area of work.

3.   **Structure**. JWP 3-80 addresses the planning and conduct of Info Ops at the operational level. Chapter 1 sets military Info Ops within the context of the higher-level Information Campaign and broader cross-government activity, describing the Information Campaign and how coherence is achieved between it and Info Ops. Chapter 2 covers Info Ops in detail, describing what it aims to achieve, how it assists the JTFC's mission, and how it integrates with the Campaign Plan. Chapter 3 addresses Info Ops planning, its contribution to the Joint Estimate and the subsequent Campaign Plan. Finally, Chapter 4 covers the execution of Info Ops, explaining its conduct and co-ordination within the JTFHQ. Although JWP 3-80 does not explicitly break Info Ops down into Offensive and Defensive Info Ops the requirement for both offensive and defensive activity is implicit throughout the publication. JWP 3-80 introduces the concept of Information Activity; this will be expanded on within future doctrine publications.

LINKAGES

3.   British Defence Doctrine (BDD), the JWP 0-10 '*United Kingdom Doctrine for Joint and Multinational Operations*' (UKOPSDOC) and JWP 3-00 '*Joint Operations*', all stress the importance of Info Ops as part of the wider campaign, and provide an introduction to the subject. JWP 3-80 provides the necessary amplification to enable commanders and staffs to successfully plan and conduct Info Ops. NATO doctrine for

Info Ops is still being developed but will appear in due course as Allied Joint Publication (AJP) - 3.10.

INFORMATION OPERATIONS

CONTENTS

(INTENTIONALLY BLANK)

JOINT WARFARE PUBLICATIONS

The successful prosecution of joint operations requires clearly understood doctrine that is acceptable to all nations and Services concerned. It is UK policy that national doctrine should be consistent with NATO doctrine and, by implication, its terminology and procedures (other than those exceptional circumstances when the UK has elected not to ratify NATO doctrine). Notwithstanding, the requirement exists to develop national doctrine to address those areas not adequately covered, or at all, by NATO doctrine, and to influence the development of NATO doctrine. This is met by the development of a hierarchy of Joint Warfare Publications (JWPs).

Joint Doctrine Pamphlets (JDPs) are published as necessary to meet those occasions when a particular aspect of joint doctrine needs to be agreed, usually in a foreshortened time scale, either in association with a planned exercise or operation, or to enable another aspect of doctrinal work to be developed. This will often occur when a more comprehensive 'parent' publication is under development, but normally well in advance of its planned publication.

The Joint Doctrine Development Process, and associated hierarchy of JWPs, is explained in DCI JS 16/2002.

RECORD OF AMENDMENTS

Amendment Number	Date of Insertion	Initials

CHAPTER 1 – THE INFORMATION CAMPAIGN

SECTION I – BACKGROUND

101.   Modern conflict is increasingly complex. Inter-state conflicts, fought by national forces within a defined and often geographically contiguous area, such as the Gulf War, are increasingly being replaced by intra-state conflicts, or asymmetric attacks by transnational organisations. These usually involve a wide variety of actors and parties, often in loose or ad hoc alliances, frequently operating outside the geographic area in dispute, or even globally. The causes of these conflicts are equally complex; religion, ethnicity, politics, poverty and perceived oppression are among the many factors behind them. Military action alone cannot resolve such situations, but it can set the conditions for resolution by other actors. Therefore there is a need for coherent activity – a cross-government approach – from all instruments of national power and where possible with other International Organisations (IOs).

102.   **The Impact of the International Media**. Virtually all crises are conducted under the spotlight of the international media. The maintenance of public support is crucial for democratically accountable governments, and this influences the options they can take, including military action, and the presentation of these options to different audiences. In order to gain and maintain public support, national and international, governments need to show a degree of transparency in their actions, and these actions should be in accordance with received ethics and international law. The influence of the media has increased as access to regional and international media has increased. This has been brought about by advances in technology in radio and television, such as satellite broadcasting, by the increasingly porous nature of international borders and by the availability of relatively cheap printing or copying equipment that has brought newspapers and other printed material to a much wider audience. Consequently there is a need to be proactive in ensuring that the presentation of our actions is positive whilst at the same time, countering the adversary's[1] or detractor's attempts to undermine public support.

103.   **The Impact of Technology**. As well as the role that is played by technology in increasing access to the media, there is an ever increasing dependence on Information Technology (IT) by both military and civilians. This introduces new opportunities that can be exploited, and new vulnerabilities that must be protected. Many people now have the ability to access information direct via the Internet and, without necessarily knowing its pedigree and source, place considerable credence on it; this is particularly so in societies without a free press. The Internet can be used to spread or circulate information and opinion, including rumour, with a speed inconceivable a few years ago. All this reinforces the need for a proactive information stance with a global reach.

---

[1] Throughout this publication, the term 'adversary' includes potential as well as actual adversary.

SECTION II – THE INFORMATION CAMPAIGN

104.   **Purpose of the Information Campaign**. Consequent to the spread of media access and technology, a vital aspect of the requirement for a coherent cross-government approach is the proactive management of the information output of government activity. This is termed the Information Campaign (Info Campaign) and is defined as: 'Co-ordinated information output of all government activity undertaken to influence decision-makers in support of policy objectives, while protecting one's own decision-makers'.[2] It is essential that the Government seizes the initiative with respect to information, sends clear political messages, maintains public confidence and, vitally, is seen as being in charge. Several Info Campaigns may take place simultaneously each focusing on a particular region, crisis or conflict. The Info Campaign recognises that all activity[3] sends a message from which deductions are drawn, aggregated, and, ultimately, actions determined, by friendly, adversary and neutral audiences. It ensures that, as far as is possible, the message put out by all parts of the UK Government is the intended message: the message that is most likely to lead to the adoption of the preferred Course(s) of Action (CoA) (or inaction) by the targeted decision-maker. The Info Campaign incorporates both the management of information in the form of themes and messages[4] and specific actions conducted with the intention of promoting a desired message. The Info Campaign is by its very nature an integrated cross–government activity that makes use of the three instruments of power,[5] drawing on the appropriate government departments. Where possible the Info Campaign should also involve non-governmental parties such as:

     a.   Commercial, business and private enterprise.

     b.   Humanitarian agencies and organisations.

     c.   International organisations such as the UN or EU.

It will often need to be cognisant of, and where possible aligned with, multinational, alliance or coalition influences and objectives. In some cases it may be possible to attach UK staff to other nations to provide assistance and advice on the conduct of their own Info Campaigns or to provide liaison between UK and allied or coalition Info Campaigns.

105.   **Structure of the Information Campaign**. The Info Campaign starts with government policy, that is, the desired outcome of a situation or crisis. This is then translated into government activity, using the three instruments of power. The Info Campaign ensures that the desired message is sent by this co-ordinated cross-

---

[2] DTIO Policy Update dated 22 Feb 01.
[3] Both activity and inactivity send a message. Throughout this publication 'activity' also implies the effects of inactivity.
[4] Themes and messages are described in para 302.
[5] BDD refers to three Instruments of Power: Diplomatic, Economic and Military.

departmental activity. The MOD, as the provider of the military instrument of power, supports this campaign. It does so directly through the MOD contribution to the Info Campaign and indirectly through broader military activity, both activities being carefully co-ordinated. This is illustrated in Figure 1.1, and expanded on in paragraph 106.
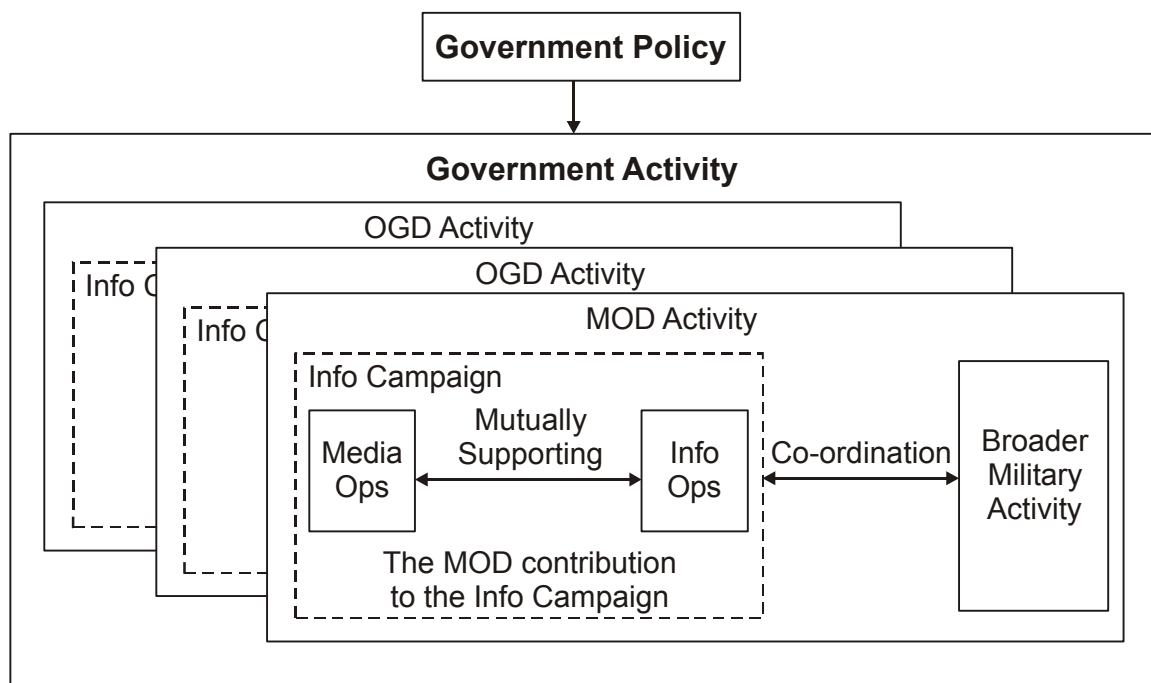
Figure 1.1 – The MOD Contribution to the Information Campaign

106.   **The MOD Contribution to the Information Campaign**. The MOD originates and directs military activity, one aspect of which is the MOD's contribution to the Info Campaign. This comprises the co-ordinated use of all or any military capability in order to influence audiences[6] (at any level) and prevent them from imposing their will. It has two parts: Information Operations (Info Ops) and Media Operations (Media Ops) both of which must be mutually supporting.[7] These can be underscored or reinforced by broader military activity such as defence diplomacy, force deployments or even the direct application, or threat, of credible military force where necessary. Victory is rarely achieved purely through the destruction of an adversary's materiel; the key is to destroy an adversary's Will to fight. Info Ops is the primary means by which Will and the ability to impose Will and exercise command is attacked.[8] It is essential that the MOD contribution to the Info Campaign and these broader military activities are co-ordinated to ensure that the effects are coherent. This

---

[6] Audiences include decision-makers (political and other leaders and military commanders), influential individuals, military personnel, armed factions and specific population groups (eg. ethnic, cultural, religious and political). They may be adversaries, the uncommitted or allied and coalition partners.
[7] Detailed guidance for Media Ops is contained in JWP 3-45 '*Media Operations*'.
[8] Will includes such factors as motivation, intent, attitude, beliefs and values.

co-ordination is achieved through the Defence Crisis Management Organisation (DCMO).

107. **Aim of the Information Campaign**. The aim of the Info Campaign is to influence decision-makers to adopt or reinforce a course of action (or inaction) that will advance the UK's policy objectives.[9] An Info Campaign should be an on-going process although the intensity and the level of the MOD contribution will vary with the situation. When a potential crisis is identified there is likely to be a sharper focus within the MOD and a step-up in the level of its contribution. The Info Campaign is therefore applicable across the spectrum of tension and in all types of operation from conflict prevention to warfighting. It has four main objectives:

a. Pre-conflict it may seek, as part of a cross-government conflict prevention strategy, to pre-dispose and persuade targeted audiences of the benefits of a specific CoA likely to prevent the situation degenerating into crisis.

b. While in crisis it may seek to persuade audiences of the benefits of one CoA while deterring them from adopting another that is more likely to lead to conflict.

c. In conflict the objective may be to coerce adversaries to adopt a desired CoA, isolate them and undermine their Will to continue aggression. It may also seek to reassure or persuade allies and neutral parties of the benefits of a particular CoA.

d. In a post conflict situation the Info Campaign may seek to reassure both the population and leadership, restoring confidence in the political process and fostering stability as part of cross-government rehabilitation activity.

108. **Cross-Government Direction and Co-ordination**.[10] The Cabinet Office, possibly supported by a cross-government working group, provides strategic direction and objectives for the Info Campaign based on national objectives set as part of government policy. Each department then develops its own line of activity to meet the Info Campaign objectives. Co-ordination of this cross-government activity is achieved through a second working group drawn from appropriate departments and usually referred to as the Cross-Government Implementation Group (CGIG). MOD

---

[9] As such the Info Campaign will for a key aspect of UK's ability to deter and coerce adversaries.

[10] This paragraph represents a simplified version of activities in order to aid understanding. The reality is a much more iterative process involving the MOD, PJHQ and other key government departments. In many cases the MOD will be proposing objectives to the Cabinet Office before receiving clear political direction.

HQ is represented by DG Op Pol or by the Directorate of Targeting and Information Operations (DTIO) staff who will update direction to the wider MOD as required.[11]

SECTION III – MINISTRY OF DEFENCE ACTIVITY

109.   **Higher Level Direction**. The MOD directs the military line of activity, through the DCMO, to meet the Cabinet Office Objectives including those of the Info Campaign. Depending on the level of involvement, the MOD contribution may initially be managed from within MOD HQ (DTIO), supported by PJHQ. At the operational level, the JTFC is responsible for Info Ops, with the Joint Commander (Jt Comd) setting boundaries and providing direction and support within the context of the Info Campaign.

110.   **Supporting Analysis**. To be effective the Info Campaign and within it Info Ops must be based on a full understanding of the crisis or conflict including its background, the parties involved, their culture and capabilities. Such understanding requires time to amass and is an ongoing and iterative process. The Defence Intelligence Staff (DIS), in conjunction with other agencies and departments, will carry out analysis to support the conduct of military operations, including Info Ops. The DIS Operations Support Group (OSG), following priorities set by the Targeting Board, will conduct analyses of both infrastructure and human factors. These analyses are then brought together by the National Infrastructure Assessment Team (NIAT) into a Target Systems Analysis (TSA) that identifies key vulnerabilities in both Will and Capability:

>   a.   The Human Factors analysis addresses the Will of the adversaries, allies, coalition partners and key uncommitted parties. It analyses their value sets in order to identify their thinking, mindset, motivation, core values, culture and social codes. This will lead to the identification of vulnerabilities in mindset that become possible themes to be attacked or protected, and strengths that should be avoided, circumvented or, in the case of allies and some uncommitted parties, to be capitalised on and exploited.

>   b.   The Infrastructure analysis addresses the physical infrastructure and capability of the adversary, focussing on those capabilities that decision-makers require to impose their Will, including infrastructure networks and Command, Control, Communications, Computers and Intelligence (C4I) capabilities and processes, in order to identify critical nodes and linkages. At the same time, it identifies vulnerabilities in other involved neutral and friendly nations that may require protection from possible adversary actions.

---

[11] Informal linkages between key members of the CGIG exist as part of normal working practice, consequently much of the early co-ordination is conducted before the CGIG is formally stood up.

The MOD uses the output from these analyses to identify the most appropriate military contribution to the Info Campaign and subsequently provide direction and support to Info Ops.

111.   **Co-ordination**. Co-ordination of the military contribution to the Info Campaign lies initially with the MOD News Release Group (NRG), which develops the Info Campaign objectives set by the Cabinet Office and, drawing on the DIS analysis, identifies common themes for both Info Ops and Media Ops, providing the higher-level co-ordination of these two separate but related activities. Info Ops is then further developed by the Military Info Ops Co-ordination Group (MIOCG). This group conducts the detailed planning, turning the NRG-provided themes into clear tasks, setting lower level objectives and providing the higher-level co-ordination within Info Ops activity. As the crisis develops the DCMO process takes over, the Strategic Planning Group (SPG), the Current Operations Group (COG) and Current Commitments Team (CCT) are established at MOD and subsume the MIOCG.

112.   **MOD Direction**. Direction for the overall military contribution to Government activity is then issued in a Chief of the Defence Staff (CDS) Directive. The Info Ops Annex to this directive will contain the Info Campaign Objectives, themes to be used and possibly themes to avoid. Key or 'Master Info Campaign Messages' that must be put across may also be listed. These 'Master Messages' are critical and must not be compromised by the conduct of lower level Info Ops. The Annex may also list target audiences and additional messages; however, these are for guidance and are generally refined and updated by both PJHQ and the JTFHQ. MOD will also pass down information from the OSG TSA.

113.   **Joint Commander's Mission Directive**. CDS's direction is received by PJHQ where a Contingency Planning Team (CPT) conduct the military strategic estimate. They draw on the OSG analysis to formulate the Jt Comd's Mission Directive, which amplifies the MOD direction for Info Ops. They will refine the direction given in the CDS Directive ensuring that coherence is maintained between direction for targeting and for Info Ops. The Jt Comd's Mission Directive will include an Info Ops Annex, which will lay out the Info Ops joint campaign objectives, themes, messages, audiences and tasks in a matrix. Further guidance and direction is also issued in the Targeting Directive, which will include the Joint Integrated Target List (JITL).[12]

---

[12] The JITL will include targets and target audiences that embody Will or Capability and can therefore vary from physical structures to specific individuals or groups. A target or target audience must always be tangible though the desired effect may be physical or cognitive.

CHAPTER 2 – INFORMATION OPERATIONS

SECTION I – FUNDAMENTALS OF INFORMATION OPERATIONS

201.   **Definition**. Information Operations (Info Ops) is defined as: 'Co-ordinated actions undertaken to influence an adversary or potential adversary in support of political and military objectives by undermining his will, cohesion and decision-making ability, through affecting his information, information based processes and systems while protecting one's own decision-makers and decision-making processes'.[1]

202.   **Focus of Information Operations**. An adversary's effectiveness is a function of his Will and Capability. Info Ops focuses on influencing Will and on affecting those Capabilities that directly enable the application of Will:

   a.   **Will**. Within the direction and goals of the Information Campaign (Info Campaign), Info Ops is targeted at all audiences at any level capable of influencing the situation whether adversary, friendly or uncommitted:

      (1)   **Adversaries**. Info Ops aims to influence the adversary's perceptions and Will, undermining cohesion and shaping the battlespace. For example, by questioning the legitimacy of their leadership and cause, Info Ops may undermine their moral power base, separating leadership from supporters, political, military and public, thus weakening their desire to continue and affecting their actions.

      (2)   **Coalition and Allies**. Info Ops aims to reinforce and protect the Will of friends and allies by strengthening resolve and by countering adversary attempts to influence it, in order to maintain friendly cohesion and reinforce freedom of action.

      (3)   **Uncommitted**. Info Ops aims to present and promote the UK or alliance case to uncommitted audiences and influence their perceptions in our favour. This can be achieved by providing, where appropriate, moral and physical support and actions to bolster their Will and demonstrate our own Will, Capability and Commitment. At the same time, adversary attempts to influence their perceptions should be countered, in order to isolate the adversary, maintain coalition cohesion and enhance our freedom of action.

   b.   **Capability**. Within Rules of Engagement (ROE) and legal constraints, Info Ops will seek to affect those Capabilities, such as the adversary's

---

[1] DTIO Policy Update dated 22 Feb 01.

Command, Control, Communications, Computer and Intelligence (C4I) infrastructure, that enable a decision-maker to impose and apply his Will.

    (1)   **Adversaries**. Info Ops seeks to affect, degrade, disrupt, deceive, destroy or deny those Capabilities that allow the decision-maker to bolster, impose, apply and sustain his Will and to exercise effective command. In concert with other military and governmental action Info Ops also seeks to attack the source of the adversary decision-maker's physical power base, splitting internal and external groupings and alliances. The aim is to influence the adversary, thereby preventing him from taking the initiative.

    (2)   **Coalition and Allies**. Info Ops aims to protect those capabilities, for example friendly Command and Control (C2) and Communications and Information Systems (CIS), that allow us to exercise effective command, seize and maintain the initiative.

    (3)   **Uncommitted**. We may seek to protect uncommitted parties' capabilities directly, by providing materiel and advice, or indirectly by targeting those adversary capabilities that he could use to attack other's Capability.

Information Operations Activities

203.   **General**. Ultimately Info Ops seeks to affect actions; it helps shape the battlespace, attacks the adversary's cohesion and protects our own whilst exploiting the situation. It can make use of all military activities to attack or defend Will and Capability and is integrated with broader military activity as part of the Campaign Plan. Clearly attacks on Capability also have an effect on Will and vice-versa, therefore both Info Ops and broader military activity must be carefully integrated to ensure that the desired overall impact is achieved. The two main aspects of Info Ops are Influence Activity, which is the primary means of influencing Will, and Counter-Command Activity (CCA), which attack Capability. However, each may have an impact on the other, and should not be considered exclusive activities. All activities, be they on Will or Capability, are dependent on the provision of good information, which is supported and protected through Information Activity. The relationship between the various aspects of Info Ops and broader military activity is shown in Figure 2.1.
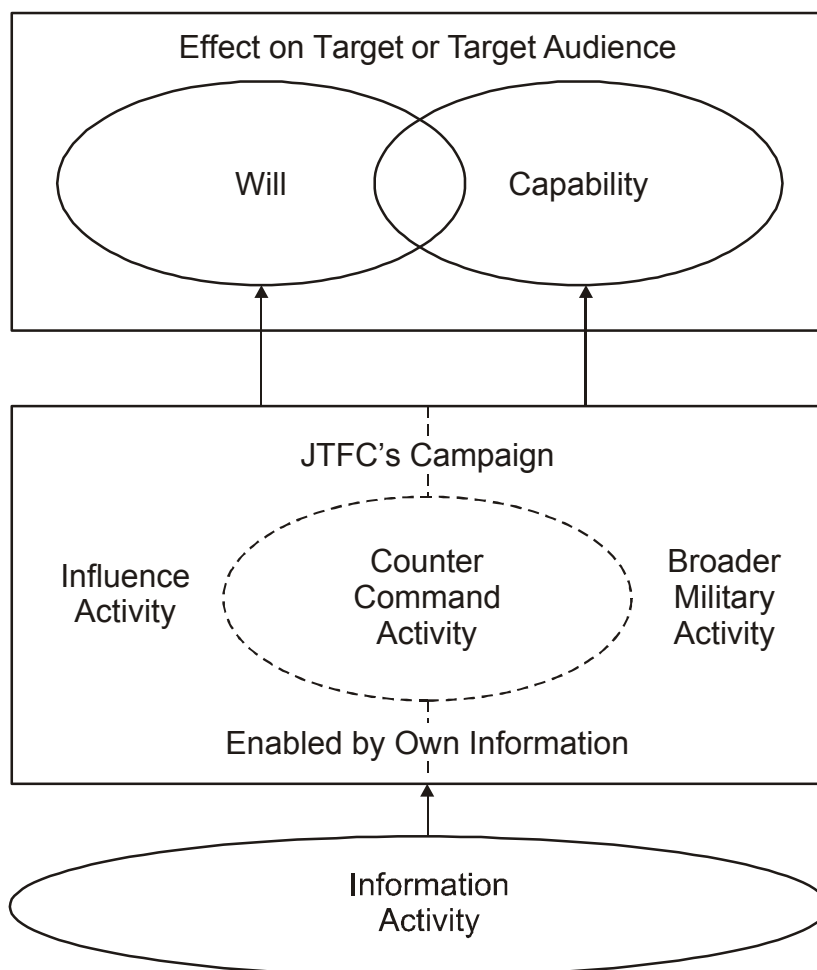
Figure 2.1 – The Relationship Between the Aspects of Information Operations and Broader Military Activity

204.   **Influence Activity**. Influence Activity comprises any activity whose primary purpose is to influence Will. Attacks on Will are achieved by the promotion of identified themes to target audiences through messages. Influence Activity seeks to predispose, persuade, convince, deter, disrupt, compel or coerce target audiences to adopt or reinforce a particular Course(s) of Action (CoA) (or inaction) or to assist, encourage and reassure those that are following a desired CoA, rebuilding confidence where necessary. Influence Activity can capitalise on, increase the effectiveness of, or in some cases may remove the need for, attacks on Capability as part of broader military activity. As part of a co-ordinating strategy it focuses the impact of existing actions against Capability to ensure that their effect on Will is coherent and supports the Joint Task Force Commander's (JTFC) objectives. It ensures that broader military activity sends the right message. It also generates actions, ranging from a show of force to the dropping of leaflets, specifically intended to promote themes and thus influence Will. Influence Activity must be coherent with the Info Campaign, and will be most effective when fully co-ordinated with it.

205. **Counter-Command Activity**. CCA can be used to affect the flow of information to a decision-maker, thereby influencing his Will, or to affect the dissemination of a decision, thus affecting the application of his Capability. CCA sits between Influence Activity and broader military activity, contributing to both, and is concentrated on undermining the adversary's ability to develop, disseminate and execute sound decisions. It attacks Capability but achieves an impact on both Will and Capability. It focuses on those capabilities that assist an adversary to make a decision and then translate that decision into action. Key decision-making and communications nodes, linkages and their associated critical vulnerabilities are identified and attacked by the most appropriate means. CCA seeks, within ROE, to disrupt, degrade, deny, deceive or destroy an adversary's information, command and associated systems, processes and networks. Actions are planned and co-ordinated to ensure that Info Campaign and Influence Activity themes are reinforced. In a post-conflict situation they seek to deny, disrupt and degrade the Capability of those attempting to undermine political agreements whilst assisting to regenerate the Capability of more positive actors.

206. **Information Activity**. Information Activity facilitates the conduct of effective operations by contributing to the provision of useful information. It contributes to all military activity, and seeks to improve our own ability to gain, analyse, manage and disseminate useful information by protecting its integrity, through Information Assurance and Computer Network Defence (CND).

207. **Related Activities**. Related activities are those that, whilst not part of, and distinct from, Info Ops, should be closely co-ordinated with them.

    a. **Media Operations**.[2]

        (1) **Relationship with Information Operations**. The aim of Media Operations (Media Ops) is to promote widespread understanding and support for military operations while maintaining Operations Security (OPSEC). The primary purpose of Media Ops is to communicate information to audiences, through the medium of national and international media. Their main effort in any military operation is to communicate the principal themes and messages in pursuit of the end-state, whilst remaining sensitive to media interests. They are an integral part of any military operation. Although Media Ops is primarily focused on the need to maintain domestic public support and hence freedom of action, its impact is much wider. Media Ops will also have an influence on adversaries, allies and uncommitted parties. It is therefore essential that Media Ops staff and Info Ops staff work closely together to ensure that the desired message is put across to the intended audiences. This is

---

[2] For further details, see JWP 3-45 '*Media Operations*'.

particularly important with respect to local and regional media within the Joint Operations Area (JOA) and to other media sources that are influential within the JOA. To avoid giving the false impression that the media are being manipulated in any way, a distinction must be maintained between Info Ops and Media Ops.

(2)   **Responsibilities**. The News Release Group (NRG) develops the Info Campaign objectives and, drawing on the Defence Intelligence Staff (DIS) analysis, identifies common themes for both Info Ops and Media Ops and provides their higher-level co-ordination. In general, MOD D News focuses on the London based national and international media, whilst the JTFHQ Media Ops staff focus on the UK national, international and regional media represented within the JOA. There is therefore a need for close co-ordination between MOD D News, PJHQ Media Ops and the JTFHQ Media Ops to ensure a fully coherent approach to news and media management.

b.   **Civil-Military Co-operation**. The role of Civil-Military Co-operation (CIMIC) is to enable the development of links between the military and non-military parties in order to enhance unity of effort. These links may offer both valuable opportunities for reinforcing Influence Activity messages, which, to be effective, must be based on actual activity, and also for gaining information on perceptions and on the effectiveness of actions. The conduct of appropriate and timely 'Hearts and Minds' tasks can add considerable credibility to an Info Ops message. However, care must be taken to avoid giving the perception that non-military parties are being exploited by the military, CIMIC must therefore remain based on an atmosphere of mutual understanding and trust. CIMIC sits within broader military activity but with respect to Info Ops is a separate, but related, activity.

SECTION II – INFORMATION OPERATIONS STAFF AND TOOLS

208.   **Level of Command**. Info Ops must be an integral part of the JTFC's Campaign Plan, within the context of the Info Campaign. The remainder of this publication will discuss Info Ops at the operational level and below. Although Info Ops can be conducted at the tactical level by Components, it must be set clearly within the JTFC's plan. The overall direction and co-ordination must remain with the JTFC, as it is only at this level that the necessary oversight is possible.

209.   **Tactical Information Operations**. At the tactical level tasks are conducted to achieve higher-level Info Ops objectives but may also be conducted in support of their own objectives provided these are coherent with the Campaign Plan. Component HQs will invariably require their own Info Ops staff and, depending on the situation, it may

also be appropriate to appoint an Info Ops Officer at subordinate HQs. The Info Ops plan will set out both specific tasks that the Components will conduct, and may delegate areas of the plan to Component Commanders (CC) to be implemented by those CC's Info Ops staff.

210. **Joint Task Force Commander's Information Operations Staff**. The JTFHQ has an Info Ops Officer supported by an Info Ops cell within J3 Operations Support (Ops Sp). The Info Ops Officer must be of suitable seniority and quality to ensure that the Info Ops requirements are given due weight at the Joint Co-ordination Board (JCB) and receive the appropriate level of support. His function is to provide advice on Info Ops to the JTFC and to plan, monitor and co-ordinate Joint Force Info Ops activities on his behalf. As such, he contributes to the mainstream operational planning, execution and evaluation process, linking closely with all staff functions and advisers. He ensures that Info Ops activity is incorporated into the targeting process, co-ordinated and deconflicted with other activity and that assets are apportioned as required.

211. **Tools**. Info Ops is an integrating strategy and not a capability. It does not command any military capability but orchestrates and synchronises as part of the overall campaign management a wide range of activities to help achieve the JTFC's objectives. Info Ops must be able to draw on any capability that contributes to the achievement of the desired objective. Info Ops staff will make use of tools to influence Will and affect those capabilities that allow Will to be translated into action. These are discussed in more detail at Annex 2A. Info Ops must not be limited to these means but is constrained only by imagination and the availability of resources.

   a. **Influence Activity**. Actions to influence Will traditionally make use of tools such as Psychological Operations (PSYOPS), deception, Electronic Warfare (EW), specifically targeted physical destruction and Computer Network Operations (CNO), which incorporates attack, exploitation and defence. However, such factors as force presence, posture and profile, along with the separate but related activities of Media Ops and CIMIC, can also have a significant impact.

   b. **Counter-Command Activity**. Actions to affect Capability can make use of any appropriate tools however they will commonly resort to specifically targeted physical destruction, the use of emerging technology, offensive EW and CNO.

ANNEX 2A – INFORMATION OPERATIONS TOOLS

2A1.   Information Operations (Info Ops) can make use of all or any activities capable of exerting influence or conducting Counter-Command Activity (CCA); it is limited only by imagination and availability. However, the tools listed in this Annex, along with the separate but related activities of Media Ops and Civil-Military Co-operation (CIMIC), are likely to be those with the greatest applicability and utility.

2A2.   **Psychological Operations**. The primary purpose of Psychological Operations (PSYOPS) is to influence the perceptions, attitudes and behaviour of selected individuals or groups in accordance with Info Ops themes. Unlike Media Ops, PSYOPS retains direct control over contents, dissemination and audience. Effective PSYOPS requires timely provision of resources such as linguistic support, graphics and print capability, broadcasting capability and other delivery mechanisms. Messages can be presented by:

      a.   Print: enduring but not responsive.

      b.   Radio: immediate impact on a large audience. Broad, simple and repeated messages are required.

      c.   TV: extremely powerful, depending on audience access.

      d.   Loudspeakers: localised impact dependent upon linguistic support and access to desired areas.

      e.   Face to face (lectures, meetings and plays) and word of mouth (rumour and gossip): can be very effective in changing attitudes but dependent on local willingness to enter dialogue.

      f.   Internet, faxes, pagers and mobile communications: can be effective but again is dependent on access.

2A3.   **Presence**, **Posture and Profile**. The impact that the mere presence of a force may have on perceptions can be significant. Deploying even limited capability to the right place at the right time can add substantial credibility to messages being delivered through other channels and provide a major contribution to deterrence. The posture of troops on the ground can demonstrate both commitment and intent and must be considered and balanced with the requirements of force protection. At the simplest level the decision to wear berets instead of combat helmets and body armour can make a considerable difference to the perceptions of both the adversary and local people. The public profile of commanders at all levels will impact on perceptions. The public role of the commander must be carefully analysed and opportunities used to transmit key messages.

2A4.   **Operations Security**. OPSEC denies the adversary access to essential elements of friendly information, preventing him from deducing details of our activities, including Info Ops, as well as dispositions, intentions, capabilities and vulnerabilities. OPSEC reduces the amount of information available to the adversary decision-maker, making it easier to influence his perceptions and making effective decision-making more difficult.

2A5.   **Deception**. The aim of deception is to mislead the adversary and thus persuade him to adopt a course of action that is to his disadvantage. It is often most effective when it aims to reinforce existing preconceptions and perceptions. Whilst OPSEC denies information to an adversary, reducing his capacity to make effective decisions, deception fills the void with information tailored for his consumption leading to definite but incorrect decision-making.

2A6.   **Electronic Warfare**. Electronic Warfare (EW) consists of three disciplines: Electronic Warfare Support Measures (ESM); Electronic Countermeasures (ECM) and Electronic Protective Measures (EPM). Each of these can make a valuable contribution to Info Ops:

   a.   ESM can be used as a source of intelligence to assist in the planning of Info Ops by identifying themes, refining messages and identifying targets. It can also be of use to monitor the effectiveness of Info Ops tasks.

   b.   ECM can be used as a means of transmitting our messages and suppressing adversary use of the Electromagnetic Spectrum (EMS).

   c.   EPM contributes to Operations Security (OPSEC) and the maintenance of our own command control and communications.

2A7.   **Physical Destruction**. The use of force sends a strong message and consequently the direct application of force through physical destruction of adversary assets will significantly impact upon perceptions. Carefully applied force can play a major role in coercion and deterrence and in reducing an adversary's ability to exercise command. However, undue collateral damage and unnecessary casualties will have an adverse effect on public support. Whilst physical destruction will almost invariably be required the JTFC must consider and balance the potential negative impact that it may cause with the expected benefits.

2A8.   **Emerging Technology**. Emerging Technology includes the use of directed energy weapons such as Radio Frequency, Laser and acoustic and other non-lethal weapons. Their use may offer alternatives to the more direct use of physical force with the possibility of reduced collateral damage and thus greater public acceptability of any attack however, additional legal constraints may limit their availability.

2A9.   **Computer Network Operations**. The opportunity for and effectiveness of Computer Network Operations (CNO) is proportional to the adversary's dependence on IT. CNO comprise attack, exploitation and defence:

    a.   **Computer Network Attack**. It may prove feasible to use novel approaches to gain access to computer networks to affect their data, processes or hardware, thereby degrading or destroying information capability.

    b.   **Computer Network Exploitation**. Computer Network Exploitation offers the opportunity to gain undetected access to information on adversary systems and indeed to make use of the system itself for our own use.

    c.   **Computer Network Defence**. Defence of own systems and networks is essential to protect against an adversary's Info Ops and to maintain the integrity of own information capabilities and information infrastructure. Computer Network Defence (CND) comprises those actions taken to protect against disruption, denial, degradation or destruction of information resident in computers and computer networks or of the computers and computer networks themselves. CND involves the use of an integrated set of protective mechanisms, processes and organisations allied with an effective command structure to deter, protect, detect and respond to electronic attack.

(INTENTIONALLY BLANK)

CHAPTER 3 – PLANNING

301.   **Information and Intelligence Sources**. Information Operations (Info Ops) is predicated on information and intelligence, the acquisition of which will need to draw on a wide range of sources:

a.   **Military Sources**. Intelligence is accessed through J2 supported by the provision of the operational picture through J3. Additional information and intelligence is available from:

(1)   The Directorate of Targeting and Information Operations (DTIO) who provide the link into:

(a)   The Defence Intelligence Staff (DIS) (Operations Support Group).

(b)   National Agencies.

(c)   Allies and other nations.

(d)   The Target Systems Analysis process.

(2)   Permanent Joint HQ (PJHQ) Info Ops staff, who will liaise with PJHQ J2 staff to provide intelligence to the Joint Task Force HQ (JTFHQ) Info Ops staff.

b.   **Non-Military Sources**. Info Ops staff will also need to draw on broader sources of information. These include:

(1)   Civil-Military Co-operation (CIMIC) staff, who have contact with:

(a)   Local communities, businesses, politicians.

(b)   Other Government Departments (OGD).

(c)   Humanitarian parties (UN, International Organisations (IO) and Non-governmental Organisations (NGO)).

(d)   Local and refugee populations.

(2)   Open sources, such as the media, academia and the Internet. The media in particular can provide much useful information, such as background to the conflict, local and national politics and insights into the will of all parties. Analysis of the media and of media reporting trends will also provide useful information on the impact of Info Ops

and can be invaluable in assessing whether certain objectives have been achieved as part of Campaign Effectiveness Analysis[1] (CEA).

(3)   The host nation or administration can provide much useful information on local or national matters, and are another source for CEA.

An indication of the type and breadth of information required is shown in the Information and Intelligence Requirements at Annex 3A.

302.   **Terminology**. Info Ops is directed by means of objectives, themes and messages, and tasks:

a.   **Objective**. An objective is the desired outcome of one or more tasks.

b.   **Influence Activity Theme**. An Influence Activity theme is the broad idea or topic on which Influence Activity action is based; it is the line of persuasion.

c.   **Influence Activity Message**. The Influence Activity message is the practical expression of an Influence Activity theme; it is a targeted statement appropriate for the target audience.

d.   **Tasks**. Tasks are specific actions involving the application of capability:

(1)   An Influence Activity task involves the application of capability in order to deliver an Influence Activity message and could range from delivering ordnance to broadcasting on civilian radio and TV stations.

(2)   A Counter-Command Activity (CCA) task involves the application of capability to affect, degrade, disrupt, deceive, destroy or deny the desired target.

303.   **Joint Task Force Commander's Direction**. The Joint Commander (Jt Comd) will include higher-level Info Ops and Information Campaign (Info Campaign) objectives in his directive to the Joint Task Force Commander (JTFC). The JTFC will then issue planning direction to his staff. His direction will specify the contribution that Info Ops is expected to make, within the parameters set by the Info Campaign, to the achievement of his overall objectives. In conjunction with the Info Ops staff the JTFC will identify the key audiences, themes and messages for his Influence Activity activity and the desired effects of his CCA.

---

[1] 'Analysis conducted at the strategic, operational and tactical level to monitor and assess the cumulative effects of military actions with respect to Centres of Gravity in order to achieve the overall end-state.' JWP 3-00 '*Joint Operations*'.

304.   **The Joint Task Force Commander's Estimate**. The JTFHQ staff will conduct the Joint Estimate at the operational level, in accordance with JWP 3-00 '*Joint Operations*', focusing on the JTFC's objectives. It is essential that Info Ops aspects are fully considered and integrated throughout the planning process and by all staff divisions; it must not become a separate driver considered in isolation. It is equally imperative that Measures of Effectiveness (MOE) be identified as part of the planning process, and J2 tasked accordingly. Assessments of the achievement of MOE will contribute to the CEA process.

305.   **Information Operations Analysis to Support the Joint Estimate**. Info Ops staff will review all available information and intelligence on the Joint Operations Area (JOA) to enable them to support the production of the Joint Estimate. This may reveal the need for further information and intelligence, for which Requests for Information (RFI) will be raised. The Info Ops staff will focus on how to apply the given Info Campaign themes and on the identification of specific target audiences, messages, CCA targets and tasks that will support the JTFC's objectives. At the same time, they will identify where Info Ops may enhance, or even be a substitute for, the effects of other military activity whilst identifying potential negative impacts that may arise from other military actions conducted as part of the Campaign Plan. If it is decided to utilise deception, it will need to be incorporated into the planning process at the earliest stage and a separate planning group set up.[2] They must ensure that these concerns are reflected in a gain/loss assessment to enable the JTFC to make a balanced judgement on the proposed action. An aide-memoire to assist the Info Ops staff is attached at Annex 3B.

306.   **Protection**. The Info Ops staff will also review adversary Info Ops capabilities to identify those that will require countering or exploitation, and friendly capabilities to identify particular strengths that can be exploited as part of Info Ops, and weaknesses that need to be protected against adversary Info Ops. This review must also look at all Information Activity in conjunction with J6 and other staff branches as appropriate. The analysis must also consider the impact of any constraints imposed by higher authority such as:

    a.   Info Campaign objectives and themes.

    b.   Political, legal and Rules of Engagement (ROE) issues.

    c.   Those arising from social and cultural attitudes which will limit Info Ops options, for example:

        (1)   Alliance or coalition sensitivities.

---

[2] Detailed guidance for Deception is contained in JDP 2/98 '*Deception*'.

(2)   Ethical and religious issues.

307.   **The Information Operations Contribution to the Campaign Plan**. Based on the analysis and recommendations in the Joint Estimate, the JTFC will decide on a Course(s) of Action (CoA) and issue direction in the form of his concept of operations, which will include his intent and main effort. Info Ops planning will be conducted in parallel with the Joint Estimate beginning as soon as the specified and implied tasks have been identified. Info Ops must be developed to support both the Info Campaign and the overall JTFC's Campaign Plan and consequently Info Ops staff must ensure that the two requirements are melded together and potential conflicts of interest highlighted. Info Ops may merit a separate line of operation but must be integrated in all lines of operation; at times it may be the main effort. Info Ops staff will be responsible for providing the following elements as part of the Campaign Plan:

a.   The JTFC's Info Ops intent, key Info Ops objectives and constraints will be included in the main body of the Campaign Plan, which must identify the role of Influence Activity and CCA within it.

b.   Key Influence Activity audiences and themes will be identified and the linkage and relationship between Media Operations (Media Ops) and Influence Activity established in the main body of the Campaign Plan. Key CCA concerns will also be listed in the main body.

c.   Detail on processes such as: co-ordination measures, Info Ops target nomination procedures, nominations for inclusion in the Restricted Target List (RTL) and Joint Restricted Frequency List (JRFL), clearance and authorisation requirements for themes and messages and measurement of effectiveness will be included in the Info Ops Annex. An outline Info Ops Annex is attached at Annex 3C.

d.   Tasking and supporting information for key contributors to Info Ops activity will be included as individual appendices to the Info Ops Annex. These appendices are not fixed but will be situation dependent. They will include the key methods of achieving influence for that Campaign, usually:

(1)   Psychological Operations (PSYOPS).

(2)   Electronic warfare (EW).

e.   The desired Influence Activity objectives, themes, messages and tasks will be listed in the 'Info Ops Objectives Matrix' along with the CCA objectives and tasks (See example at Appendix C1). The matrix links Info Ops tasks back to the original Info Campaign or JTFC's Campaign Objectives and decisive points. These tasks will then be submitted for inclusion in the Joint Integrated Prioritised Target List (JIPTL) to ensure coherence between Info

Ops and broader military activity. Info Ops staff will also contribute to other annexes of the Campaign Plan such as targeting, Media Ops and CIMIC.

(INTENTIONALLY BLANK)

ANNEX 3A – INFORMATION AND INTELLIGENCE REQUIREMENTS FOR INFORMATION OPERATIONS

3A1.   Information Operations is predicated on good information and intelligence. This Annex provides a guide to those requirements. It is not intended to provide a detailed list of all intelligence requirements but indicates the type and range of intelligence required.

3A2.   **Background Information**. A thorough understanding of a crisis or conflict is essential to the conduct of Info Ops. This understanding enables the identification of target audiences and themes for Influence Activity and enables effective targeting of fixed installations as part of Counter-Command Activity (CCA). This understanding should include analysis of underlying structures and key actors.

3A3.   **Structures**. The structural analysis should cover the causes and enablers of conflict breaking them down into military, political, economic, social/cultural (including the media) and technological aspects.

> a.   **Military**. The regular (uniformed and state-employed) and irregular (terrorist, guerrilla, and paramilitary) military capability, its strengths, weaknesses, allegiances and motivation must be analysed. The attitudes of the population towards the military and the relationship of the military with the political leadership must be understood. HQs and other Command and Control (C2) nodes, formal civilian and military communications (fixed and mobile telephones, radio and Information Technology (IT) networks) and their supporting services, such as power supplies, should be analysed. The importance of informal linkages, such as long established social or tribal mechanisms along with modern developments such as text messaging and the Internet must also be understood.

> b.   **Political**. The political process both overt and behind the scenes must be understood. Relationships and dependencies between political parties, financial, media and military sources of support should be analysed. Formal and informal alliances, supportive and sympathetic organisations and countries should be noted.

> c.   **Economic**. The economic structure of the region, both formal (eg. manufacturing and agricultural) and informal (eg. drug production and the black market) must be analysed and the linkages between them and with the key actors identified.

> d.   **Social and Cultural**. The nature of society, its core values and beliefs, customs, attitudes and taboos must be understood, as must the degree and nature of politicisation. The analysis should consider the demographic

composition and population distribution of the region noting differentials that could be exploited. Many conflicts have their roots in events in the past, and certain events may have a symbolic importance. The local received version of history is critical to full understanding; local perceptions will be more important than historical fact. All media (international, regional and local) operating or with influence on the parties to the crisis must be analysed. The reach, influence, audience and credibility of all media must be understood.

e. **Technological**. The dependence of the state on IT and its use of the Electro-Magnetic Spectrum must be analysed in detail. The information systems used to support decision-making and disseminate decisions must be fully understood.

3A4. **Key Actors**. All key actors and their inter-relationships should be identified. Their personalities, leadership styles, ambitions, motivation, objectives (short and long term), current stance, dependencies, psychological profile and personal history must be fully understood. The complex, adaptive relationships and dependencies that exist between actors and social groups must be recognised.

3A5. **Dynamics**. Crisis and conflict is a dynamic process, dependencies, alliances and key issues will change, consequently background information must be updated with current information and intelligence. This will allow the development of specific Influence Activity messages and targeting as part of CCA.

3A6. **Monitoring**. The environment must be continuously monitored to measure the effectiveness of Info Ops actions and to guide their development. Measures of Effectiveness (MOE) will have been included in the Info Ops plan, and J2 should be tasked to collect the necessary information and intelligence. Particular attention should be paid to:

a. **Will**. Changes in the attitude of the civilian population, political activity, expressions of unrest. Amongst the military, increased desertion and line-crossing, and willingness to surrender. Signals Intelligence (SIGINT) and Human Intelligence (HUMINT) may detect reduced morale of leaders.

b. **Capability**. Reduced efficiency, disorganisation, slower reactions to events and specific actions in response to deception.

ANNEX 3B – FACTORS TO BE CONSIDERED FOR INFORMATION OPERATIONS PLANNING

3B1.   **Objectives**.

a.   **Own Objectives**. Analyse the CDS Directive, Joint Commander's (Jt Comd) Directive and Joint Task Force Commander (JTFC) mission analysis and guidance to identify:

(1)   The role of Information Operations (Info Ops) in supporting the achievement of the mission.

(2)   How master themes and master messages can be prosecuted within the Joint Operations Area (JOA). Ensure that they are entered into the Info Ops Objectives Matrix.

(3)   How Influence Activity and/or Counter-Command Activity (CCA) can assist in meeting specified and implied tasks as well as adding to the Info Ops Objectives Matrix.

(4)   How Info Ops actions can assist in meeting the JTFC's Campaign objectives and decisive points recommending options. Info Ops objectives must be linked to the JTFC's Campaign Decisive Points.

b.   **Allied/Coalition Objectives**.

(1)   Seek clarification on allied and coalition partners' objectives.

(2)   Do they have an Info Campaign and do they intend to conduct Info Ops?

(3)   If so, what procedures are in place to ensure coherence – is there a requirement for liaison and/or deconfliction mechanisms? Consider how to mitigate the impact of any lack of coherence and ensure that DTIO are aware of any conflicts of interest.

(4)   Do differences in objectives offer opportunities for adversary Info Ops and if so how can these be countered?

c.   **Host Nation/Administration Objectives**.

(1)   What role does the host nation or administration play in promoting messages?

(2)   How is coherence maintained between own, allied, coalition and host nation info campaigns?

(3)   Is there scope to support, make use of or influence host nation activity?

d.   **Regional/Neighbouring Objectives**.

(1)   What are the objectives of regional powers, neighbouring states and major adversary allies?

(2)   What effect might these have within the JOA?

(3)   How can these effects be countered or supported and who is responsible for doing so?

e.   **Other Actors' Objectives**.

(1)   What other actors, such as the UN, regional bodies or Non-Governmental Organisations (NGOs) are active within the JOA?

(2)   What are their objectives and what effect are they likely to have within the JOA?

(3)   How can these other actors be supported or influenced to assist in meeting Info Ops objectives?

3B2.   **Situation**.

a.   **Knowledge**.

(1)   Analyse current knowledge identifying gaps and submitting Requests for Information (RFI) as required.

b.   **Key Political, Cultural or Military Events**.

(1)   Can these be used as opportunities to promote themes and deliver messages?

(2)   Are sensitivities such that Info Ops and broader military activity should be constrained over these periods?

(3)   Ensure that key events are entered in the synchronisation matrix.

c.   **Political or Military Deadlines**.

(1)   Do these become Info Ops deadlines? If so they are likely to impact on the balance between Influence Activity and CCA and between persuasion and coercion.

d. **The Legal Status**.

(1)   What Memoranda of Understanding (MOUs) or Status of Forces Agreements (SOFAs) exist and how do these constrain activity.

(2)   What are the current Rules of Engagement (ROE)? Are these suitable or do changes need to be requested?

(3)   Do dormant ROE need to be developed?

e. **Availability of Resources**.

(1)   What resources are available and by when?

(2)   In conjunction with J3 advise on the Joint Force Element Table (JFET) and with J4 Movements (J4 Mov) begin to form the Desired Order of Arrival (DOA) of Info Ops assets.

(3)   What are the likely financial requirements? Bid through J8 Finance (J8 Fin) for money to ensure that in theatre activity is not delayed.

3B3.   **Influence Activity**. Identify:

a. **Influence Activity Objectives**.

(1)   Is the objective to reinforce or to change behaviour? This will have an impact on the time required to achieve the objective.

(2)   Can this be achieved by providing or denying information?

(3)   Can the objectives be achieved by assisting the target audience through informing or educating them or, do they need to be persuaded through force of argument and demonstration.

(4)   When should they be told of the benefits, risks and costs of particular behaviour?

(5)   Alternatively, does the objective require that the target audience to be mislead or compelled?

b. **Target Audiences and Themes**.

(1)   Analyse the population considering the leadership (Political, Military and Social/Cultural), regional and local groupings or factions as well as refugee, expatriate and internally displaced groups.

(2)　　Look for differences in perception, opportunity or status that could be exploited as themes.

(3)　　Consider possible divisions between urban and rural, employed and unemployed, rich and poor, nomadic or settled and within ethnic and religious groups.

(4)　　Analyse their value sets examining their motivation, beliefs and symbology establishing how these can be used as possible themes.

(5)　　Identify dependencies within and between groups and consider how these may be exploited.

(6)　　Identify those who will always resist the message.

c.　　**Message Propagation**.

(1)　　Consider how messages are spread within the target audience.

(2)　　What impact does the media have?

(3)　　What access does the population have to the media and to communications more generally (internet, mobile phones etc)?

(4)　　Which sources of information are trusted and which are not?

(5)　　What is the level of literacy and education, how will this impact on the format of messages?

(6)　　Identify the most effective available means of propagating messages.

3B4.　　**Counter-Command Activity**. Drawing on the Target Systems Analysis (TSA) identify:

a.　　**Counter-Command Activity Objectives**.

(1)　　Is the objective to affect command capability temporarily or permanently, partially or completely?

(2)　　Can this be achieved by disrupting, denying/degrading capability or will it need to be destroyed?

b.　　**Targets**.

(1)　　Analyse the processes, mechanisms and systems by which information is gathered and decisions made and disseminated in order to

identify critical nodes, redundancy and back up systems. These become potential CCA targets.

(2)   Identify the social and cultural importance of identified targets and cross check the impact that their attack may have on Influence Activity objectives.

3B5.   **Countering the Adversary Information Operations**.

a.   **Analysis**. Conduct a similar analysis of own objectives, motivation, capabilities and decision-making processes in order to identify weaknesses and vulnerabilities that the adversary may seek to exploit.

b.   **Objectives**. Identify possible adversary Info Campaign objectives, targets, target audiences and themes.

c.   **Defence**. Determine how to counter possible adversary Info Ops.

(INTENTIONALLY BLANK)

ANNEX 3C – OUTLINE INFORMATION OPERATIONS ANNEX

1. **SITUATION**	
a. Adversary Forces.	This paragraph should identify the decision-makers and influence holders at the appropriate levels. It should state their current positions and clarify their decision-making processes identifying both strengths and vulnerabilities within them. Plausible themes and approaches that might affect their decisions should be listed. Their ability, available techniques and likely intent to carry out Info Ops against allied forces should also be identified, as should their defensive capability. Key aspects of the human factors and infrastructure analyses should be listed.
b. Friendly Forces.	The main objectives of the Information Campaign and higher-level Info Ops plans should be summarised. The current positions of relevant allied forces, nations, factions and organisations (UN, EU, NATO etc.) should be stated and strengths and weaknesses identified. National capabilities to carry out Info Ops should be listed.
c. Other Nations.	The positions of other influential nations should also be identified. These may be neighbouring countries, regional organisations or members of the UN Security Council. Their ability to affect the desired end-state should be given and the key events or trends that may influence their action identified.
d. Main Target Audiences.	The main target audiences should be listed.
2. **MISSION**	This should be the mission statement from the Joint Commander.
3. **EXECUTION**	
a. Concept of Operations.	The concept of operations should list any Info Ops Decisive Points en-route to the end-state identifying lines of operation and applying tools to pursue approaches to achieve the desired effect. Key Info Ops objectives, themes and messages should be stated.
(1) JTFC's Intent.	The intent should state the decision and resulting action from each of the players: adversary, friendly or non-aligned.
(2) Main Effort.	

b. Tasks.
   (1) Influence Activity.
   (2) Counter-Command Activity.
	Tasks should be listed and identified in the Info Ops Objectives Matrix and then allocated and amplified in the text. Other annexes/appendices such as PSYOPS and EW should refer to the Info Ops Annex as appropriate.

c. Co-ordinating Instructions.
 	
   (1) Info Ops Objectives.
   (2) Measures of Effectiveness and Impact Analysis.
   (3) Intelligence Support.
   (4) Linguistic Support.
   (5) Infrastructure Support.
   (6) Approval and Release Authority.
	Co-ordinating Instructions should include the procedure for authorising subordinates Info Ops plans and specify any new co-ordination mechanisms/meetings. The subjects listed below will usually need to be addressed. Contained in the Info Ops Objectives Matrix (Appendix).
	
	In particular, the production of printed, voice and image material.

4. **ADMINISTRATION AND LOGISTICS**	
5. **COMMAND AND CONTROL**	

Appendices:	1. Info Ops Objectives Matrix. 2. Info Ops Synchronisation Matrix. 3. EW 4. PSYOPS Appendices should include the key means 5. OPSEC of achieving influence; these will depend 6. Deception on the situation. 7. CNO 8. Etc.

APPENDIX 3C1 - EXAMPLE OF THE INFORMATION OPERATIONS OBJECTIVES MATRIX

Themes to Avoid

Theme	Reason
• *Length of UK Deployment.*	• *Avoid constraining future options.*
• *Linkage between current operations and activities in other theatres.*	• *Retain focus on JOA and avoid mission creep*

Words or Phrases to Avoid

Words or Phrases to Avoid	Preferred Term
• *Crusade or Holy War*	• *War on Terrorism*
• *Evidence*	• *Information*

Objectives Matrix.

JTFC Campaign Phase	JTFC / Info Campaign DP/Obj	Info Ops Objective	Theme/Purpose	Message	Target/Target Audience	Task
All	JTFC-1 IC-3	1. *Establish legitimacy of military operations*	1.1 *Coalition is acting under a UN mandate*	1.1.1 *'The deployment of UK forces has been sanctioned by UNSCR 4325. Those acting to undermine peace have no mandate'*	1.1.1.1 *Neutral/ Uncommitted* 1.1.1.2 *Adversary*	• *Leaflet Drop* • *Radio Interview*
			1.2 *Coalition has wide international Support*	1.2.1 *'The coalition is made up of 12 nations from around the world'*	1.2.1.1 *International*	• *Press Article* • *Hold national cultural events*
1	JTFC-5	2. *Degrade radio and landline links between commander and deployed headquarters*	2.1 *Encourage use of alternative comms links to enable interception.*	2.1.1 *Your comms are unreliable and you should use eg. HF*	2.1.1.1 *Adversary C2*	• *Prevent (permanently) comms centre at ST43679826 from operating*
2	JTFC-2 IC-1	3. *Damage legitimacy of military leadership*	3.1 *Encourage dissent in adversary forces*	3.1.1 *Your leaders send you to face danger whilst remaining in safe locations* 3.1.2 *We have superior firepower*	3.1.1.1 *Adversary rank and file*	• *Leaflet drops* • *Constant harassment arty fire*

CHAPTER 4 – EXECUTION

401.   Information Operations (Info Ops) is essentially a co-ordination stratagem, with tasks being implemented by all or any military capabilities. Co-ordination of these tasks is therefore a major element in the execution of Info Ops to ensure that the desired and secondary effects of all Info Ops tasks, and broader military and civilian activities, are fully co-ordinated and coherent both on Will and Capability. This is achieved by considering the message that any action or inaction may send to the parties, and modifying or mitigating that message or activity during execution in response to developments in order to achieve coherence.

402.   **Co-ordination**. Within the Joint Task Force (JTF), Info Ops are integrated with broader military activity and executed through the existing targeting and campaign management procedures:[1]

    a.   **The Commander's Brief**. The aim of the Commander's Brief is for the Joint Task Force HQ (JTFHQ) staff to brief the Joint Task Force Commander (JTFC) on Campaign activity. The JTFC is briefed on the current and developing situation and likely adversary future intentions, which includes input from the Info Ops Officer on the progress towards Info Ops objectives.

    b.   **Joint Command Group Video Teleconference**. The aim of the Joint Command Group Video Teleconference (JCG VTC) is for the JTFC to receive output from the Defence Crisis Management Organisation (DCMO) with further direction from the Joint Commander (Jt Comd). Direction may include changes or additions to the Info Campaign themes and feedback on the success or otherwise of extant themes. The conference brings together the DCMO, JTFC and Component Commanders (CC), and acts as a catalyst to produce the day's agenda and focus for JTFHQ staff activity.

    c.   **Joint Operations Planning Group**. The Joint Operations Planning Group (JOPG) is the key working level meeting, ensuring continual development and synchronisation of the campaign plan. Info Ops staff will contribute to the review of progress against the Campaign Plan, as part of the Campaign Effectiveness Analysis (CEA) process and will update or modify their part of the plan as required.

    d.   **Joint Co-ordination Board**. The primary function of the Joint Co-ordination Board (JCB) is as an operations synchronisation board that reviews mission progress and allows the JTFC to update intent and guidance. He gives targeting guidance, approves the draft Joint Integrated Prioritised Target List (JIPTL) and authorises the Target Nomination List (TNL) and Joint Restricted

---

[1] Detailed guidance on the targeting and campaign management procedures is contained in JWP 3-00 '*Joint Operations*'.

Frequency List (JRFL). The Info Ops Officer attends the JCB to ensure that the Info Ops Plan is updated and that in managing the wider Campaign due note is taken of Info Ops issues.

e. **Joint Fires Element**. The Joint Fires Element (JFE) is effectively the 24 hr-targeting secretariat for the JCB and selects and prioritises targets from the Joint Integrated Target List (JITL) and JRFL in accordance with the JTFC priorities. Their output is a draft JIPTL for endorsement by the JCB. The Info Ops cell attends to ensure that proposed attacks are coherent with the Info Ops objectives and themes, proposes Info Ops targets for inclusion in the JIPTL and identifies where Info Ops may be able to contribute to the tasks of other Staff Divisions.

f. **Information Operations Planning Group**. The Info Ops cell is supported in its preparation for the JFE by the Info Ops Planning Group (IOPG). The Group is chaired by the Info Ops Officer and membership will comprise representatives from all key contributors to Influence Activity and Counter Command Activity (CCA) and from the Components. The Group will usually include J2, J3, J5(Plans), Media Ops, Civil Military Co-operation (CIMIC), Psychological Operations (PSYOPS), Electronic Warfare (EW), Political Advisor (POLAD) and Legal Advisor (LEGAD). The IOPG ensures that:

    (1) Info Ops targets and target audiences are nominated for inclusion in the JIPTL.

    (2) Resource requirements are identified and justified.

    (3) That gain/loss assessments have been conducted.

    (4) Proposed actions are legal and within the Rules of Engagement (ROE).

    (5) Progress is measured towards Info Ops Objectives and changes recommended where appropriate.

    (6) Measure(s) of Effectiveness (MOE) have been identified and are realistic.

g. **Joint Electronic Warfare Co-ordination Cell**. The Joint Electronic Warfare Co-ordination Cell[2] (JEWCC) co-ordinates EW with Info Ops through the IOPG and, with J6, compiles the JRFL to prevent electronic fratricide.

---

[2] Increasingly becoming known as the Joint EW and Signals Intelligence (SIGINT) Co-ordination Cell (JEWSICC), reflecting the increasing importance of SIGINT.

403.   **Civilian Linkages**. The effectiveness of Info Ops is improved if influence is exerted by all instruments of power and by local and regional governments and organisations that may be more readily trusted than 'external' parties. This requires the development of linkages to a wide range of external actors. Linkages should be enabled through CIMIC staff initially; however, the development of personal relationships is often the key to good information sharing and co-ordination. The JTFC may consider inviting key civilian actors to attend some co-ordination boards, or alternatively he may choose to exchange or accept liaison staff. It may prove appropriate to attach Info Ops staff to other nations' government, military and civilian HQs to advise and assist them in the conduct of Info Ops.

404.   **Clearance and Authorisation**. Info Ops requires the application of the principles of legality, military necessity, distinction, proportionality and cultural protection. The scale, tempo and sensitivity of operations will determine the level of ministerial involvement in the procedure for targeting and Info Ops with, where possible, target packages (or entire target lists) and intended themes being submitted for clearance in advance of operations. Ideally, 'silence procedures' should be used wherever possible. The detail on authority and powers of delegation are stated in the Targeting Directive, and Chief of the Defence Staff (CDS), with ministerial endorsement, may delegate the authority for target approval to the Jt Comd and ultimately to the JTFC.

405.   **Measuring Effectiveness**. CEA takes a broad view of the campaign and determines if the required effects as envisaged in the plan are being achieved, drawing on a wide range of sources, military and non-military. It is conducted across all levels. In order to feed the J5 led CEA process, Info Ops staff should identify the expected responses to a task during the planning phase and establish the indicators, known as MOE, that would demonstrate that these responses are taking place. The Info Ops contribution to CEA has four stages:

   a.   When possible identify the immediate impact of Info Ops tasks, confirming that the message has been delivered.

   b.   Task collection assets to detect the MOE indicators in order to confirm the expected longer-term response of each task.

   c.   Measure the cumulative effect over time of a series of tasks. This is achieved by:

      (1)   Establishing current attitudes and perceptions and articulating possible responses.

      (2)   Monitoring the environment over time and detecting trends.

(3)   Comparing subsequent actions with the pre-prepared model to allow trends to be identified and effects established.

d.   Recommend follow-up action where appropriate.

GLOSSARY OF TERMS AND DEFINITIONS

The reference for the terms and their definitions used in this Glossary is indicated in parentheses.[1] Those marked (JWP 3-80) are new and have yet to be endorsed.

Campaign
A set of military operations planned and conducted to achieve a strategic objective within a given time and geographical area, which normally involve maritime, land and air forces. (AAP-6)

Campaign Effectiveness Analysis
Analysis conducted at the strategic, operational and tactical level to monitor and assess the cumulative effects of military actions with respect to centres of gravity in order to achieve the overall campaign End State. (JWP-3)

Civil-Military Co-operation
The co-ordination and co-operation, in support of the mission, between the NATO commander and civil actors, including national population and local authorities, as well as international, national and non-governmental organisations and agencies. (MC411)

Command
The authority vested in an individual for the direction, co-ordination and control of military forces. (AAP-6)

Commander's Intent
A concise expression of the purpose of the campaign, the desired results and how operations will progress towards the desired end-state. At the tactical level, the commander's intent should be focussed on the effect that he wishes to achieve on the enemy. (JWP 0-01.1)

Components
Force elements grouped under one or more component commanders subordinate to the operational level commander. (JWP 0-01.1)

Computer Network Attack
Operations to disrupt, deny, degrade or destroy information resident in computers and computer networks or the computers and networks themselves. (MC 422)

---

[1] JWP 0-01 '*British Defence Doctrine*', JWP 0-10 '*United Kingdom Doctrine for Joint and Multinational Operations*' (UKOPSDOC), JWP 0-01.1 '*The United Kingdom Glossary of Joint and Multinational Terms and Definitions*', AAP-6 '*The NATO Glossary of Terms and Definitions*'.

Computer Network Defence
Actions to protect against disruption, denial degradation or destruction of information resident in computers and computer networks or the computers and networks themselves. (MC 422)

Computer Network Exploitation
Actions to gain access to, and exploit, the information hosted on information systems, and to make use of the system itself. (JWP 3-80)

Computer Network Operations
Actions to attack, exploit and defend friendly and adversary computers, computer networks and other information systems, and the software and data resident on them. (JWP 3-80)

Counter-Command Activity
Counter-Command Activity seeks to disrupt, degrade, deny, deceive or destroy those capabilities that assist or enable an adversary in making decisions and subsequently translating that decision into action. (JWP 3-80)

Deception
Those measures designed to mislead an adversary by manipulation, distortion or falsification. (AAP-6)

Decisive Point
A point from which a hostile or friendly centre of gravity can be threatened. This point may exist in time, space or the information environment. (AAP-6)

Directive
A military communication in which policy is established or a specific action is ordered. (AAP-6)

End-State
The political and/or military situation to be attained at the end of an operation, which indicates that the objective has been achieved. (AAP-6)

Electronic Countermeasures
That division of electronic warfare involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum through the use of electromagnetic energy. There are three subdivisions of electronic countermeasures: electronic jamming, electronic deception and electronic neutralisation. (AAP-6)

Electronic Protective Measures

That division of electronic warfare involving actions taken to ensure effective friendly use of the electromagnetic spectrum despite the enemy's use of electromagnetic energy. There are two subdivisions of electronic protective measures: active electronic protective measures and passive electronic protective measures. (AAP-6)

Electronic Warfare

Military action to exploit the electromagnetic spectrum encompassing: the search for, interception and identification of electronic emissions, the employment of electromagnetic energy, including directed energy, to reduce or prevent hostile use of the electromagnetic spectrum, and actions to ensure its use by friendly forces. (AAP-6)

Electronic Warfare Support Measures

That division of electronic warfare involving actions taken to search for, intercept and identify electromagnetic emissions and to locate their sources for the purpose of immediate threat recognition. It provides a source of information required for immediate decisions involving electronic countermeasures, electronic protective measures and other tactical actions. (AAP-6)

Forward Mounting Base

A base (also deployed operating base) established within the operational area, to support operations at forward operating bases. It will be resourced to a greater level than a forward operating base, including C2, logistics and administration support elements. (JWP 0-01.1)

Information Assurance

Information Assurance are Info Ops that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities. (DTIO Policy Paper dated 22 Feb 01)

Information Campaign

Co-ordinated information output of all government activity undertaken to influence decision-makers in support of policy objectives, while protecting one's own decision-makers. (DTIO Policy Update dated 22 Feb 01)

Influence Activity

Influence Activity comprises any activity whose primary purpose is to influence will, and is achieved by the promotion of identified themes to target audiences through messages. Influence Activity seeks to predispose, persuade, convince, deter, disrupt, compel or coerce target audiences to adopt a particular Course of Action CoA), or to assist, encourage and reassure those that are following a desired CoA. (JWP 3-80)

Joint
Connotes activities, operations, organisations, etc., in which elements of more than one service of the same nation participate. (AAP-6)

Joint Commander
The Joint Commander, appointed by CDS, exercises the highest level of operational command of forces assigned with specific responsibility for deployments, sustainment and recovery. (JWP 0-01.1)

Joint Co-ordination Board
The Joint Co-ordination Board (JCB) is an operation synchronisation meeting used to promulgate the JTFC's guidance and objectives to component commanders. It is his method of ensuring unity of effort. The board will review the Joint Integrated Prioritised Target List (JIPTL) to ensure that it reflects the JTFC's Campaign Plan and is in line with HMG objectives. (JWP 3-00)

Joint Fires Element
The Joint Fires Element is a staffing board whose role is to ensure the targeting plan takes full account of the JTFC's prioritised objectives within the overall campaign plan. It is also responsible for the co-ordination and de-confliction of JTFC controlled assets. It will produce the daily TNL from the JIPTL for later approval by the JCB. (JWP 3-00)

Joint Integrated Prioritised Target List
A prioritised list of targets, approved by the JTFC and maintained by a joint task force, which includes the Component Commanders' requirements. (JWP 0-01.1)

Joint Integrated Target List
A list of strategic and operational targets, co-ordinated by the PJHQ, to meet the JTFC objectives. (JWP 0-1.1)

Joint Operations Area
An area of land, sea and airspace, defined by a higher authority, in which a designated Joint Task Force Commander plans and conducts military operations to accomplish a specific mission. A Joint Operations Area including its defining parameters, such as time, scope and geographic area, is contingency/mission specific. (JWP 0-01.1)
A temporary area defined by a NATO strategic or regional commander, in which a designated joint commander plans and executes a specific mission at the operational level of war. Note: It is defined in co ordination with nations and approved by the North Atlantic Council or the Military Committee as appropriate, in accordance with NATO's Operational Planning Architecture. A Joint Operations Area and its defining parameters, such as time, scope of the mission and geographical area, are contingency- or mission-specific and may overlap areas of responsibility. (AAP-6)

Joint Operations Planning Group
The JOPG, attended by the JTFC and normally chaired by his COS, is the forum where progress against the campaign plan is analysed and measured. From this assessment will come direction on contingency planning that can be undertaken to capitalise on favourable developments or indeed help to offset or overcome setbacks. (JWP 3-00)

Joint Task Force Commander
The operational commander of a nominated joint force. (JWP 0-01.1)

Joint Task Force Headquarters
A purely national deployable joint headquarters of variable size commanded at the operational level by a Joint Task Force Commander. (JWP 0-01.1)

Media Operations
That line of activity developed to ensure timely, accurate, and effective provision of Public Information (P Info) and implementation of Public Relations (PR) policy within the operational environment, whilst maintaining Operations Security (OPSEC). (JWP 0-01.1)

Operations Security
The process which gives a military operation or exercise appropriate security, using passive or active means, to deny the enemy knowledge of the dispositions, capabilities and intentions of friendly forces. (AAP-6)

Psychological Operations
Planned psychological activities designed to influence attitudes and behaviour affecting the achievement of political and military objectives. (AAP-6)

Rules of Engagement
Directives issued by competent military authority which specify the circumstances and limitations under which forces will initiate and/or continue combat engagement with other forces encountered. (AAP-6)

(INTENTIONALLY BLANK)

GLOSSARY OF ABBREVIATIONS

C2	Command and Control
C4I	Command, Control, Communications, Computers and Intelligence
CC	Component Commander
CCA	Counter Command Activity
CCT	Current Commitments Team
CDS	Chief of the Defence Staff
CEA	Campaign Effectiveness Analysis
CGIG	Cross-government Implementation Group
CIMIC	Civil-Military Co-operation
CIS	Communications and Information Systems
CoA	Course of Action
CoG	Centre of Gravity
COG	Current Operations Group
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CPT	Contingency Planning Team
DCMO	Defence Crisis Management Organisation
DIS	Defence Intelligence Staff
DP	Decisive Point
DTIO	Directorate of Targeting and Information Operations
ECM	Electronic Countermeasures
EMS	Electromagnetic Spectrum
EPM	Electronic Protective Measures
ESM	Electronic Warfare Support Measures
EW	Electronic Warfare
FMB	Forward Mounting Base
HUMINT	Human Intelligence
Info Campaign	Information Campaign
Info Ops	Information Operations
IO	International Organisation
IOPG	Information Operations Planning Group
IT	Information Technology
JCB	Joint Co-ordination Board

JCG VTC   Joint Command Group Video Teleconference
JEWCC   Joint Electronic Warfare Co-ordination Cell
JFE   Joint Fires Element
JIPTL   Joint Integrated Prioritised Target List
JITL   Joint Integrated Target List
JOA   Joint Operations Area
JOPG   Joint Operations Planning Group
JRFL   Joint Restricted Frequency List
Jt Comd   Joint Commander
JTFC   Joint Task Force Commander
JTFHQ   Joint Task Force Headquarters

LEGAD   Legal Advisor

Media Ops   Media Operations
MIOCG   Military Information Operations Co-ordination Group
MOE   Measures of Effectiveness
MOU   Memorandum of Understanding

NIAT   National Infrastructure Assessment Team
NRG   News Release Group

OGD   Other Government Department
OPSEC   Operations Security
OSG   Operations Support Group

PJHQ   Permanent Joint Headquarters
POLAD   Political Advisor
PSYOPS   Psychological Operations

RFI   Request for Information
ROE   Rules of Engagement
RTL   Restricted Target List

SIGINT   Signals Intelligence
SOFA   Status of Forces Agreement
SPG   Strategic Planning Group

TNL   Target Nomination List
TSA   Target Systems Analysis

UNSCR   United Nations Security Council Resolution