Communications and Information Systems Support to Joint Operations

Joint Doctrine Publication 6-00
Third Edtion

JOINT DOCTRINE PUBLICATION 6-00

COMMUNICATIONS AND INFORMATION SYSTEMS SUPPORT TO JOINT OPERATIONS

Joint Doctrine Publication 6-00 (JDP 6-00) (3rd Edition) dated January 2008 is promulgated as directed by the Chiefs of Staff

Director General Development, Concepts and Doctrine

AUTHORISATION

The Development, Concepts and Doctrine Centre (DCDC) is responsible for publishing Joint Doctrine Publications (JDPs) within a hierarchy of similar publications. Readers wishing to quote JDPs as reference material in other work should confirm with the DCDC Doctrine Editor whether the particular publication and amendment state remains authoritative. Comments on factual accuracy or proposals for amendment are welcomed by the Doctrine Editor at:

The Development, Concepts and Doctrine Centre
Ministry of Defence
Shrivenham
SWINDON, Wiltshire, SN6 8RF

Telephone number: 01793 314216/7
Facsimile number: 01793 314232
Facsimile number: 01793 314232
Military Network: 96161 4232
E-mail: publications@dcdc.org.uk

DISTRIBUTION

Distribution of JDPs is managed by the Forms and Publications Section, DSDA Operations Centre, C16 Site, Ploughley Road, Arncott, Bicester, OX25 1LP. Requests for issue of this publication, or amendments to its distribution, should be referred to the DSDA Operations Centre. All other DCDC publications, including a regularly updated CD '*Joint Doctrine Disk*' (containing both JDPs and Allied Joint Publications (AJPs)), can also be demanded from the DSDA Operations Centre.

DSDA Help Desk: 01869 256052
Military Network: 94240 2052

All publications (including drafts) are available to view and download at: www.dcdc.dii.r.mil.uk. This publication is available on the internet at: www.mod.uk/dcdc.

JOINT DOCTRINE PUBLICATIONS

The successful conduct of military operations requires an intellectually rigorous, clearly articulated and empirically-based framework of understanding that gives advantage to a country's Armed Forces, and its likely partners, in the management of conflict. This common basis of understanding is provided by doctrine.

UK doctrine is, as far as practicable and sensible, consistent with that of NATO. The development of national doctrine addresses those areas not covered adequately by NATO; it also influences the evolution of NATO doctrine in accordance with national thinking and experience.

Endorsed national doctrine is promulgated formally in Joint Doctrine Publications (JDPs).[1] From time to time, Interim Joint Doctrine Publications (IJDPs) are published, caveated to indicate the need for their subsequent revision in light of anticipated changes in relevant policy or legislation, or lessons arising from operations.

Urgent requirements for doctrine are addressed in Joint Doctrine Notes (JDNs). JDNs do not represent an agreed or fully staffed position, but are raised in short order by the Development, Concepts and Doctrine Centre (DCDC) to establish and disseminate current best practice. They also provide the basis for further development and experimentation, and a doctrinal basis for operations and exercises.

Details of the Joint Doctrine development process and the associated hierarchy of JDPs are to be found in JDP 0-00 *Joint Doctrine Development Handbook*.

[1] Formerly named Joint Warfare Publications (JWPs).

RECORD OF AMENDMENTS

Amendment Number	Date of Insertion	Initials
Change 1	December 2011	DCDC

Change 1 to JDP 6-00 CIS Support to Joint Operations was promulgated in December 2011 and comprised a complete rewrite of Chapters 3 and 4. Change 1 provides updated or new doctrine on:

a. The nature and character of information flow on Joint operations.

b. The information services planning process.

c. The requirement for the commander to articulate his information needs.

d. The information exchange requirement process to translate the commander's information needs (*ends*) through the development of an appropriate architecture of core services and applications (*ways*) that can then be delivered by information and communication services (*means*).

e. The information services support to the conduct of operations during the deploy, operate and recover phases.

PREFACE

1. **Purpose**. Joint Doctrine Publication (JDP) 6-00 *Communications and Information Systems Support to Joint Operations* provides guidance for the planning and execution of Communications and Information Systems (CIS) support to Joint operations. This edition is intended primarily for personnel employed within the Defence Crisis Management Organisation (DCMO) including the Permanent Joint Headquarters (PJHQ), a Joint Task Force Headquarters (JTFHQ), Joint Force CIS (JFCIS) staff, Front Line Commands (FLCs), the Directorate General Information Systems and Services (DG ISS) and the wider CIS community. In any operation, it is essential that staff understand the Commander's information needs and support them with CIS; all staff branches have an important role in CIS planning, and all officers engaged in Joint operations should be familiar with this publication.

2. **Context**. This 3rd Edition of JDP 6-00 builds upon previous editions, and includes updated processes and procedures developed for the ongoing evolution of CIS. Although this document is based on the deployment of a JTFHQ, it is equally valid under other operational constructs and different scales of operations. The generic principles contained within this document should be adapted for specific operations.

3. **Structure**. JDP 6-00 has 4 Chapters: Chapter 1 introduces the fundamental elements and principles governing CIS support; Chapter 2 outlines the roles and responsibilities of those organisations that contribute to CIS planning and capability; Chapter 3 describes the information services planning process; and Chapter 4 describes the processes and activities that provide information services support to the conduct of operations.

4. **Linkages**. To satisfy an urgent need for CIS doctrine, JDP 6-00 was drafted ahead of the 4th Edition of JDP 0-01 *British Defence Doctrine* and the revised editions of JDPs 01 *Campaigning*, 3-00 *Campaign Execution* and 5-00 *Campaign Planning*, which together will provide the updated overarching context.

(INTENTIONALLY BLANK)

COMMUNICATIONS AND INFORMATION SYSTEMS SUPPORT TO JOINT OPERATIONS

CONTENTS

CHAPTER 1 – INTRODUCTION

101. Successful Communications and Information Systems (CIS) support to operations combines the fundamentals of the Information Exchange Requirement (IER), CIS capability and Information Management (IM) to achieve operational advantage. After describing these fundamentals in detail, this Chapter introduces enduring CIS principles of prioritisation, agility, capacity, interoperability and security that are applied to operational CIS planning and execution. It then outlines the operational context for CIS support.

Fundamentals

102. **Communications and Information Systems**. CIS are 'the assembly of equipment, methods and procedures, and if necessary personnel, organised so as to accomplish specific information, conveyance and processing functions'.[1] In the modern battlespace, effective IM and subsequent information superiority is only achieved with properly deployed and managed CIS. CIS are an essential part of military operations and provide commanders at all levels with the means to exercise Command and Control (C2) and disseminate vital information. CIS are also an essential prerequisite for Network Enabled Capability (NEC),[2] which allows increased situational awareness, supports better decision making and greater operational agility for an Effects-based Approach (EBA).[3] The role of J6 staff is to ensure that CIS delivers robust and flexible solutions to meet this requirement.

103. **Information Exchange Requirement**. The IER translates an operational information requirement into the detail required by CIS staff to provide capability throughout all phases of an operation. It stimulates development of the CIS solution and forms the basis for developing a CIS network design.

104. **Information Management**. IM underpins the successful prosecution of military operations. It is 'the integrated management processes and services that provide exploitable information on time, in the right place and format, to maximise freedom of action'.[4] It enables effective information exploitation and the achievement of situational awareness by commanders and staffs. IM is as much about managing people, and their methods of working, as it is about the provision of CIS. Detailed aspects of IM are at Annex 1A.

---

[1] AAP-6 '*NATO Glossary of Terms and Definitions*'. Note that CIS represents a capability; the term Information and Communication Services (ICS) describes the services available.

[2] Strategic Defence Review New Chapter (July 2004) defined NEC as 'encompassing the elements required to deliver controlled and precise military effect rapidly and reliably'.

[3] UK EBA embodies a way of thinking and specific processes that together enable the effective use of military capability, usually as part of a Comprehensive Approach (CA), to achieve favourable outcomes. (See JDP 01 (2nd Edition) '*Joint Operations*' – programmed for promulgation early 2008).

[4] New term developed for this publication and future UK doctrine – see Annex 1A2.

105. **Battlespace Spectrum Management**. The use of and reliance upon the Electromagnetic Spectrum (EMS), by both military and commercial users, has increased significantly in recent years and shows no signs of abating. Effective use of the Electromagnetic Environment (EME)[5] is a prerequisite for successful operations, and the ability to manoeuvre within it is enabled by Battlespace Spectrum Management (BSM).[6]

106. **Operational Advantage**. The relationship between the 3 fundamentals of CIS – the IER derived from the Operational and CIS Estimate, the CIS capability itself, and associated IM – together with the enabling BSM, is shown at Figure 1.1.

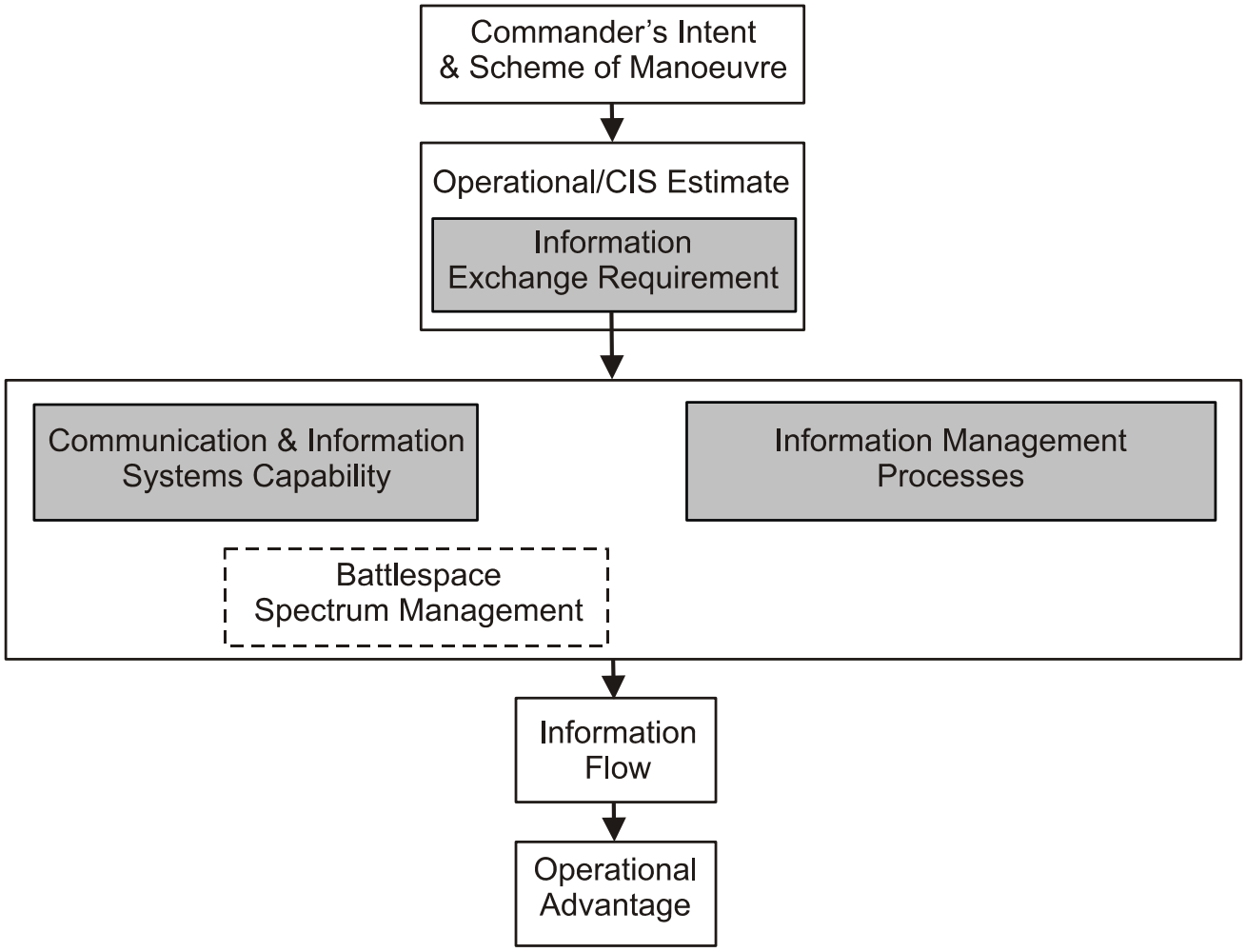


Figure 1.1 – Fundamentals and Operational Advantage

[5] Electromagnetic Environment is 'the totality of electromagnetic phenomena existing at a given location'. (JDP 0-01.1) Also see CDS 01/06 '*UK Joint EW Policy*'.

[6] Battlespace Spectrum Management (BSM) is defined as 'the planning, coordination and management of the electromagnetic spectrum through operational, engineering and administrative procedures'. (ACP 190(B)) The BSM function and process is covered in Chapter 3.

Principles of CIS

107. Throughout all stages of operational CIS planning and execution, a number of enduring principles are applied to ensure that the most effective and efficient CIS solution emerges to accommodate the Commander's Intent. These principles are:

a. **Prioritisation**. Commanders and their staffs should be aware that the CIS required are roughly proportional to the scale of the operation. However, other factors also need to be considered. There is an irreducible minimum level of CIS capability required to support either a Joint Task Force Headquarters (JTFHQ) or National Contingent Commander's Headquarters (NCCHQ) and their subordinate Component Headquarters (HQ), irrespective of the scale of combat forces deployed. This is an important consideration when the UK is involved in multiple, concurrent operations even of moderate scale. In all operations, there is a need to set rigorous priorities for the allocation of limited CIS resources, including bandwidth, based upon the Commander's Intent and information needs set out in the IER.

b. **Agility**. Agility[7] provides the ability to respond quickly and appropriately to change; as with other critical combat assets, flexibility and resilience are of particular importance for CIS:

(1) **Flexibility**. Flexibility ensures that deployed CIS can respond to changes in scales of effort, operational tempo and posture. Changes in posture, such as from peacekeeping to peace-enforcement, may result in minor changes to force structure, but could result in a considerably different CIS requirement. Flexibility is achieved through the production and rehearsal of contingency plans, the standardisation of equipment, the use of commercial systems and infrastructure, mobile and transportable CIS equipment, freedom of manoeuvre within the EME and reserve capability.

(2) **Resilience**. Availability, permanence and training all contribute to resilience. Due to its critical enabling role, the availability of CIS is a high priority. However, available and durable CIS is not necessarily resilient without properly trained personnel to run and manage it. Permanence is a significant element of resilience and is achieved by redundancy. This includes the distribution and replication of CIS and its associated data, and protection against physical, electronic and environmental attack.

c. **Capacity**. Although CIS capacity is invariably finite, advances in technology have increased significantly the volume and rate of data delivery.

[7] Agility has 5 attributes: responsiveness, resilience, flexibility, acuity and adaptability'.

To avoid slowing decision-making processes, care should be taken to ensure that sufficient CIS capacity is available to support IM and Information Exploitation (IX) requirements. Sufficient capacity should be made available to meet predicted demand, but occasions may arise where CIS limitations precipitate the adoption of different IM or IX strategies. Where possible, technologies and procedures are used to maximise capacity, for example through the use of dynamic bandwidth management, Internet Protocol (IP) switching and efficient IM. Early use may also be made of commercial CIS to increase capacity.

d. **Interoperability**. Interoperability[8] of systems is required to allow the passage of information between different elements of a deployed Joint Task Force (JTF) or, on multinational operations, between allies. However, optimal IM and IX are only achieved through operating with common systems. Where common systems are not available, such as is in coalition operations, interoperability between systems offers the next best option to support Joint or multinational operations. The requirement is essential, to allow commanders to exercise command and to enable all elements of the (Combined) JTF to coordinate activities. A core CIS requirement of a Comprehensive Approach (CA)[9] is for integrated IM techniques, infrastructure and connectivity, to enable advanced working practices, including communication networks for collaboration between Other Government Departments (OGDs), Non-Governmental Organisations (NGOs) and International Organisations (IOs).

e. **Security**. Operations Security[10] (OPSEC) can be compromised unless consideration is given to the security of information held on, and transmitted by, CIS. The quality and reliability of CIS have a direct impact on security.[11] If commanders, staff and CIS users perceive or experience poor communications, they frequently revert to unprotected devices such as civilian mobile telephones. On Joint and multinational operations, there is a requirement to work in multiple information domains (RESTRICTED, SECRET and TOP SECRET). These levels may be supplemented by others defined by release criteria, such as UK/US, NATO, or 'Coalition'. Such hierarchies enable concurrent handling of sensitive, protected intelligence, UK Eyes-Only information, information shared on a bilateral or multilateral basis and unprotected information.

[8] Interoperability of systems is defined as 'the ability of systems to provide services and information to (or accept services and information from) other systems'. (AAP-31)
[9] A Comprehensive Approach is 'an approach that responds effectively to complex, contemporary crises by the orchestration, coordination or de-confliction of military, OGD, and (where possible) IO and NGO activity'. (See JDP 01 (2nd Edition) for detail – programmed for promulgation early 2008).
[10] OPSEC is 'the process which gives a military operation or exercise appropriate security, using passive or active means, to deny an adversary knowledge of the dispositions, capabilities and intentions of friendly forces'. (AAP-6)
[11] Security is dealt with in detail in Chapter 3.

108. Security principles are interrelated and should be considered together, noting that some appear to act in opposition; for example, the need for security versus the need for interoperability. The overriding premise throughout is to understand and meet the commander's requirements.

Operational Level

109. JDP 6-00 '*Communications and Information Systems Support to Joint Operations*' primarily addresses the provision of CIS at the Operational level;[12] that is, providing CIS capability spanning strategic to tactical assets and at all scales of operation to enable C2 between the Permanent Joint Headquarters (PJHQ), the JTFHQ[13] and Component HQs.[14] A simplified diagram showing the principal HQ engaged at this level of command is at Figure 1.2. Operating with other nations and IOs may generate a more complex C2 structure than that shown at Figure 1.2; the detail is considered in later chapters.

[12] The Operational level is 'that at which campaigns and major operations are planned, conducted and sustained to accomplish strategic objectives within theatres or areas of operations'. (JDP 0-01.1)
[13] A JTFHQ is 'a purely national deployable joint headquarters of variable size commanded at the operational level by a Joint Task Force Commander'. (JDP 0-01.1)
[14] Components are 'force elements grouped under one or more component commanders subordinate to the operational level commander.' (JDP 0-01.1)

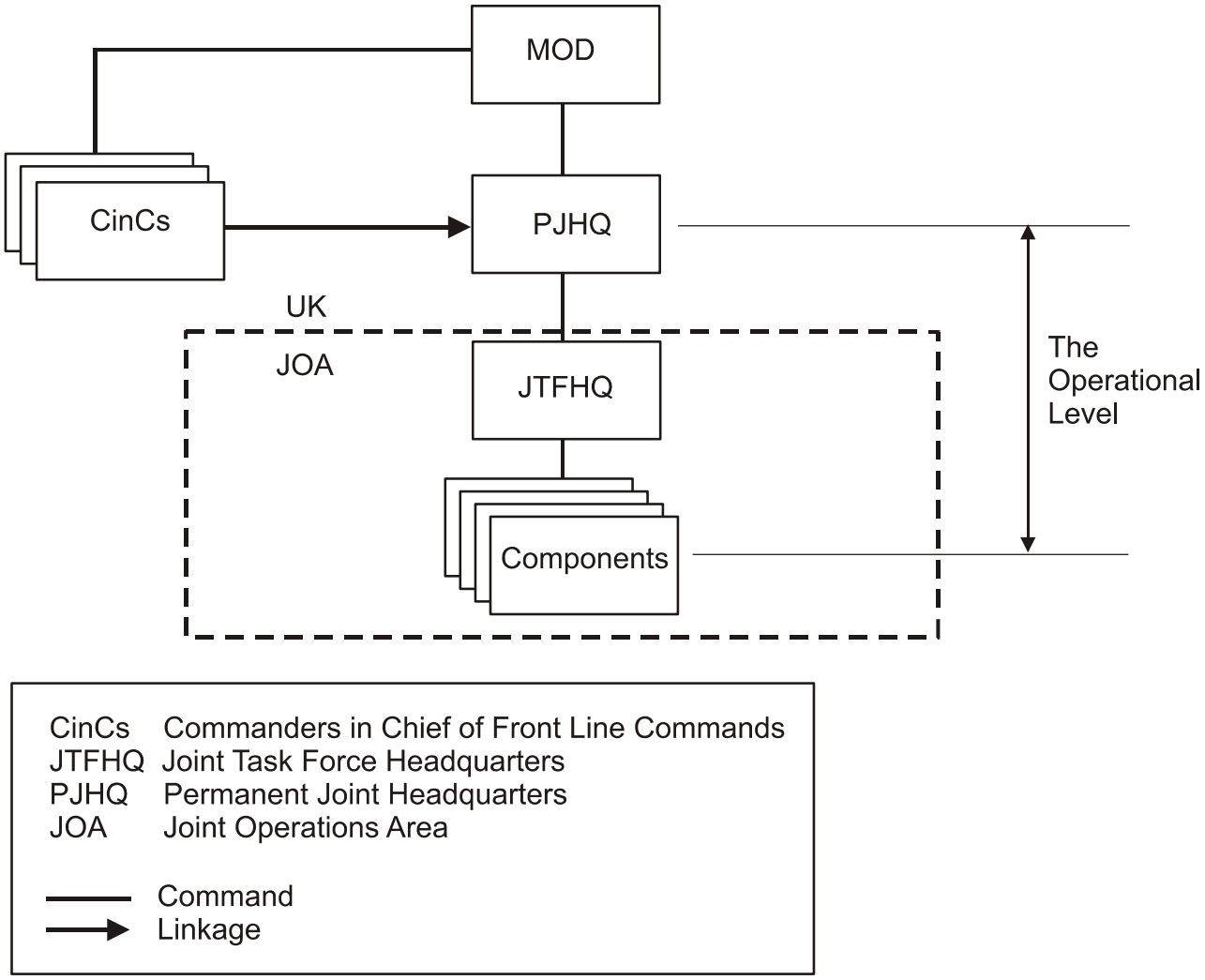


Figure 1.2 – Operational Level of Command

110. Within a JTFHQ, the J6 Division is normally led by Commander Joint Force CIS (Comd JFCIS) (OF-4 to OF-6 dependent on scale). J6 is responsible for enabling the IER across the JTF, and for planning and controlling Joint Operations Area (JOA) CIS architectures, including integration at the Strategic and Tactical levels. Comd JFCIS directs the Joint Network Centre (Jt NETCEN) to manage, coordinate and control the delivery of CIS capability across the JOA.

ANNEX 1A – INFORMATION MANAGEMENT

CONTEXT AND DEFINITIONS

1A1. **Information**. Data, information, knowledge and intelligence are inter-related manifestations of fact or perceived fact that have varying degrees of utility for commanders and their staff. Data is the basic building block of information, comprising facts and statistics that can be manipulated by individuals or machines. Information is the meaning that an individual associates with data when it is presented in context. Information combined with experience, interpretation and reflection, generates knowledge and thereby enables effective use of the information, for example in decision-making. One individual's knowledge becomes another's information, and thus information and knowledge are managed through the same Information Management (IM) processes.[1] In parallel, intelligence is an ability to acquire and apply knowledge. Military intelligence normally refers to processed, analysed and assessed information and knowledge about adversaries or potential areas of operation.[2] Management of intelligence is the same for that of any other information.

1A2. **Definitions**. IM and its associated terms[3] are defined as:

a. **Information Management**. Integrated management processes and services that provide exploitable information on time, in the right place and format, to maximise freedom of action.

b. **Information Exploitation**. The use of information to gain advantage and improve situational awareness to enable effective planning, decision-making, and coordination of those activities required to realise effects.

c. **Information Administration**. The structuring and handling of information to enable it to be stored, archived, located and retrieved efficiently, whilst ensuring its integrity.

d. **Information Assurance**. The confidence that the information within the Defence Community is maintained reliably, accurately, securely and is available when required.[4]

1A3. IM encompasses the Joint enabling activity that underpins effective information exploitation and common situational understanding by commanders and

[1] The term knowledge management is in common use in parts of industry and academia and with some international partners. It is not used in this JDP.
[2] Intelligence is 'the product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations'. (AAP-6 '*NATO Glossary of Terms and Definitions*')
[3] New terms developed for this publication and for future UK doctrine.
[4] JSP 440 '*Defence Manual of Security*'.

staffs. Figure 1A.1 demonstrates the IM bridge between the infrastructure, upon which the bulk of information resides, and its exploitation. Exploitation leads to situational understanding that, when combined with experience and culture, results in intuitive or reasoned risk assessment and decision-making. IM comprises:

a. Determining information needs.

b. Managing information flow.

c. Administering information.

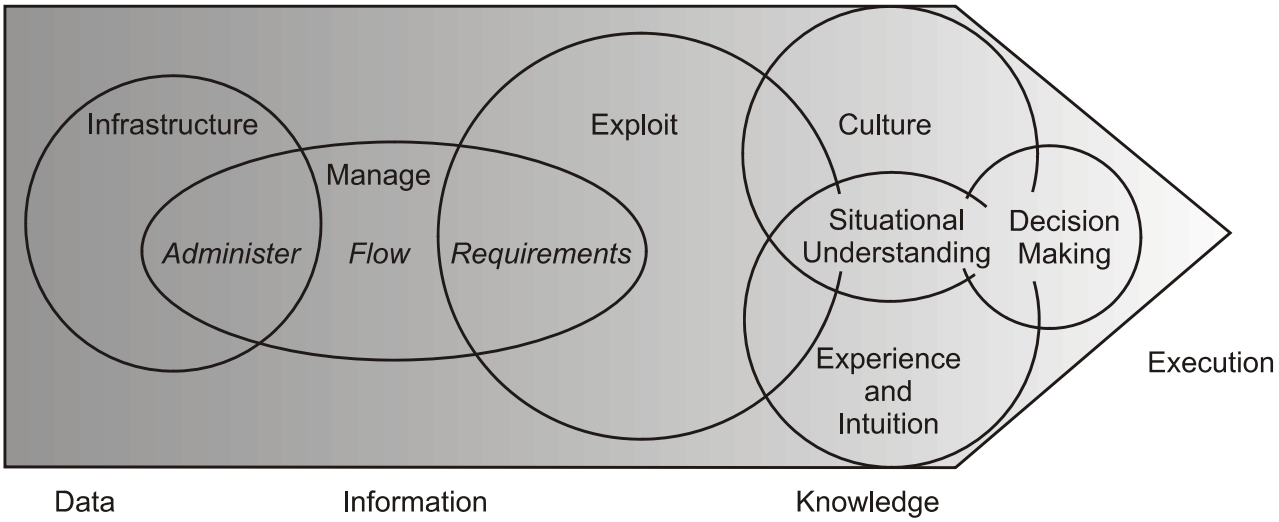


Figure 1A.1 – Place of IM in Decision-making

Information Needs and Planning

1A4. **Information Management Planning**. An IM Plan is derived from the Operational Estimate, the Permanent Joint Headquarters (PJHQ) Information Exploitation (IX) Directive, and associated Force IM planning conferences. It sets out the direction, priorities and resource allocation for IM within the HQ and its subordinate commands, taking account of the Commander's Intent and Communications and Information Systems (CIS) constraints. This relationship is shown in Figure 1A.2. Once IM is reflected comprehensively in HQs' Standing Operating Procedures/Instructions (SOPs/SOIs), an IM Plan should focus simply on any variations to established procedures. IM planning specifically:

a. Determines the information needs and outputs of the organisation, leading to a Joint Operations Area (JOA) Information Flow Analysis (IFA). This in turn enables production of the Joint Information Exchange Requirement (IER) and identifies changes to Reports, Returns and Responses (R3).[5] Many

[5] R3 provide information to meet Campaign Rhythm decision-making requirements. They are directed by the chain of command and may be automated or achieved through the maintenance of common databases or publishing to the web.

information needs are standard and are captured in SOPs/SOIs, but others are operation-dependent and specifically identified.

b. Provides input to the CIS estimate and to national/international system interface requirements, whilst taking account of CIS constraints.

c. Determines changes to Information Administration, particularly for coalition operations, and takes account of planned Campaign Rhythm .

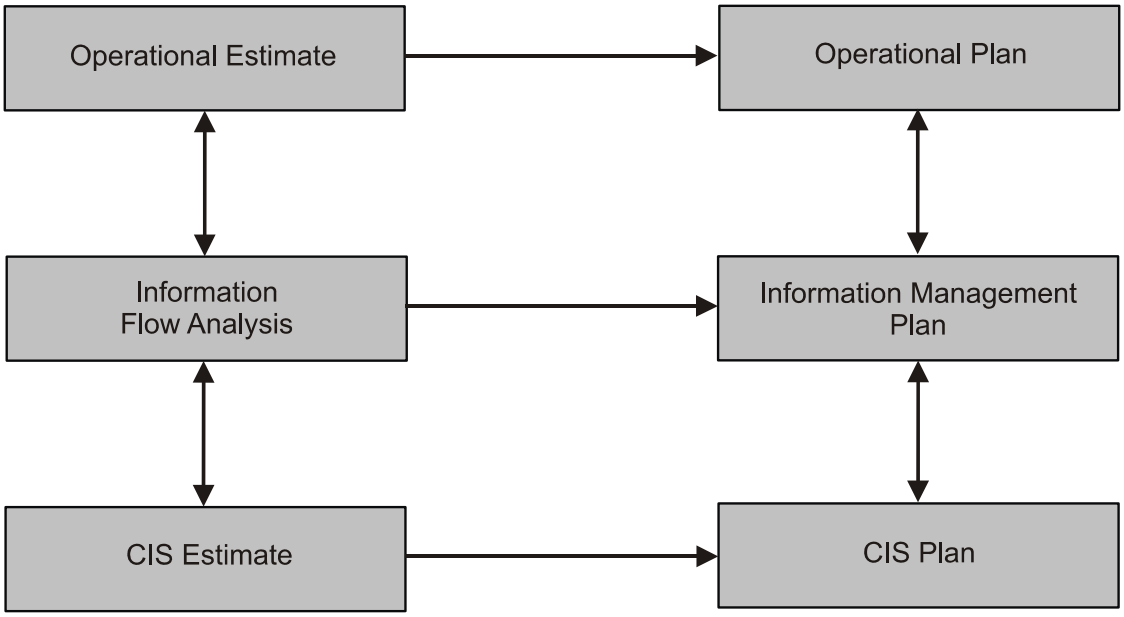


Figure 1A.2 – Plans and Estimates

1A5. **Information Needs Analysis**. Information needs vary according to task, mission, own and coalition force composition, opposition and neutral forces and JOA. Framing these needs requires input from all elements of an organisation and, whilst adaptive, the initial analysis should be comprehensive if information providers and the information infrastructure are to deliver effectively. Whether for the Operational Estimate, during the planning process, or by individuals and teams engaged in particular tasks, framing information needs requires identification of:

a. The content, format and timeliness of outputs to deliver the effect, from formal directives through R3 to the Joint Operations Picture (JOP). Maintaining output currency is a prime consideration, in which case modularity or use of databases is preferable to single long documents.

b. The membership of teams to deliver these outputs. Increasingly, these are cross-organisational, rather than J1-J9 focused, in order to bring the requisite expertise to bear.

c. Information needs to service required outputs.

d. Acquisition sources and lead times. Compiling reference and environmental information for a particular operation can take significant time and could impose a constraint unless providers are identified and tasked early.

1A6. **Agility**. Unresponsive operational plans, information clutter and lack of actionable information all impede the decision-making cycle. To be flexible and adaptable, staffs at all levels should continually think ahead to ensure that potentially critical information is available to their own organisation and, as importantly, to superior, subordinate or peer organisations. With fluent retrieval techniques, sharing information allows rapid access and is fundamental to the achievement of agility.

1A7. **Coalition**. Information flow within a coalition is constrained by immature system interfaces, language difficulties and security concerns. A coalition generally operates a tiered structure of network domains, interfacing through gateways that ideally allow information to be transferred automatically between partners. On enduring operations, a coalition network may be established for exactly this purpose. Sharing information is, however, limited by national security or release constraints. National Senior Information Officers (SIOs)[6] should engage early with coalition partners to determine how and what information flows across coalition interfaces. Where the UK provides the operational lead, the senior deployed UK SIO takes responsibility for multinational Joint Force information flow.

1A8. **Comprehensive Approach**. Within a Comprehensive Approach (CA), IM relies on an understanding of the complex, multi-dimensional information requirements of each department and the needs of the inter-departmental structure. Whilst there is an enabling technological aspect to IM, the fundamental issue is the orchestration of collaborative ways of working between departments. In the context of Government-wide crisis management, the MOD should be prepared to harmonise its IM requirements, principally those of the Defence Crisis Management Organisation (DCMO), with those of other Government Departments (OGDs) and agencies as detailed in paragraph 203.

[6] The Senior Information Officer (SIO) owns the information within the organisation, sets policy and culture and is accountable for the quality, and provenance of the information produced. The SIO leads the organisation's staff work and is likely to be the Chief of Staff (COS) or equivalent.

CHAPTER 2 – ROLES AND RESPONSIBILITIES

201. Chapter 2 outlines the roles and responsibilities of those organisations that contribute to the planning and provision of Joint Communications and Information Systems (CIS). The process of planning and conducting a campaign is explained in detail elsewhere.[1] This Chapter covers those organisations that provide high-level context and direction, and then focuses on the roles responsibilities of the CIS community at the Operational level, including the Front Line Commands (FLCs), to deliver CIS operational capability. A diagram outlining how these organisations interact is at Annex 2A. The Chapter also highlights the additional complexities and terminology of multinational operations. The roles and responsibilities outlined below introduce elements of the Joint CIS planning process, examined in detail in Chapter 3.

SECTION I – HIGH LEVEL CONTEXT

Defence Crisis Management Organisation

202. The Defence Crisis Management Organisation (DCMO) is formed from existing Ministry of Defence (MOD) departments and the Permanent Joint Headquarters (PJHQ). It is the MOD's agent for the overall management and resolution of crises, including the higher level direction of operations. It is responsible for the dissemination of strategic direction through PJHQ to the Joint Task Force Commander (JTFC) and Component Commander(s) (CC).

203. Whilst the DCMO does not have dedicated CIS staff, it receives advice on J6 issues from Director Command and Battlespace Management/J6 (D CBM/J6). Within a Comprehensive Approach (CA), the DCMO is responsible for integrating Information Management (IM) techniques, infrastructure and connectivity with Other Government Departments (OGDs), Non-Governmental Organisations (NGOs) and International Organisations (IOs).

Directorate of Command and Battlespace Management/J6

204. D CBM/J6 is the MOD's Joint Customer for J6 strategic systems and Joint CIS capabilities. A principal role of D CBM/J6 is to provide military strategic CIS guidance, and advice on relevant CIS freedoms and constraints, leading up to and during the formulation of any Joint CIS plan. The primary planning output from D CBM/J6 is the CIS Annex to Chief of Defence Staff's (CDS') Directive. This Annex nominates the supported and supporting commands, confirms the contribution of Directorate General Information Systems and Services (DG ISS) as a supporting

[1] JDP 01 '*Joint Operations*' explains the principles that underpin the planning and conduct of campaigns and operations by the UK's Armed Forces. JDP 5-00 '*Joint Operations Planning*' flows directly from JDP 01, and together with JDP 3-00 '*Joint Operations Execution*', form the UK authority on the conduct of deployed Joint operations.

agency, and provides high-level CIS direction to the Joint Commander (Jt Comd). It is produced with input from DG ISS and in consultation with PJHQ.

205. From an early stage of crisis management and preparation for operations, D CBM/J6 liaises with PJHQ J6 and DG ISS, and coordinates activity with Director Special Forces (DSF) J6 staff. D CBM/J6 allocates military satellite terminal equipment and satellite channels and sets high-level service restoration priorities. If there is insufficient military bandwidth available, D CBM/J6, through DG ISS, arranges support from other nations via a Memorandum of Understanding (MOU) or uses other methods to secure services from another country or commercial provider.

206. D CBM/J6 also acts as the focal point for Computer Network Defence (CND) and works with the Joint Security Coordination Centre (JSyCC) to ensure that any Computer Network Attack (CNA) on CIS inside or outside the Joint Operations Area (JOA) does not disrupt the Global Information Infrastructure (GII) supporting the operation. Additional responsibilities include the provision of secure voice equipment for Defence Attaches, and Foreign and Commonwealth Office (FCO) Posts at a time of crisis.

Deputy Chief of Defence Staff (Equipment Capability)

207. The MOD's Deputy Chief of Defence Staff (Equipment Capability) (DCDS(EC))'s support to CIS is provided by Capability Manager (Information Superiority) (CM(IS)). Within CM(IS), the Directorate of Equipment Capability Command Control and Information Infrastructure (DEC CCII), and its associated Integrated Project Teams (IPTs) within Defence Equipment and Support (DE&S), are responsible for staffing Urgent Operational Requirements (UOR). UORs address gaps in operational CIS capability, and may include accelerating ongoing projects or implementing commercial solutions.

Directorate General Information Systems and Services

208. DG ISS provides Information and Communication Services (ICS) to meet Defence needs and a single point of contact for strategic planning. The organisation was formed to subsume all the former single-Service elements, providing strategic communications. DG ISS is involved at an early stage of crisis management. Consultation with PJHQ J6, for example, may enable reconfiguration of strategic communications assets in response to evolving plans.

209. DG ISS and FLCs satisfy Information Exchange Requirements (IER) for PJHQ in order to meet the Commander's Intent, and DG ISS provides end-to-end service assurance for Defence CIS. DG ISS is engaged in operational planning with PJHQ J6, Joint Force CIS (JFCIS) staff, DSF and FLCs from the earliest opportunity; the

organisation is a major contributor to the CIS Estimate[2] through all phases of an operation. DG ISS achieves this by coordinating the efforts of its IPTs and Defence CIS Service Delivery partners, and by working with PJHQ, Commander JFCIS (Comd JFCIS) and FLCs to design the optimum ICS solution. The resultant 'network of networks' is managed through DG ISS' Global Operations and Security Control Centre (GOSCC). As the primary Defence CIS service provider, DG ISS is the Design Authority for the operational CIS solution.[3]

SECTION II – OPERATIONAL LEVEL OF COMMAND[4]

Joint Commander and Permanent Joint Headquarters

210. **Joint Commander**. The Jt Comd, appointed by CDS, is usually the Chief of Joint Operations (CJO) and he commands assigned UK forces on most deployed operations. He also provides military advice to CDS and is responsible for liaison with the MOD, allies, coalition partners and OGDs.

211. **Permanent Joint Headquarters J6 Division**. The J6 Division is integral to the PJHQ and supports the Jt Comd in planning, directing and sustaining CIS capability. It is involved in all stages of the crisis management process and at all stages of operations. It is thus the pivotal J6 organisation and is critical to mounting and conducting Joint CIS operations.

Front Line Commands

212. The 3 single-Service Commanders-in-Chief (CinCs), Commander- in-Chief Fleet (CINCFLEET), Commander-in-Chief Land Command (CINCLAND) and Commander in Chief Air Command (CINCAIR), provide trained Force Elements (FE) for Joint and multinational operations. Each FLC has a CIS Branch to undertake operational planning in support of the Jt Comd. Although operational command and control of assigned FE is exercised through the Joint chain of command, individual FLCs retain full command of their respective FE. FLCs are also responsible for the provision of CCs and their Headquarters (HQs) including CIS, infrastructure, life support and protection.

Director Special Forces

213. DSF commands all UK Special Forces (UKSF) and provides advice to CJO and the JTFC. He nominates a Special Forces (SF) CC and the DSF J6 Branch

[2] PJHQ or Commander JFCIS lead the Joint CIS Estimate, see Chapter 3.
[3] The role of Design Authority is defined by JSP 440 '*Defence Manual of Security*' as 'A Single Point or Committee that has the knowledge and the authority to ensure that technical decisions relating to the end-to-end Service delivery architecture are informed and coherent with wider plans and future projections.'
[4] This Section should be read in conjunction with JDP 3-00 (3rd Edition) '*Joint Operations Execution*', programmed for promulgation early 2008.

coordinates the CIS support required. The deployed SF J6 staff, signal unit, or detachment commanders coordinate Joint Force CIS with Joint Task Force Headquarters (JTFHQ) J6.

Joint Task Force Commander and National Contingent Commander

214. CDS appoints a JTFC for Joint national or multinational operations, based upon the recommendation of the Jt Comd. In multinational operations not under a UK lead, the UK National Contingent Commander (NCC) normally sits alongside the Lead Nation's appointed JTFC. Comd JFCIS is the senior J6 staff officer to the UK JTFC or NCC. In a national operation, all of the JTFHQ's CIS capability is provided through Comd JFCIS, but in a multinational context the CIS requirement is influenced by the UK's role in the operation.

Joint Task Force Headquarters

215. **Joint Force Headquarters**. The Joint Force Headquarters (JFHQ) is an integral element of PJHQ, under the command of a 1* Chief of Joint Force Operations (CJFO); it provides an experienced and cohesive staff to project military forces rapidly and over long distances. JFHQ is held at the highest readiness and, where speed is paramount, is the JTFHQ of choice. It provides the basis of other potential JTFHQs[5] held at lower readiness states. All of these HQs have the J6 capability to support enduring operations worldwide.

216. **Operational Liaison and Reconnaissance Team**. A core JFHQ capability is the Operational Liaison and Reconnaissance Team (OLRT).[6] Each OLRT comprises a small team of personnel with organic CIS capability, held at the highest readiness. Several OLRTs can be deployed simultaneously to give expert advice on contingency planning and operational issues, including force composition, logistics, command, control, and communications.

217. **Commander Joint Force Communications and Information Systems**. The delivery and management of Joint CIS across the JOA is a complex task, usually requiring a Comd JFCIS, reflected in the CIS Annex to CDS' Directive. From this, the Jt Comd issues a CIS Annex to his own Directive, written by PJHQ J6, detailing Comd JFCIS' responsibility to direct the CIS/Information and Communications Services (ICS) in the JOA and to provide operational CIS advice to the JTFC and staff. The CIS Annex also specifies the Operational level freedoms and constraints for Comd JFCIS. Typically, Comd JFCIS is delegated Operational Control (OPCON) of all CIS assets in the JOA, less SF, and draws core staff from JFHQ J6. It is augmented by other J6 staff from PJHQ, FLCs, DG ISS and other organisations, to match the scale and nature of the operation. Comd JFCIS' responsibilities are outlined in the generic

[5] There are 5 principal JTFHQ models. (See JDP 3-00 (3rd Edition) – programmed for promulgation in early 2008).
[6] For detailed information on ORLTs. (See JDP 5-00 (2nd Edition) – programmed for promulgation in early 2008).

Terms of Reference at Annex 2B. When CDS' Directive does not stipulate the need for a dedicated Comd JFCIS, in a small-scale operation for example, then a post should be nominated within JFHQ J6 or the J6 Division at PJHQ to fulfil the role. In the case of concurrent operations, when more than one Comd JFCIS is required, they are likely to be provided from 1 and 11 Signal Brigade (Sig Bde).

218. **Joint Network Centre**. An integral element of the JFCIS staff is the Joint Network Centre (Jt NETCEN), which has responsibility for the management, coordination, control and delivery of CIS across the JOA. The Jt NETCEN's role is to provide technical advice, undertake service, network and asset management, identify risks to the required CIS capability, liaise with OGDs and implement Comd JFCIS' direction. In a Joint Rapid Reaction Force (JRRF) deployment, a cadre of staff from 11 Signal Sig Bde form the core of the Jt NETCEN, augmented by personnel held at graduated readiness in FLCs and DG ISS. In operations without a significant JRRF contribution, the Jt NETCEN function is provided by the lead FLC. DG ISS acts in support of the GOSCC to manage the operational network. Dependent on the CIS design and the scale and nature of the operation, further augmentation may be required from the Defence Computer Incident Response Team (DCIRT) and the Joint Data Link Management Organisation (JDLMO).

Components

219. The UK's JTF uses 5 Tactical-level Components whose individual size and shape are determined by the operation.[7] These are the Joint Force Maritime, Land, Air, Special Forces and Logistic Components (JFMC, JFLC, JFAC, JFSFC and JFLogC).

220. **Maritime Component**. The Joint Force Maritime Component Commander (JFMCC) and his staff are likely to be found from the Maritime Battlestaff (MARBATSTAFF).[8] The JFMC HQ is located either afloat or ashore depending on the operation. The deployment or transition of the Maritime Component Commander (MCC) ashore requires significant planning and CIS capability that may have to be provided from outside CINCFLEET's resources, through liaison between PJHQ, Comd JFCIS and HQ FLEET.

221. **Land Component**. The Joint Force Land Component Commander (JFLCC) and his staff may come from any Field Army formation. The JFLC HQ may be augmented with strategic communication bearers and information systems to allow integration into a Joint Force, but there is no standing JFLC J6 staff branch.

[7] For more detail see JDP 3-00 (3rd Edition) – programmed for promulgation in early 2008.
[8] These are: at the 2* level, COMUKAMPHIBFOR and COMUKMARFOR and, at the 1* level, COMUKTG, COMATG and Commander 3 Commando Brigade. The commander of a smaller Task Group (TG) may also be appointed the MCC, if appropriate.

Consequently, the planning, execution and integration of Land CIS capability relies heavily on liaison between PJHQ, Comd JFCIS staff and HQ LAND.

222. **Air Component**. The standing Joint Force Air Component Headquarters (JFACHQ) provides the Joint Force Air Component Commander (JFACC) and core staff. Like the JFHQ, it is fully resourced and supported with CIS capability, elements of which are held at very high readiness.

223. **Special Forces Component**. Given the complexity and sensitivity of SF operations, the command of the SF Component is exercised in different ways, with the Joint Force Special Forces Component Commander (JFSFCC) reporting to MOD, PJHQ or the JTFHQ. The JSFC HQ may collocate with the JTFHQ. SF J6 staff, signal unit or detachment commanders coordinate SF CIS issues with the JFCIS.

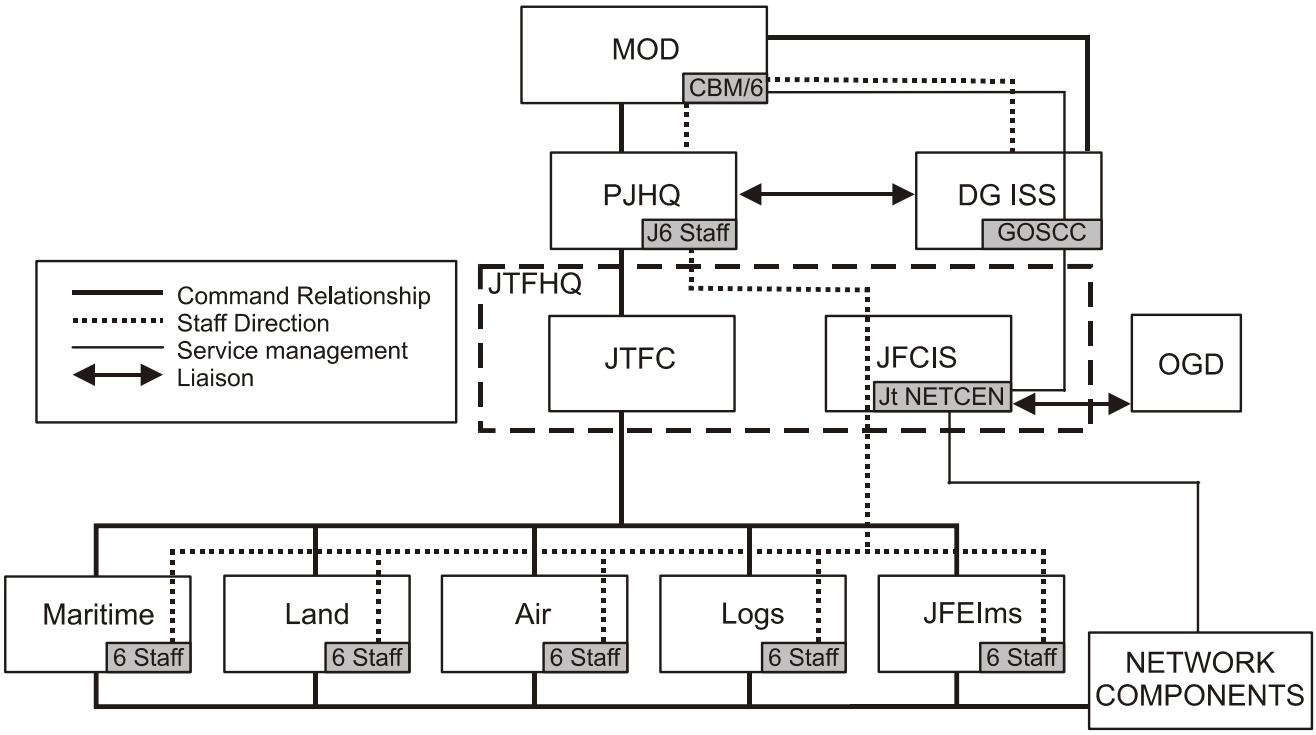
224. **Logistic Component**. The standing Joint Force Logistic Component Commander (JFLogCC) serves under CJFO with a small permanent cadre of staff including a J6 officer. The JFLogCC's responsibility for Reception, Staging, Onward Movement and Integration (RSOI) places a high priority on the early identification of the JFLogC IER.

225. **Component and Unit Network Centres.** Individual components and specialist formations may have their own NETCENs. Where appropriate, these NETCENs are linked through the Jt NETCEN to the GOSCC and use common processes and procedures to provide coherent end-to-end CIS service delivery. A core capability in all network operations is the full integration of Paradigm Services, DG ISS' civilian Private Finance Initiative (PFI) partner in providing an array of ICS for Defence, including SKYNET Satellite Communications (SATCOM) and the 'Welcome' welfare package for deployed personnel. Similarly, current and future Defence Information Infrastructure (DII) is being delivered in partnership between DG ISS' DII IPT and the ATLAS consortium.

SECTION III – MULTINATIONAL OPERATIONS

226. The CIS requirements of a UK force in multinational operations, whether North Atlantic Treaty Organisation (NATO), European Union (EU) or within an *ad-hoc* coalition, are influenced by the UK's role and status within that operation. The most likely roles for the UK, including general and specific CIS considerations, are described in Annex 2C.

ANNEX 2A – ORGANISATIONS THAT DELIVER OPERATIONAL COMMUNICATIONS AND INFORMATION SYSTEMS



Note: All of the organisations shown, from the Strategic to Tactical level, either liaise or work directly with civilian partner companies to deliver operational Communications and Information Systems (CIS) capability. Paradigm Services is the Directorate General Information Systems and Services' (DG ISS) Private Finance Initiative (PFI) partner in delivering an array of Information and Communications Services (ICS) for Defence, including SKYNET Satellite Communications (SATCOM) and the 'Welcome' welfare package for deployed personnel. Similarly, current and future Defence Information Infrastructure (DII) is being delivered in partnership between the DG ISS and the ATLAS consortium.

(INTENTIONALLY BLANK)

ANNEX 2B – GENERIC TERMS OF REFERENCE FOR COMMANDER JOINT FORCE COMMUNICATIONS AND INFORMATION SYSTEMS

2B1. Commander Joint Force Communications and Information Systems (Comd JFCIS) is an officer experienced in Joint CIS matters, normally from the permanent CIS staff of the Front Line Commands (FLCs), Permanent Joint Headquarters (PJHQ) or Joint Force Headquarters (JFHQ). He is delegated Operational Control (OPCON) of all CIS capability in the Joint Operations Area (JOA), less Special Forces (SF), and directs all CIS on behalf of the Joint Task Force Commander (JTFC).

2B2. Comd JFCIS is appointed by the Joint Commander (Jt Comd), as detailed in the CIS Annex of the Jt Comd's Directive to the JTFC. The rank of the Comd JFCIS is determined by the scale of the operation, the quantity and complexity of the CIS support required, and by any representational considerations arising in multinational operations.

2B3. Comd JFCIS is responsible for:

a. Providing CIS advice to the JTFC.

b. Exercising OPCON of all JTFC-assigned CIS capability within the JOA, less SF, commensurate with the JTFC's Scheme of Manoeuvre (SoM).

c. In conjunction with J3 staffs, developing, ratifying and maintaining the Joint Information Exchange Requirement (IER) for the operation.

d. Conducting the CIS Estimate.

e. Leading the CIS capability audit for the operation, facilitating the agreed design of the CIS solution, and staffing Urgent Statements of User Requirement (USUR) to PJHQ so that existing capability can be generated or Urgent Operational Requirements (UORs) can be staffed.

f. Overseeing and producing the CIS Implementation Plan, Operations Orders, configuration (authority for design and control), freedoms and constraints[1] and information/CIS risks in the Joint CIS Instruction (JCISI) to all JOA CIS elements.

g. Informing PJHQ J6 of all CIS issues and risks that may have impact at the operational level, including the Alerting, Warning and Reporting of

[1] Freedoms and constraints are derived from the Operational Estimate, and other sources such as doctrine and SOPs. Where constraints are not specified, Comd JFCIS allows components the freedom to configure and operate CIS assets provided they are not part of a wider network or Joint Force Command and Control integration.

incidents, including those from the Joint Network Centre (Jt NETCEN), as the sub-Warning and Reporting Point (WARP).

h. Liaison with Host Nation (HN), multinational, Other Government Department (OGD), Non-Governmental Organisation (NGO) and International Organisation (IO) representatives for JOA CIS requirements.

i. Adhering to the Joint Operational Standards (JOS) for the JFCIS.

j. Directing the Jt NETCEN.

k. Ensuring the effective integration of civilian service providers in JFCIS and Jt NETCEN to achieve the required level of operational CIS capability.

ANNEX 2C – MULTINATIONAL AND MULTI-AGENCY OPERATIONS

2C1. There are many considerations peculiar to multinational and multi-agency operations, including the nuances of Other Government Departments (OGDs) and Host-nation Support (HNS), which are considered during the planning process. Moreover, the UK may play different roles which impact upon Communication and Information Systems (CIS) planning.

2C2. **General Considerations**. General considerations for multinational operations include interoperability, Information Management (IM) and liaison:

a. **Interoperability**. Interoperability in a multinational or multi-agency environment adds considerable extra complexity.[1] This complexity is reflected at each level of command and should be considered under 3 main categories: technical, security and procedural.

b. **Information Management**. Effective IM is critical to maintaining operational tempo in a multinational or multi-agency environment. An Information Manager is appointed to ensure that appropriate IM processes are established and adhered to. UK protectively marked information is released in accordance with UK security procedures.[2]

c. **Liaison**. The potential frictions of working in a multinational or multi-agency environment are mitigated by the use of Liaison Officers (LO). While too many LOs could potentially slow Headquarters' (HQ) tempo, multinational or multi-agency environments usually benefit from employing LOs. In support of a Comprehensive Approach (CA), LOs from OGDs and Non-Governmental Organisations (NGOs) are particularly useful in overcoming procedural and cultural barriers.

2C3. **Specific Circumstances**.

a. **Lead Nation**. As Lead Nation, the UK is responsible for CIS planning and provision of CIS to the multinational Joint Task Force HQ (JTFHQ). This includes embedding UK LOs with partner nations to coordinate planning in the Joint Operations Area (JOA). Other nations are expected to provide their own CIS in accordance with the overall CIS plan. Early liaison between CIS staff is essential to ensure coherence, including the incorporation of other nations' LOs into a national HQ.

[1] PJHQ J5 should provide detailed guidance on the status of any UK force.
[2] JSP 440 '*Defence Manual of Security*'.

b. **Framework Nation**. As Framework Nation, the UK is expected to provide the majority of the CIS infrastructure to enable other nations to integrate within the overall force structure. There may also be a requirement for LOs with organic CIS, should interoperability issues arise in a multinational or multi-agency environment.

c. **Contributing Nation**. Where the UK's role is that of a Contributing Nation, there is a requirement to appoint a UK National Contingent Commander (NCC), who is located in, or represented at, the multinational HQ. As a Contributing Nation, the UK seeks to establish a NCC HQ alongside the multinational JTFHQ. It is also possible that the UK could provide embedded staff within the JTFHQ. Any requirement to provide national CIS for embedded staff is the responsibility of the NCC J6 staff. Integration and interoperability of multinational CIS remains a challenge, and this can result in the provision of numerous national systems to enable personnel to operate effectively in the multinational environment.

d. **Joint Task Force Headquarters and Combined Component Headquarters**. The Lead Nation for a multinational operation is expected to provide the JTFHQ and much of the multinational component HQs.[3] On high-readiness operations, such HQs are usually established using national CIS assets. LOs are expected to operate within these HQs, and the deployed HQ then migrates to a fully integrated HQ with embedded staffs from other nations.

e. **North Atlantic Treaty Organisation Operations**. UK forces engaged in North Atlantic Treaty Organisation (NATO) operations are incorporated into NATO Command and Control (C2) structures and use a combination of NATO and national CIS. The UK often contributes personnel to a NATO CIS cell.

f. **European Union Operations**. In European Union (EU) operations, an Operational HQ (the equivalent of PJHQ), and a Forward HQ (the equivalent of JTFHQ), are nominated.

g. ***Ad Hoc* Coalitions**. *Ad hoc* coalitions are increasingly common.[4] They are invariably based on *ad hoc* C2 structures, and interoperability challenges may be exacerbated by the lack of protocols or common operating procedures. A centralised coordination function is required in most *ad hoc* operations to facilitate the interconnection and interoperability of CIS.

[3] The Component HQs for combined maritime, land, air, logistics and Special Forces (SF) operations.
[4] For example, Non-combatant Evacuation Operations (NEOs) in Africa with France and Belgium, Op LANGER in East Timor with Australia.

2C4. **Host-Nation Support**. On many operations, deployed CIS is enhanced by local CIS, thereby adding diversity and robustness to the CIS solution. Factors to be considered for HNS CIS support include:

a. **Availability**. The ability of Host Nation (HN) civil and allied military communications to support military operations, including peacekeeping operations, depends upon the local situation. The lack of HN commercial services usually requires the deployment of an alternative CIS solution to cater for the majority of Information Exchange Requirements (IERs). Communications support is often central to broader HNS, and this should be coordinated centrally through J4 for inclusion in any Memorandum of Understanding (MOU) or other agreements between the UK and the HN. It will be necessary to obtain the appropriate clearances for spectrum use from the HN as detailed in Annex 3B.

b. **Permanence**. HNS may not endure throughout the operation, particularly if the political situation changes. This requires further negotiation with the HN government, through UK diplomatic representatives, to secure HNS CIS for the full duration of the operation.

c. **Location**. The availability of HN civil and military CIS varies considerably. Where some HN CIS capability exists, consideration should be given to using the HN's commercial international telecommunications services, provided that appropriate security safeguards are established. It is vital that Joint Task Force (JTF) capability does not rely wholly on facilities that are susceptible to poor maintenance, equipment failure, financial constraints or sabotage.

d. **Diplomatic Communications**. In the early stages of an operation, the local Diplomatic Post may provide the primary communications link with the UK, particularly for a reconnaissance team. Most Diplomatic Posts have a range of communications facilities that can be augmented during a crisis through coordination with Directorate of Command and Battlespace Management J6 (D CBM/J6).

e. **Civil Air Management**. Civil air management communications may not be available. Local and coalition circumstances may influence the use of military air management vice civilian communications systems.

f. **Liaison**. To facilitate a CA, communications links may be required from the JTF to local government and administrative authorities. Should HN or commercial services be unsuitable for the task, UK military CIS capability may be needed.

(INTENTIONALLY BLANK)

CHAPTER 3 – INFORMATION SERVICES PLANNING

SECTION I – INFORMATION FLOW ON JOINT OPERATIONS

301. There has always been a requirement to transfer information across the battle space. Operational advantage can be gained by managing information better, in relative terms, than your adversary to gain understanding and influence; this is known as information superiority.[1] Conceptually the flow of information has 3 component parts. First; the commander directs what information he needs so that it can be collected from all sources, fused, interpreted and fed to him/his staff. Second; the commander and his staff use the information to gain a degree of understanding and situational awareness of the battle space; this understanding, which is influenced by the commander's experience and intuition, enable him to make a decision on what actions to take next. Finally; the commander's decision on a course of action is disseminated to the organisation so that they can enact his direction.

302. **The Character of Information Flow**. Advances in technology have not changed the nature of the information requirements but have changed its character. Modern technology has revolutionised the information flow in the battle-space providing the commander with significant new capabilities that can deliver operational advantage. Information can now be transferred almost instantaneously, over greater range and volume, in a range of formats to commanders located anywhere in the world. This explosion in the availability of information and ability to manipulate does not in itself enhance either understanding or decision-making but it is critical enabler. Conversely the volume of information, the requirement to integrate numerous information sources and speed of reaction can result in information overload that can lead to decision paralysis. It can also lead to dependency on specific technology, applications or bearers to deliver mission critical information; this leads to reliance on potential single points of failure.

303. **Exploitation and Management of Information**. Information superiority is enabled by the successful management and exploitation of information. The management and exploitation of information are interdependent and delivered by a combination of the bearer systems that transfer data, the applications[2] that convert data into information, and the automated and staff functions to understand the information and then exploit it. Information management is a set of integrated management processes and services that enable and support the capability of collectors, producers and users to store, locate, retrieve and transform information, allowing it to become the right information in the right form and of adequate quality. Information

[1] Defined as *possessing a greater degree of information about the Battlespace, being able to exploit that information more rapidly and preventing the adversary from obtaining or exploiting information which would give combat advantage.* JDP 0-01.1, *UK Glossary of Joint and Multinational Terms and Definitions* (7th Edition).

exploitation is a function for all the staff branches because it gets the most value out of the information we have. The key is the common sharing, usage and re-usage of information to support the provision of staff situational awareness and understanding, planning, decision-making and the co-ordination of desired effects.

304. **Risk Management**. Managing the risk of single points of failure requires that the planning process considers the primary, alternative, contingent and emergency modes of working. This will require the allocation of sufficient resources to each mode and that training in using these reversionary modes is conducted by both specialist J6 and the wider staff. The risk must also be considered when assessing the balance between information-rich static headquarters and the more limited connectivity available to agile manoeuvring or mobile headquarters. The Joint Task Force Commander (JTFC) owns these risks and mitigates them by balancing the resilience of the information flow across the battlespace against the availability of resources; requiring him to prioritise mission critical services. To manage the risk requires a clear appreciation of the commander's information needs and how they both enhance his understanding and support his decision-making process. This appreciation must inform and guide the development of staff processes and provision of applications. Only through a combination of process and technology can effective information management be achieved that delivers the right information, on time, in the right place and in the correct format in order to exploit it.

305. **Information Services Planning Process**. The information services planning process develops the JTFC's information needs to the detail required for execution by specialist J6 staff. This requires the identification of:

a. What information the commander needs?

b. What timeframe (real-time, near real-time or higher latency)?

c. How is it presented, to what level of depth or detail, how accurate does it need it to be?

d. Who does it need to be shared with (multinational, host nation, other government departments etc)?

306. While many of the commander's information needs can be explicitly drawn out of his statement of information needs and the operational estimate, others may be implied or not immediately identifiable. The information services planning process must test the completeness of the requirement by running a set of standard *mission threads* against the proposed concept of operations, using the intended command and control structure; identifying the totality of information flows required across the battlespace. The combination of specified, implied and derived information needs

provide the foundation for developing the required information and communications services architecture and eventual network design.

307. The rest of this Chapter describes the information services planning process and explains how it contributes to the overall operational planning process.[3] It emphasises the key deliverables and highlights the fundamental elements that are required to fully enable, exploit and support information services on operations

SECTION II – LIFECYCLE

308. Planning and execution of information services are broken down into 4 phases of *prepare* (discussed in this Chapter), *deploy*, *operate* and *recover* (discussed in Chapter 4). These sub-headings derived from the High-Level Operational Concept are broadly aligned with the information services lifecycle known as the Joint Information Communications Services Operating Framework[4] (JICSOF). In outline these phases are:

a. **Prepare**. During this phase, the PJHQ J6 staff, normally augmented by Commander Joint Force CIS (Comd JFCIS), SO1 J6 within the Joint Task Force Headquarters (JTFHQ), Director Information services and Service (DISS) and Front Line Commands (FLCs) develop an information services plan that can deliver the commanders information needs. Several courses of action are developed and refined in line with the emerging direction from the JTFC. The final solution is selected by Comd JFCIS; endorsed by PJHQ J6; and DISS,[5] as the network authority, with the FLCs delivers the plan. The *prepare* phase concludes after a successful testing and commissioning of the selected information services plan articulated as the CIS Directive.[6]

b. **Deploy**. Upon deployment Comd JFCIS will deliver the initial operating capability identified in the CIS Directive. This will define and prioritise the delivery of services to the key staff. Component J6 staff will advise Comd JFCIS of their initial operating capability states and identify any

[3] See JDP 5-00, *Campaign Planning*, (Edition 2).
[4] The JICSOF is derived from Information Technology Infrastructure Library (ITIL) version 3. ITIL version 3 was developed by the UK Office of Government Commerce and industry and is the most widely accepted approach to information services management. The lifecycle consists of Strategy, Design, Transition, Operation and Continual Service Improvement. The information services lifecycle can be mapped against the sub-headings used in this Chapter. The strategy and design phases of the JICSOF aligned with the key elements of *prepare*. The operation phase in the JICSOF is aligned with *sustain*. JICSOF transition appears twice; first, as the final part of the *prepare* continuing through to *deploy*, and secondly, as part of *recover*. This is because both provisioning and retiring an information service are both transitional activities. For an expeditionary operation the lifecycles align but during the *sustain* phase of an enduring campaign the information services lifecycle will be continuously followed as new or updated services are provisioned or old services are retired.
[5] DISS is the Network Authority for all defence information architectures. It does this through its role as the Network Capability Authority (NCA), Network Technical Authority (NTA) and Network Operating Authority (NOA) – See paragraph 404 for more details.
[6] The CIS Directive forms the J6 element of the JTFC Mission Directive.

issues that may affect delivery within the timelines prescribed in the CIS Directive. Once full operating capability has been achieved for all the Joint staff and components then Comd JFCIS will declare this to the commander and PJHQ.

c. **Operate**. The provision of information services will constantly adapt during an operation as the commander's information needs, technology and other factors change. This can lead to enhancements, reductions and other developments of the architecture and network design. The operation of information services is the business of DISS, as the Network Operating Authority, and the Joint Network Centre (Jt NETCEN). These 2 organisations have joint responsibility for maintaining the network, conducting service management and delivering service assurance. JFCIS staff focus on delivering new requirements and maintaining the information exchange requirement.

d. **Recovery**. Termination of the operation or transfer of services to another Nation will result in the *recovery* phase being initiated. Maintenance of relevant information services until the last person departs will be a significant challenge; however, data management and retention of historical data will be equally time consuming unless considered early within this phase. Upon return to the UK, the FLCs are responsible for the regeneration process.

SECTION III – FUNDAMENTALS

309. To deliver the JTFC's information needs J6 staff must develop a detailed understanding of all C4ISR,[7] logistic and medical applications and core services, how information flows to enable the services, and the network design and capabilities over which the information is collected, transmitted, stored, retrieved and protected. This understanding of how the layers are interconnected, especially in the ISR[8] domain, enables the successful planning and execution of information services in the contemporary operating environment.

310. The information services planning process is shown at Figure 3.1. It should start as early as possible; recognising that in the early stages of planning, key political decisions may not have been made. The commander must clearly articulate his information needs to achieve an effective and appropriate plan. Information services planners will also require a full understanding of the information needs of staff branches, components, subordinate levels of command, and other supported actors[9]

[7] C4ISR: C4 Intelligence Surveillance and Reconnaissance or Command, Control, Communications and Computation Intelligence Surveillance and Reconnaissance. C4 ISR is the more common usage.
[8] Intelligence, surveillance and reconnaissance.
[9] Within a integrated approach military information services may require to support, or interact with, other government departments, host nation and multinational partners. In addition the Special Forces (SF) component will be supported.

involved in the operation. This ensures that any limitations in delivering the required information services can be used to inform the commander's operational estimate.

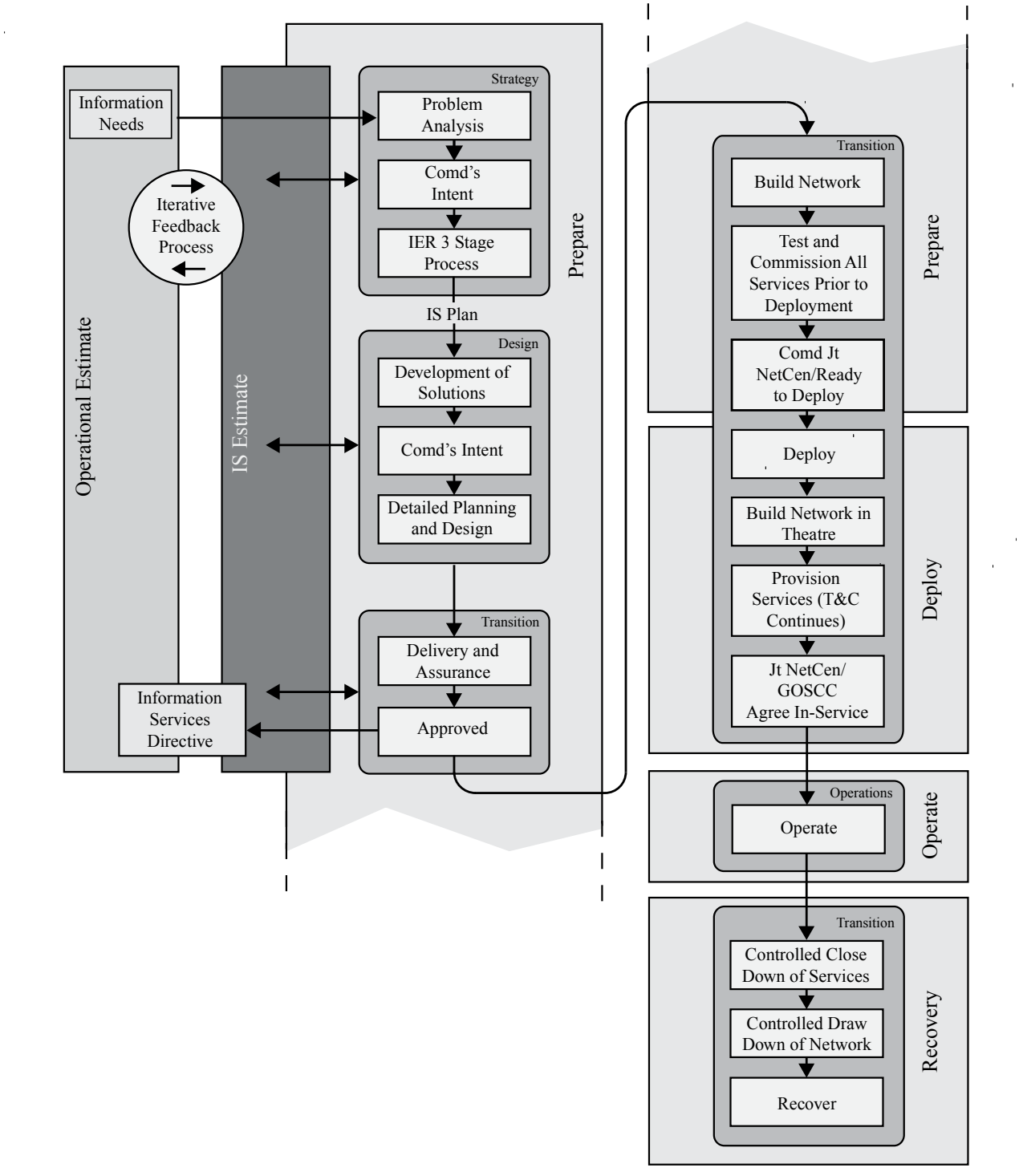


Figure 3.1 – Information Services Planning Process

311. The information services estimate informs the information exchange requirement[10] and is primed by the commander's statement of his information needs[11] and will be further developed by the staff.[12] The information exchange requirement 3-stage process, described in detail in Annex 3B, translates the commander's information needs (*Ends*) through the development of an appropriate architecture of core services and applications known as the information services requirement (*Ways*).[13] The information services requirement is then delivered by the communications service requirement (*means*).[14] The culmination of the planning process is the production of the CIS Directive which is the J6 annex within the JTFC Directive. Although this process may appear linear it is in fact iterative and subject to regular review. As understanding of the problem develops throughout the estimate the plan is further refined. Critically there is an explicit requirement to feedback the *art of the possible* to the JTFC, noting that information services can both enable *and* constrain.

312. The CIS Directive articulates the types and quantity of equipment that will be needed to deliver the required information services. The designed solution, when fully resourced, will meet the commander's information needs. These include, for example ISR dissemination and the reach of logistics services across extended lines of communication both within theatre, inter-theatre and back to the UK, while throughout continuing to enable effective C2. The final element of the *prepare* phase will be the testing and commissioning of the PJHQ J6 endorsed information services solution prior to deployment.

SECTION IV – PREPARE PHASE

313. Information services planning is an iterative process conducted continually throughout the operation. It is both harmonised with and integral to the J5 process to ensure that it reflects the status and progress of the overall planning effort. Consideration must be given to possible changes in scale of effort, posture, tempo, or main effort as the operation progresses. Potential resource and capacity limitations are also assessed and information services requirements prioritised in order to meet the commander's intent.

[10] The information exchange requirement addresses the JTFC's C4ISR requirements for the Joint Task Force, the interaction of components and agencies as well as tasks required to enact the Campaign plan.
[11] Output of Step 2a of the Operational Estimate.
[12] Output of Step 2b of the Operational Estimate.
[13] The information services requirement identifies the applications and core services (namely applications, e-mail, voice, and so on) to meet the Users' information needs.
[14] The communication services requirement identifies the network systems (for example trunk (FALCON), satellite (REACHER)) and infrastructure systems (for example DII (Future Deployed) and JPA) that deliver the applications and core services identified in the information services requirement.

Strategic Level Information Services Planning

314. The wider context for information services planning as part of Defence Crisis Management is described in JDP 01 *Campaigning* and JDP 5-00 *Campaign Planning*.

315. **CDS Directive**. Chief Information Officer-J6 Operations (CIO/J6-Ops), PJHQ J6 and DISS (as the Network Authority) contribute throughout the planning cycle to develop the information services element of the Chief of Defence Staff's (CDS) Directive. The information services element of the Directive, known as the CIS Annex, normally states the requirement for a Comd JFCIS although this role may be assigned to the senior J6[15] representative within the deployed lead headquarters if the scale of the task does not warrant a separate command appointment.[16] The CIS Annex gives broad direction on planning freedoms and constraints and the C2 relationships for strategic and high value CIS assets.

316. **Mission Directive**. The Joint Commander issues a Mission Directive to the JTFC, expanding upon the military strategic direction in CDS' Directive. The Joint Commander is responsible for: giving further direction and advising the JTFC as necessary; deploying, sustaining and recovering the force; and for monitoring and reporting the progress of the campaign to CDS. The Joint Commander's Mission Directive normally includes a CIS Directive as an annex to the main document.[17] PJHQ J6 staff usually form the core elements of the JFCIS staff early in the operational planning cycle to provide continuity throughout the operation.

Operational Level Information Services Planning

317. **Information Services Estimate**. The JTFC uses the Joint Commander's Mission Directive to prime his operational estimate, supported by the senior J6 representative[18] for the J6 elements. The information services estimate, shown at Annex 3A, is harmonised with the operational estimate and subject to regular review and feedback from the Joint Command Group. This allows the information services estimate to track the commander's guidance and direction to ensure that the solution supports the JTFC's plan. To ensure coherence, the deductions, tasks, commanders critical information requirements and requests for information identified by the commander during mission analysis, or by other staff branches during the operational estimate process, are considered by J6 in the information services estimate. In turn,

[15] For the purposes of this publication Comd JFCIS will be used to refer to the senior J6 representative deployed.
[16] Normally, the SO1 J6 post within the standing Joint Task Force Headquarters (JTFHQ) will routinely fulfil the role of Comd JFCIS for Disaster Relief Operations (DRO), Non-combatant Evacuation Operations (NEO) or during the early stages of a larger operation. Alternatively, the SO2 G6 within a Spearhead Lead Element (SLE) force elements may assume the role if the JTFHQ is not mobilised.
[17] Small scale tasks often do not require a separate information services Annex; therefore IS will be covered under a separate entry within the main body of the Mission Directive.
[18] If a Comd JFCIS is not deployed because the scale of the operation does not require one or the nominated Comd JFCIS is not available within the planning timelines; either SO1 J6 within the JTFHQ will subsume this role (if the JTFHQ is to be deployed) or ACOS J6 at PJHQ will retain the responsibility.

key deductions, tasks and risks developed in the information services estimate must feed the development of Courses of Action (CoA)s and the subsequent campaign plan to ensure that they properly reflect the information exchange requirement and specific information services considerations and limitations. This iterative process is the basis for the detailed design, delivery and assurance of the information services plan. The end product is promulgated in the J6 CIS Directive. The directive states how information services will be deployed and managed within the JOA.

318. Capability deficiencies, identified during the information services estimate, are addressed by CIO/J6-Ops, PJHQ or FLCs through the reallocation of assets or, alternatively, through the UOR process.[19]

Information Exchange Requirement

319. PJHQ J6, or Comd JFCIS, lead and co-ordinate the information exchange requirement process of transforming the commander's information needs into a co-ordinated and prioritised information services requirement by location, service, latency, quality of service, availability and level of assurance. DISS, the network authority, leads the design for the CIS solution, and is supported by the Jt NETCEN, or lead CIS support element.[20] In turn, PJHQ J6/Comd JFCIS approve the solution. The information exchange requirement process is collaborative, iterative and dynamic. It includes specialist contributions from the FLCs and DISS. At the earliest opportunity, DISS convenes and co-ordinates an internal planning team to support the operational planning process. The planning team ensures timely and coordinated engagement across DISS to prioritise and allocate resources for the operation.

320. The first and most important stage of the information exchange requirement process is the analysis of the commander's information needs to establish the requirements of all organisations that are supported by information services during the operation. The second stage, scaling analysis, derives the number of users for individual information services. The third stage is the production of the information service requirement and communications service requirement. The information services requirement identifies the capability to access and manipulate the information. When combined with the scaling requirements this starts to identify discrete capabilities. The communications service requirement provides a broad operational architecture and details how the network elements will be delivered to meet the commander's information needs. The information exchange requirement process is at Annex 3B and is the baseline from which the solution is designed, developed and delivered. The chosen solution balances the requirement for service

[19] In accordance with Defence urgent operational requirement procedures.

[20] If a Jt NETCEN is not deployed because the scale of the operation does not require one; either the Officer Commanding (OC) of the Signal Squadron deployed in support of the JTFHQ (if they are deployed), or OC of the Spearhead Lead Element (SLE) Signal Detachment or the Global Operations Security and Communications Centre (GOSCC) will subsume the responsibility. For the purposes of this publication, Jt NETCEN will be used to cover all these eventualities.

assurance and availability against acceptable cost, timescales for delivery and other risks.

Design, Delivery and Assurance

321. As the Network Authority, DISS leads the detailed design, delivery and service assurance of the information services solution. DISS is supported by the Jt NETCEN and other external stakeholders, such as: FLCs, Level 3 and 4 Support Organisations and other military and commercial service providers. The objective of this process is to deliver PJHQ with detailed planning guidance on the timeline and costs of service delivery options to develop potential solutions. These potential solutions, which also identify initial operating capability and full operating capability targets to support the commander's plan, are prioritised and endorsed by PJHQ J6/Comd JFCIS. Gap analysis, conducted by DISS and front line commands against the overall requirement, may identify capability shortfalls which are submitted as candidate urgent operational requirements in accordance with extant procedures. As the planning progresses, DISS's focus shifts towards the fulfilment and delivery of the end-to-end services to meet the information exchange requirement. DISS provides end-to-end assurance of service delivery for systems under the organisation's responsibility, including the coherence of delivery between service providers.

Implementation

322. Comd JFCIS sets out the tasks and timelines required to implement the information services solution. This includes dates for the achievement of initial operating capability and full operating capability for particular information services resources and detailing the priority services that will initially be required upon deployment. Comd JFCIS continuously reviews the progress of design, its implementation and any risks identified.

323. The CIS Directive, issued by Comd JFCIS, details the selected information services solution, the information exchange requirement, information services requirement, communication services requirement, freedoms and constraints and the associated Reports, Requests and Returns required from J6 formations across the JOA. It will also give the desired order of arrival. The CIS Directive is subject to configuration control and is regularly updated to ensure the information services solution continues to satisfy the operational requirement. The framework for the CIS Directive format is at Annex 3C and forms the J6 Annex to the JTFC Mission Directive.

SECTION V – CONSIDERATIONS

324. There are important planning considerations that complement the principles of CIS.[21] These considerations cover operational, technical and personnel factors. Additionally they inform the information services estimate.

325. **Command and Control**. C2 relationships between all deploying force elements should be defined early in the planning process, particularly in multinational or multi-agency operations, to fully capture the information needs of all participants. A UK force deploying on operations will often form part of a broader coalition and may be under the command of, or be in command of, other nations' forces. The status of the UK force as a contributory, lead or framework nation has significant impact on the scale and nature of national and coalition information services required. Therefore, the UK status within the coalition needs to be clearly articulated.[22] Planning should also consider any transition of capability provision to another nation as part of a *roulement* or redeployment.

326. **Security**. Two factors to consider are the ability of an opponent to disrupt friendly information services and the prevention of inadvertent disclosure of information. Operations Security (OPSEC) protects essential elements of friendly information against disclosure to an opponent. OPSEC is tailored to specific threats on individual operations and seeks to strike an appropriate balance between *need to know* and *duty to share* information.[23] Information Assurance (IA) considers protecting information and information services by ensuring their availability, integrity, authentication and confidentiality, and includes measures to ensure physical security. Information security covers technical security measures to protect information while in electronic form, and includes computer security, communications security and radiation security.[24] Details of specific considerations for the planning process are at Annex D.

327. **Warning Time**. Warning time influences the depth and scope of information services planning as well as force elements held at readiness. Short warning tends to limit the ability of industry to deliver urgent operational requirements or other capabilities. Contributions from FLCs may be limited to that held at extremely high readiness or very high readiness. Conversely, long lead times allow the development of in-depth solutions, with enhanced resilience, encompassing the broader application of commercial information services solutions.

328. **Concurrency**. Enduring or concurrent operations may limit the availability of information services, requiring economy of effort and prioritisation between

[21] See Chapter 1
[22] Permanent Joint Headquarters (PJHQ) J5 should provide detailed guidance on the status of any UK force.
[23] JDP 3-80.1, *OPSEC, Deception and PSYOPS*.
[24] Authoritative CIS Security Policy is detailed in Joint Service Publication (JSP) 440, *Defence Manual of Security*.

commitments. This may require strategic direction to either release additional resources or accept a constraint on the freedom of manoeuvre of the relevant commanders.

329. **Environmental Considerations**. Extremes of temperature, weather, terrain and adverse electromagnetic conditions have a detrimental effect on the availability, mobility, resilience and sustainability of information services equipment. The information services plan will consider the requirement for environmental protection and will balance the operational imperative against the demands of providing logistic support to equipment in remote locations. It will also consider any environmental limitations of the proposed equipments.[25]

330. **Force Protection**. A less permissive operational environment will constrain the freedom of movement of assets within the theatre. Force protection considerations therefore may impact the provision of information services plan. The use of remote sites to extend the range of terrestrial systems[26] represent a major challenge and will often require dedicated force protection, logistic and level 2 and 3 support.

331. **Host-Nation Support**. Information services planning must take account of the availability of host nation support across the JOA, as well as an understanding of the interfaces required with the host government and its agencies.[27] Analysis includes consideration of technical capabilities, the co-ordination of the Electromagnetic Spectrum (EMS) between participating nations, arrangements for network (including satellite communications) usage, and the potential use of other information services provided by other government departments, international organisations and non-governmental organisations.[28]

332. **Integrated Approach**. It is important that commanders at all levels are able to share information with non-military organisations. The information requirements of other government departments, non-governmental organisations and international organisations need to be captured as they are potential users of military information services. The subsequent information services plan should facilitate a layered or sectioned network to achieve interoperability within national and other government departments. Although constrained by security considerations, this approach is necessary to establish information flows across cultural divides, security gateways and other barriers.

[25] Equipment Programme (EP) funded equipment will be capable of working within adverse conditions.
[26] If these cannot be provided or guaranteed, the resulting network will be less resilient and robust, which subsequently leads to an increase in the number of personnel required to maintain the delivery of the CIS or the requirement for b*eyond line of sight* technology to be used at an increased cost to the operation.
[27] PJHQ J4 should be consulted at an early stage and throughout planning when considering host nation support issues.
[28] See Annex 2C for host nation support CIS matters; however, it should be noted that interoperability with outside organisations is currently limited.

333. **Sustaining Information Services**. To sustain information services an end-to-end approach should be used to quickly identify and rectify any failures. Considerations for Comd JFCIS during the *prepare* phase are:

a. **Level 3 Support Organisations**. Various military organisations, such as 15th Signal Regiment, 90 Signals Unit and the Fleet Information Services Support Unit (FISSU), can provide level 3 support to deployed information services. The size and composition of this deployed support will be identified in the estimate process having considered the following factors:

(1) The scale of the deployment.

(2) The diversity of systems and networks deployed.

(3) The information services environment (austere or rich).[29]

(4) The availability targets required by the JTFC for information services.

(5) The size of the JOA.

(6) Anticipated movement constraints in the JOA.

b. **Surge Personnel**. Surge personnel may be required to install information services during the deployment phase of the operation and provide specific additional support, such as upgrades, throughout the operation. Factors to be considered during the estimate include:

(1) Any constraints on manning levels in the JOA.

(2) The time required to generate and deploy a surge capability.

(3) Force protection and Contractor Support to Operations (CSO) management issues.

(4) Whether existing information services resources in the JOA, such as manpower from another component, could meet the requirement.

(5) Disposition of forward and rear-based personnel to support CIS capabilities linking the UK and the JOA.

[29] An austere information services environment (for example, limited in resilience and robustness due to force protection issues) will require a larger support envelope than a rich information services environment where sufficient resilience and robustness exists such that some loss of services can be tolerated.

c. **Logistic Support**. Comd JFCIS should consider logistic support to information services as part of his planning process; and ensure that it is co-ordinated with the Logistic Component staffs.

d. **Environmental Support**. Some Commercial Off-the-Shelf (COTS) products may not be designed for use in extreme environments and may be prone to degradation or failure due to temperature extremes, vibration, water and foreign particles ingress. COTS equipment may, therefore, require additional power as well as climatic, physical and electronic protection, which will be delivered and managed by the Theatre J4. If COTS equipment is needed a full understanding of the service management plan identifying how, and by whom, equipment will be supported is required.

e. **Contractor Support to Operations**. Contractor support to operations covers all forms of contractor support and encompasses: Contractors Deployed on Operations (CONDO); contractor logistic support, where in-service equipment is maintained under contract with the equipment provider; and the use of contractors through the PJHQ Contractor Logistic contract, where a range of services are provided from a long term commercial contract.[30] The increase of long-term partnerships with industry through Private Finance Initiative (PFI) to deliver military CIS capability has seen civilian staff become fully integrated into all layers of information services provision. It is necessary to be clear in advance on the status of contractors, including their status under military law, the impact of any Memoranda of Understanding (MOU) with a host nation (regarding their employment) and whether they are subject to a Status of Forces Agreement. Operational circumstances may preclude the use of contractor support to operations [31] and contractors may choose not to deploy their personnel into high threat or austere environments. In the CIS context, this risk is mitigated by the use of the long-term PFI partnerships that help to develop military-commercial relationships, and early engagement of contractors in the planning cycle. Nevertheless, should the local situation deteriorate to the point that contractor support to operations no longer wish to remain in the JOA, contingencies should be developed to address their potential withdrawal of service delivery. This is a significant planning constraint and one that requires capturing and investigating early to ensure the risk is articulated to the JTFC and mitigation sought.

334. **Interoperability**. Interoperability provides connectivity across applications, core services, infrastructure and networks to enable multinational and multi-agency partners, components and force elements to share information. A degree of

[30] As operations reach 'steady-state', early consideration should be given to recovering critical, high-readiness military assets and replacing them with CSO assets where appropriate. PJHQ J6 is responsible for managing commercial solution implementation.
[31] MOD use of CSO is articulated in JSP 567 *Contractors on Deployed Operations.*

interoperability with partners will have been included in the initial equipment programme requirement although this may not provide a complete solution for a specific operation. Therefore Comd JFCIS, PJHQ J6 or DISS must consider the interoperability standards required during the planning process. Specifically the planning process must consider: applications and databases and their associated data standards; agreed technical protocols, configuration control, gateway management, service management procedures, security and national caveats and common standard operating procedures. Often a less capable solution that is interoperable with partners is preferable to a more capable UK only solution. If a technical solution is not available then information management and staff processes will need to be developed to mitigate the risk.

335. **Battlespace Spectrum Management**. Battlespace Spectrum Management is essential to enable optimal use of the EMS; this includes consideration of deconfliction, protection, exploitation and denial. There are many competing demands on the EMS and considerable risk of *electronic fratricide*,[32] which could lead to loss of situational awareness or severely impact the commander's ability to conduct the operation by a denial of service. The Battlespace Spectrum Management process is detailed at Annex 3E.

336. **Personnel**. Greater connectivity and the multinational and multi-agency nature of the contemporary operations have increased the risk of information overload.[33] It is essential to ensure that information management is driven by the staff with a full understanding of the operational requirements for information exploitation whatever their discipline. Staff selected to fulfil critical information services roles should have the knowledge and experience to advise on the capabilities and limitations of the CIS, information management, and information exploitation and information superiority. Early identification of personnel to fill these roles presents the best opportunity for induction, refresher, or technical update training. The need for additional training increases significantly where a high percentage of the information services plan is new or theatre specific.

[32] Potential interference in the EMS that could impact radar, telemetry, Unmanned Aerial Systems (UAS) and radio frequency capabilities.
[33] Annex 1A provides a detailed insight into how Information Management (IM) is used to determine the information needs and outputs of an operation.

ANNEX 3A – INFORMATION SERVICES ESTIMATE

OP NAME

File Reference: Date:

References:

A. JDP 5-00 *Joint Operations Planning.*
B. JDP 6-00 *Delivering Information Services to Enable Joint Operations*.
C. Operational Estimate and Directives.

Time Zone Used Throughout Estimate:

MISSION ANALYSIS

MISSION: (from Jt Comd's Directive)
(When known, JTFC Planning Guidance, outline Concept of Operations and Main Effort can be included here.)

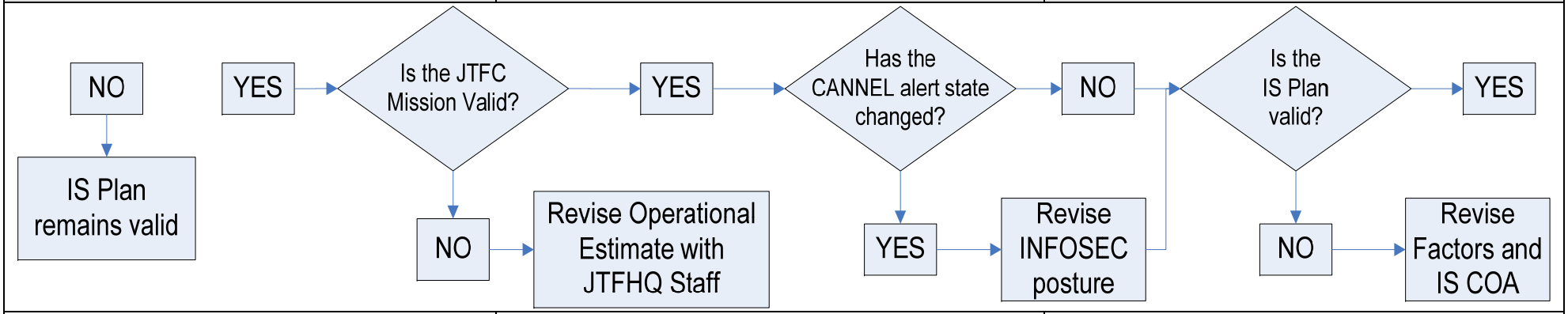
(The text included in the Considerations/Deductions and Tasks/Constraints is included for guidance purposes only)

Factor	Deduction	Output
1. **Intention of Superior Commander**. a. Joint Commander (Jt Comd) intention is to…. b. Joint Task Force Commander (JTFC) intention is to….	It is important that the information services Estimate examines the output of the Operational Estimate.	

Factor	Deduction	Output
c. Deductions, tasks and constraints from Operational Estimate.		
2. **Tasks**. a. **Specified**. b. **Implied**.	Tasks will be specified in the commander's statement of his information needs. Specified and implied tasks will be derived from the Jt Comd Directive as part of the Operational Estimate. Consider also known tasks from Joint Planning Guide (JPG)/Joint Contingency Plan (JCP) and doctrine (JDP) or Standard Operating Procedure (SOP). Test the completeness of the requirements set by running a set of standard mission threads against the CONOPS, using the intended C2 structure, ORBAT and scheme of manoeuvre to identify the totality of information flows required across the battlespace (and back into the business space where applicable).	**Remember**: 1. Force Command and Control (C2) – Joint Task Force Headquarters (JTFHQ), C2 Structure, coalition partners, allies. 2. Joint (and Coalition) activities. 3. Co-ordination and interoperability with allies. 4. The principles of CIS planning. **All tasks must be considered and information services issues identified.** **Information services issues not for JTFHQ must be briefed to components**. **JTFC Main Effort must be reflected in** information services **Main Effort**.
3. **Constraints**.	Detail on constraints will be derived as part of the Operational Estimate. Consider also constraints already identified in JPG/JCP and doctrine (JDP) or SOP.	
a. **Time**.		**Disseminate** information services **planning timeline**.
(1) Time available for planning.	Long lead times may be required if there is a requirement to generate commercial information	**Include Op Timeline and deductions in Warning Order to Permanent Joint**

Factor	Deduction	Output
	services.	**Headquarters (PJHQ) & Commands CIS Staff**.
(2) Operation timelines.	Consider implications for PJHQ, Commands & Units. Remember 1/3, 2/3 Rule (1/3 time to conduct your planning – 2/3 time to conduct their planning).	Constraints relating to: - JTFHQ & Force deployment. - Operation Phases & Activities. - Recovery or Relief.
b. **Space**.		
(1) JOA (size and location).		
(2) Jt force elements locations.	How does the Joint Operations Area (JOA) and the lines of communication (loc) of the deployed force constrain or influence the information services CONOPS? Consider JTFHQ/National Contingent Commander (NCC), Component HQs, Joint Force Elements (JFEs), National Support Element (NSE), Forward Mounting Base (FMB), Airport of Disembarkation (APOD), Seaport of Disembarkation (SPOD), Deployment Operation Base (DOB), etc.	
c. **INFORMATION SERVICES Resources**.	Are there requirements for data separation, closed user groups, compartmented information, etc.? Will some users require additional resources to meet these requirements?	

Factor	Deduction	Output
(1) UK information services.	How does concurrent deployment, UK infrastructure and information services equipment availability constrain this operation? What is the appropriate degree of resilience required to meet the Comd's intent?	
(2) Allied information services.	What part do allies play? How may this constrain the information services Course of Action (CoA)? What are the responsibilities for communication between higher and lower headquarters?	
(3) Host Nation (HN) information services.	What is Global System for Mobile communications (GSM) coverage?	
(4) Other agencies.		
d. **ROE**.	How do the Rules of Engagement (ROE) affect the use of the spectrum in the JOA?	
e. **CANNEL Alert State**.	What additional steps will be required to reach the desired Information Security posture?	
4. **Has the Operational Environment Changed?** (Since the Jt Comd's Directive was received or the estimate completed.)		

Factor	Deduction	Output
		
5. **Commander's Direction**.		
a. **JTFC Planning Guidance**.	What planning guidance must be passed to PJHQ J6 & Components at this stage?	**Complete Warning Order to PJHQ and Front Line Commands (FLCs)**.
b. **CCIR/RFI**.	Are there information services related Commander's Critical Information Requirements (CCIR)/ Requests for information (RFI)? What CCIR/RFI will impact on the information services CoA and how? What are the J6 RFI?	**Ensure information services related CCIRs and RFI are addressed**.
c. **Clarification**.	What issues requiring clarification will impact upon the information services CoA? How?	

EVALUATION OF FACTORS

Factor	Deduction	Output
6. **Environment**.		
a. **Terrain**.	How will terrain features affect wireless (Local Area Network) LAN and other radio transmissions?	
b. **Weather**.	How will prevalent and expected weather conditions affect wireless LAN and other radio transmissions? What environmental protection will equipment need (for example, air conditioning, radomes, dust protection)?	
c. **National Culture**.	What aspects of National culture within the JOA impact on use of information services with allies and the host nation? Consider language requirements.	
d. **National information services within JOA**.	Refer to host nation Joint Tactical Procedure (JTP) for initial data on host nation information services ifrastructure.	
e. **Spectrum Utilistion**.	Determine the current usage of the spectrum in the JOA..	**Generate RFI – What is the usage of the spectrum in the JOA?**
7. **Adversary Forces**.	How do adversaries' CoAs affect the information services plan? What is the threat to maritime, land–based and air information services from adversary physical attacks?	**Task J2 to provide a specific electronic threat assessment**.

Factor	Deduction	Output
	Does threat preclude use of contractor support to operations (CSO)?	
a. **Physical Threat**.		
b. **Electronic Threat**.	What ability does the enemy have to intercept, monitor or interfere with friendly transmissions?	
c. **Cyber Threat**.	What ability does the enemy have to conduct a cyber attack on deployed networks and systems?	
d. **CBRN**.		
8. **Friendly Forces**.		**Confirm Force C2**.
a. **UK Joint Force**. (JTFHQ, Mar, Land, Air, Special Forces (SF), Logistics (Log).	Consideration must be given to inter-component co-ordination staff.	**Remember**: 1. Force C2 ((Combined (C)) JTFHQ, C2 Structure, coalition partners, allies). 2. Joint (and Coalition) activities. 3. Co-ordination & interoperability with Allies.
b. **Coalition**. (Lead Nation, information services Framework Nation, UK NCC, UK NSE, UK MAR/LAND/AIR/SF/Log).		
c. **Allies**.		
d. **International, National and Non-Governmental Organisations**.	Consideration should be given to the use of information services by such agencies as well as the need for communications to and from them. What is the minimum security level for each facility?	

Factor	Deduction	Output
e. **SIGINT and Electronic Warfare**.	How will SIGINT and electronic warfare impact on the information services plan? Are there information services requirements for co-ordination with J3 Operations Support?	
f. **Inter-agency**.		
g. **Welfare**.		**Provide advice to J1 on Welfare information services**.
h. **Spectrum Management**.	What are the spectrum management requirements?	**Define spectrum requirement for deployment**. **Identify available spectrum within the JOA**. **Identify spectrum clearance procedures**. Determine Joint Force spectrum management plan.
i. **Logistics**.		
(1) Sustainability.	Consider the disposition of spares, supply lines and support elements.	
(2) Critical information services.	Consider the disposition of mission-critical spares.	
j. **Movement and requirement for asset tracking**.	Who, what, where to and when?	
(1) Strategic Movement.		

Factor	Deduction	Output
(a) Availability of assets.		**Ensure information services is reflected on the Desired Order of arrival Staff Table (DOAST)**.
(b) Desired Order of Arrival (DOA).		
(c) Import restrictions.		
(2) Intra-Theatre Movement.	The need to manoeuvre may dictate the static/transportable/mobile options available in a commercial solution.	
(a) Availability of assets.		
(b) Import restrictions.		
(c) Extra time for road/air transport.		
k. **Force Protection**.		
9. **Information Operations**.		
a. **Security – Protecting UK Information and Network Infrastructure**.		
(1) Electronic protection measures.	In addition to considering the enemy threat, consider issues relating to working alongside coalition partners and allies. How will UK information be protected whilst also protecting coalition information?	

Factor	Deduction	Output
	What aspects of the Information Operations (Info Ops) plan impact on Joint Force information services?	
(2) Physical security.		**Wireless LANs introduce additional challenges**.
(3) Crypto protection.	What gateways to other nations' Crypto may be required?	**Determine crypto plan, including responsibility for distribution of both materiel and regular KEYMAT updates across the JOA**.
(4) EMCON.		
(5) Information Security.	Does the JTF require a Force INFOSEC Team (FIT)? Is there a need for a deployed Monitoring and Reporting Centre (MRC)? Is there a need for Computer Incident Response?	A FIT would normally be deployed if the JTFHQ were deployed and would work alongside the deployed Computer Network Defence (CND) effort, based in the NETCEN for Comd JFCIS.
(6) Co-ordinating Installation Design authority (CIDA) Requirements.		
(7) Personnel Security.	Will security access for foreign nationals be required?	
b. **Deception**.		

Factor	Deduction	Output
10. **Time**.	Identification of fixed or proposed times for the deployment of Force Elements, establishment of HQs and the development of Op phases across the JOA, including any subsequent needs to commercialise. How should the information services deployment be phased?	**Op timelines must be reflected in information services CoA**.
11. **Pre-deployment information services preparation and training**.	What is the impact of pre-deployment information services preparation and training on CoA?	**Any requirement for pre-deployment preparation and training must be reflected in the Assessment of Tasks, the information services CoA and the information services CONOPS**.
12. **C2 of information services**.	What augmentation of the JTFHQ J6 or JFCIS/Jt NETCEN staff is required? What Level 3 Support provision is required?	**Determine C2 arrangements for Joint, operational level information services, including relationship with ISS/GOSCC**.
a. **Command and control arrangements**.		
b. **Information services staff**.		
c. Specify freedoms and constraints.		
13. **Information management**.	What impact will the Joint Information Management Plan have on information services CoA?	
a. **JTFHQ**.		
b. **Components**.		

Factor	Deduction	Output
c. **Coalition Partners & Allies**.		
d. **Host Nation**.		
e. **International Organisations (IOs)/ Non-Governmental Organisations (NGOs)**.		

14. **Summary of Possible Tasks**.

All tasks should be identified as essential or optional. In addition, it may be helpful to prioritise essential tasks.

Task	**Resources / Comment**	**Task**	**Resources / Comment**
Identify Tasks by: Task, Staff Check, Clarification, RFI.			

CONSIDERATION OF INFORMATION SERVICES COURSES OF ACTION

Factor	Deduction	Output
15. **List all CoAs from the operational estimate**.	**List all possible information services CoAs to satisfy each CoA**.	**Consider advantages and disadvantages of each CoA**. Backbrief J3/J5 on any information services CoA that impacts adversely on CoA in Operational Estimate.
What tasks, advantages or disadvantage are common to all information services CoAs?		
16. **Selection of CoA**. **This can only be done when the JTFC has made his decision as to the CoA for the JTF**. **An outline information services CONOPS, including Main Effort, is produced now**.		

STANDARD REQUEST FOR INFORMATION

On most operations many of the questions generated by the information services Estimate are routine. Nevertheless they must be answered in order to inform the planning process. It may be useful to produce these RFI early in the planning process and refine them later.

The J6 officer on an Operation Liaison and Reconnaissance (OLRT) or advance party could answer many of them.

Ser	RFI Area	Considerations
1.	**Electromagnetic Environment**	What limitations - physical or financial - are there on the JTF's use of the Electromagnetic Spectrum (EMS) across the JOA? Who and where is the local spectrum management authority? What extant agreements exist for our use of the spectrum?
2.	**Enemy Forces**	What are the SIGINT capabilities of the adversary? What are the EW capabilities of the adversary? What are the Computer Network Attack (CAN), Computer Network Exploitation (CNE) and CND capabilities of the enemy? Request information services vulnerability report on own forces to match with the threat above.
3.	**Allies**	What coalition information services will be used within the Force? What military information services or support, including EW and SIGINT, can the HN provide? What information services or support, including EW and SIGINT, can allies provide? Confirm understanding/acceptance higher-to-lower principle coalition-wide.

Ser	RFI Area	Considerations
4.	**Other Agencies**	What information services do OGDs (including British Missions), NGOs and IOs have in the JOA?
5.	**Security**	Is a Force INFOSEC Team (FIT) survey required, and, if so, what capabilities will they need? Request deployed CND capability commensurate with information services vulnerability report. What are the accreditation requirements for the desired equipment? Does the JTF require a Theatre Cryptographic Distribution Agency? Is there suitable crypto available for coalition use?
6.	**Host nation information services**	What is the SATCOM footprint for all likely friendly military and civil satellites to be used (SKYNET, INMARSAT etc)? What cellular phone coverage is there in the JOA? How reliable are the cellular networks? What cellular protocols are used in the JOA (that is, GSM, DAMPS, analogue, WAP, GPRS, 3G) and in what band? Who are the main suppliers of cellular services in the JOA? Are cellular handsets readily available, what is the cost to hire and who are the best local suppliers? How is the local telephone network provided and controlled? What is the HN telephone socket format? Who is our point of contact for local telephone network service provision? Who are the main suppliers of PTT services in the JOA? How reliable is the local telephone network? What are the local telephone network call response times (International)?

Ser	RFI Area	Considerations
	Host nation information services (continued)	What are the local telephone network call charges (international and local)? What are the local telephone network engineering response times? Is ISDN available and if so what type of ISDN protocols are used? How are international trunks accessed, is it direct (IDD) or through an exchange? What Local Internet Service Providers (ISPs) are available and are they reliable? Which major International ISPs (CompuServe/AOL, etc..) are available? What are the host nation domestic electrical power standards and normal wall socket and plug formats? What are the host nation frequency clearance procedures? Do any MOUs or other agreements exist for SATCOM access? Are there any bandwidth limitations/special baseband requirements? Are there any local microwave interference issues?

ANNEX 3B – INFORMATION EXCHANGE REQUIREMENT

SECTION I – INTRODUCTION

3B1. The information exchange requirement translates the commander's information needs (*ends*) through the development of an appropriate architecture of core services and applications known as the information services requirement (*ways*). This provides the foundation for developing the network design that is articulated in the communications service requirement (*means*). This process, supported by the output from the information services estimate, develops the detail required by information services staff to provide robust and capable operational capability throughout all phases of the campaign. To ensure maximum flexibility with limited capability and within resources, the JTFC and his staff should articulate their information needs rather than the process or systems they may already be familiar with.

SECTION II – 3-STAGE INFORMATION EXCHANGE REQUIREMENT PROCESS

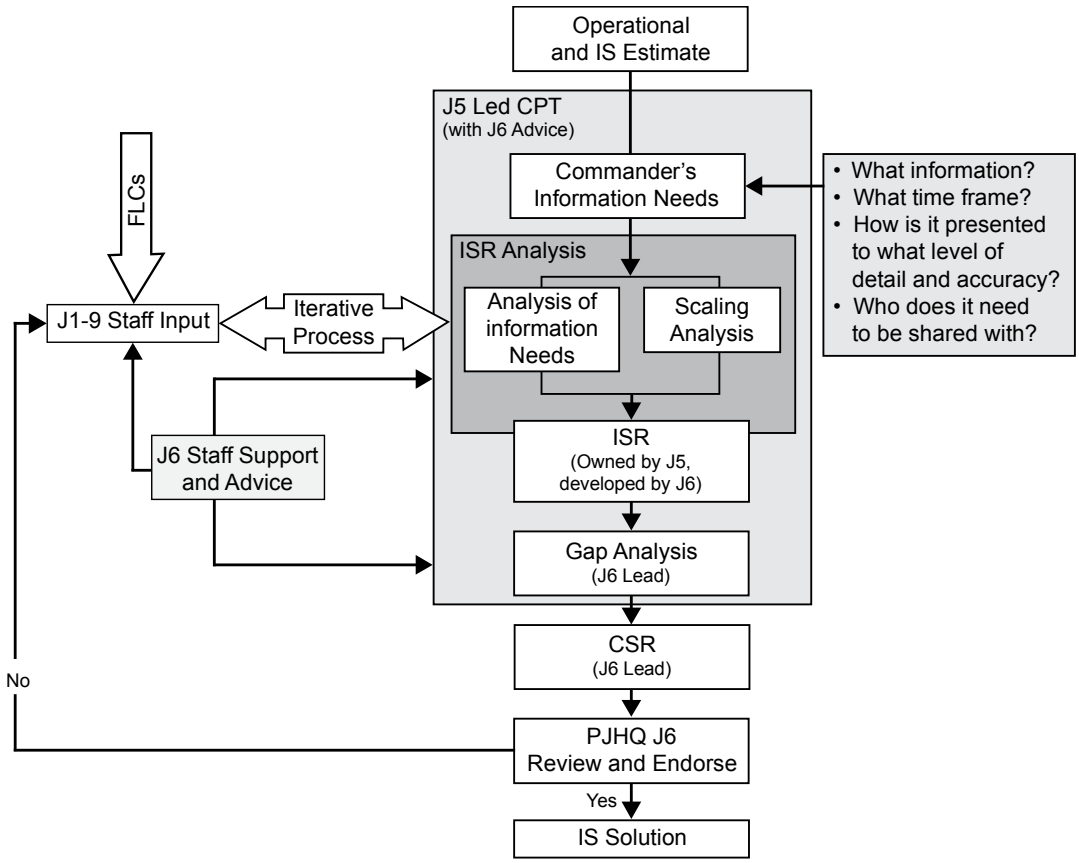


Figure 3B.1 – Information Exchange Requirement Process

3B2. The 3-Stage information exchange requirement process ensures that all staff branches contribute the necessary information at the appropriate time, as shown in Figure 3B.1.[1]

3B3. **Analysis of Information Needs**. The analysis of the information needs is the first and most important stage of the information exchange requirement process and aims to identify the ways of working required between the organisations supporting an operation. This requires the identification of: what information the commander needs, in what timeframe (real-time, near real-time or higher latency); how is it presented, to what level of depth or detail, how accurate does it need it to be; and who does it need to be shared with (multinational, host nation, other governmental departments and so on)? This analysis defines the transfer and sharing of information between staff branches within the JTFHQ and components, including special forces, headquarters and other formations both inside and outside the JOA. It should include other government departments, coalition partners, international organisations and non-governmental organisations. While many of the commander's information needs can be explicitly drawn out of his statement of information needs as well as the operational and information services estimate, others may be implied or not immediately identifiable. The analysis provides the foundation for developing the required architecture and eventual network design, and constitutes the rationale for all information services requirements. J1-9 staffs must provide the underpinning information required for the analysis with J6 staff providing support and advice as required.

3B4. **Scaling Analysis**. Scaling Analysis is the second stage in the information exchange requirement process. It details the number of personnel associated with each formation and how many of them require concurrent access, grouped against generic information services. Again, staff branches must provide the appropriate information, with the support of J6/JFCIS staff.

3B5. **Components**. Component commands conduct their own analysis and ensure that the resulting information exchange requirement for their information services is incorporated in a timely manner into the overall campaign information exchange requirement and is passed through their front line commands into the J5-led contingency planning team.

3B6. **Production of the Information Services Requirement and Communications Services Requirement**. Production of the information services requirement is the stage at which J6 staff combines the data captured within the analysis of information needs and the scaling analysis, and apply their technical expertise and experience to develop the information services architecture. This process must take into account any resource constraints such as availability of network

[1] Further detail may be found in Commander Joint Force CIS Standing Operating Instructions.

and infrastructure equipment. Any gaps in capability can then be fed back to the commander to prioritise his information needs or request that additional capability is provided; often this is will require a urgent operational requirement process. Representative examples of a completed information services requirement and communication services requirement are at Appendices 3B1 and 3B2 respectively.

(INTENTIONALLY BLANK)

APPENDIX 3B1 – EXAMPLE INFORMATION SERVICES REQUIREMENT

Ser	Area	Class	Core Services							Application Services				Loc A	Loc B	Loc C	Loc D	Remarks
			Voice	Email	Web	Publish	Collate	Office Extras	VTC	HR	C2	SA	ISR					
1	JTFH QJ1	U	-	20	20	5	-	-	-	Y	N	N	N	UK	-	-	-	
2	JTFH QJ1	R	-	20	20	10	20	Visio, Project	-	Y	N	Y	N	CC	UK	NATO HQ	APOD	
3	JTFH QJ1	SUKEO	5	5	5	5	5	Project	10	N	Y	Y	N	CC	UK	-	APOD	
4	JTFH QJ1	MS	20	20	20	20	20	-	10	Y	Y	Y	N	CC	UK	NATO HQ	-	
5	JTFH QJ2	U	-	-	5	-	5	-	-									
6	JTFH QJ2	R	-	10	10	-	5	-	-									
7	JTFH QJ2	SUKEO	10	10	10	10	10	Access, Visio, Project	5									
8	JTFH QJ2	MS	10	10	10	10	10	Access, Visio, Project	5									
9	JTFH QJ2	TS	5	5	5	5	5	Access	2									

Figure 3B1.1 – Example of the Information Services Requirement

3B1.1. **Information Services Requirement Completion**. The information needs of all deploying personnel must be collated and translated into capabilities in order to enable J6 to deliver an appropriate solution. The naming of specific systems must be avoided to enable the delivery of a coherent and supportable network to enable information services. To assist with developing this information, the framework offered in the table shown at Figure 3B1.1 should be used. The table should be amended for each location and each operation. It is divided into the following components:

a. **Area**. The group name of the working area, i.e. J1 within the JTFHQ or A1 within the Air Component Headquarters.

b. **Classification**. The classification that the users predominately require to work on. The normal choices will be *unclassified, restricted, secret UK eyes only*, *mission secret*[1] *and top secret*. Other classifications can be added, such as *US/UK Eyes Only, NATO Secret*, etc.

c. **Core Services**.[2] These are the core tools that users will require on a daily basis that will be delivered on every operation. The number represents how many users, by each area, require access.

d. **Application Services**. This area captures the generic application set that the user will require access to. For example, Human Resources (HR) will result in delivery of the most appropriate HR application, not necessarily a specific one. This information enables J6 to deliver the CIS that can meet the operational requirement, while maintaining the integrity of the system, delivering services with in-built resilience and reducing pre-deployment training overheads. The cells should be completed with either *yes* (Y) or *no* (N) to identify each area's access requirements.

e. **Locations**. The location boxes will enable J6 to identify who the users need to communicate with most and how best to enable those services. The locations should be broken down by order of priority, for example component commands may be their highest priority, then UK, then NATO headquarters, etc.

3B1.2. J6 staff will advise and support all staff branches during completion of the information services requirement, to ensure all users' information needs have been captured and accurately articulated. Upon completion, the information services requirement will form the basis of identifying any gaps in capability, which could result in urgent operational requirement action, and used to develop the communications services requirement which is covered in detail at Appendix 3B2.

[1] Generic term to identify a coalition system specifically designed for the operation.
[2] Services those are normally available through the appropriate service catalogue.

APPENDIX 3B2 – EXAMPLE COMMUNICATIONS SERVICES REQUIREMENT

JTFHQ Communications Services Requirement

Service	Classification	Preferred Solution	Users	Throughput/ Traffic Profiles	Intra/Inter Theatre	Comments
DATA						
Internet	Unclass	PJHQ.COM	10	RLI tunnelled – 128k	Inter	
Log IS	Restricted	HOUSEKEEPER	30	RLI – 512k	Inter and Intra	
C2	SUKEO	DII/FD	50	SLI – 512k	Inter and Intra	
C2	Mission Secret	OVERTASK	150	Blue – 2M	Intra	
ISR	Top Secret Strap 1	LABYRINTH	20	RLI – 2M	Inter and Intra	
VTC	UKEO	xxxxx	40	SLI – 512k	Inter and Intra	
VOICE						
UK	SUKEO	FALCON	150	SLI – 128k	Inter and Intra	
UK	Top Secret	BRENT	20	RLI – 128k	Inter and Intra	
Coalition	Mission Secret	VOIP	150	Blue – 128k	Intra	
MESSAGING						
FAX	SUKEO	xxxxx	5	SLI – 128k	Inter	
FORMAL	Top Secret Strap 1	xxxxx	2	SLI – 128k	Inter and Intra	
APPLICATIONS						
HR	Restricted	JPA	20	-	Inter and Intra	
HR	Mission Secret	NATO Admin	20	-	Intra	
SA	SUKEO	JOP	150	-	Inter and Intra	
C2	Mission Secret	JADOCS	50	-	Intra	

Figure 3B2.1 – Template of the Communications Services Requirement

3B2.1. **Communications Services Requirement Completion**. Using the information services requirement completed in accordance with Appendix 3B1, J6 staff will identify how the information services will be delivered. Figure 3B2.1 to this Appendix is used to capture the common requirements and will identify the broad order bandwidth requirements. Much of this work will use pre-defined information to assist with the capture.

3B2.2. Following completion of the communication services requirement it will be released to DISS and the front line commands to derive the plans for the delivery of the information services solution. The use of the preferred solution will enable the delivery team to better understand what system could meet the user's information needs; however, it may not be feasible to deliver that particular element for a variety of reasons.

ANNEX 3C – COMMUNICATIONS AND INFORMATION SERVICES DIRECTIVE

Issuing Headquarters:
Place of issue:
Date/Time Group of Signature: XXXXXXZ MMM YY

File Reference:

INFORMATION SERVICES DIRECTIVE
OP [****]

References: *[Add references as required, for example a Joint Task Force Commander's (JTFC's) Campaign Directive and other instructions should be included and referred to in the detail of the document.]*

Time Zone Used Throughout the Order: XXXX

Other time zones in which elements of the Force are located should also be detailed.

SITUATION

[Taken from the JTFC's Campaign Directive or equivalent documentation.]

1. **Situation**. *[Detail as required to set the context for CIS staff required to satisfy the IXR.]*

2. **Mission**. The Joint Task Force (JTF) is to…*[a clear, concise statement of the task of the command and its purpose]*.

a. **Commander's Intent**. My Intent is ... *[This should focus on the overall effect the JTF is to have and the desired situation it will bring about. It should be a concise and precise statement of what the JTFC intends to do and why, and should not be a synopsis of the operation. In effect it provides the enduring logic behind the whole Campaign Plan.]*

b. **Scheme of Manoeuvre**. *[This should describe how the JTFC sees the Campaign Plan unfolding. The JTFC should explain where, when and how the JTF will achieve its purpose, so that subordinates can understand what their particular role is in the overall plan and the effects they are to achieve.]*

c. **Main Effort**. *[Main Effort is the concentration of forces or effect, in a particular area, in order to bring about a decision. It is the principal method by*

which a JTFC makes his overall intent clear to his subordinates and will usually be supported by the allocation of resources in order to give substance to that which he considers crucial to the success of his mission.]

3. **JTF C2**. Annex A.

4. **JTF Liaison Matrix**. Annex B.

5. **Task Organisation**. Annex C.

a. **Attachments**. Describe which units will be attached from where, for what purpose, and to be effective from what date/time.

b. **Detachments**. Describe which units will be detached to where, for what purpose, and to be effective from what date/time.

INFORMATION SERVICES

6. **Information Exchange Requirement**. Annex D.[1]

7. **Threat to CIS**. A clear articulation of the threat to CIS in the JOA is essential from the outset to ensure that all the security factors are considered, safeguards established and information appropriately assured. The threat statement includes the opponent's ISTAR threat (for example, SIGINT) and Cyber Threat within the JOA and globally as it applies to the operation.

JFCIS MISSION

8. A succinct statement of Comd JFCIS' Mission. For example, *to provide Communication and Information Services within the JOA in order to enable the JTF to set the conditions for…*

EXECUTION

END-STATE

9.

[1] Described in Annex 3B to this publication.

INFORMATION SERVICES CONCEPT OF OPS

10. **Intent**.

11. **SoM**.

12. **Main Effort**.

13. **Role of Jt NETCEN**. The Jt NETCEN is to determine and maintain configuration control of the operational network and systems required to meet the IXR under the direction of Comd JFCIS. Jt NETCEN is the nominated engineering and configuration authority for the deployed network and associated systems.

FREEDOMS AND CONSTRAINTS

14. Comd JFCIS is delegated OPCON of all information services within the JOA, with the exception of the following (for example *SF CIS*[2] *and SATCOM*[3]), to support the JTFC's Intent and Main Effort. To achieve this, Comd JFCIS directs the disposition and usage of CIS within the JTF, regardless of origin or ownership.

15. **Key Principle**. Where constraints have not been specified by the Network Operating Authority or PJHQ, Comd JFCIS allows components the freedom to configure and operate information services to support local Comds, but this only applies to capability which is not part of a wider network or Joint Force C2 integration.

16. **Specific Constraints**.

JOA CIS LAYDOWN

17. **Core Information Services Architecture**. Annex E.

18. **Operational-level Information Services**.

19. **Tactical Networks**.

    a. Secure and Insecure Voice.

    b. Formal Messaging and Secure Facsimile.

---

[2] The reallocation of SF CIS requires Director SF approval.
[3] Strategic satellite communications (SATCOM) capability remains OPCOM with CIO/J6-Ops and CJO retains OPCON. It cannot be delegated.

20. **Satellite Communications**.

21. **Radio Networks**.

    a. Point-to-point service.

    b. Radio Automatic Tele-Type (RATT).

    c. Air-to-ground.

    d. Shore-ship.

    e. Ship-ship.

    f. Air Traffic control.

22. **Tactical Data Links**.

23. **Coalition Information Services**.

24. **Host Nation Services**.

25. **Inter Agency Information Services**.

26. **Special Information Services**.

27. **Service Delivery**. Annex F.

JOINT (AND MULTINATIONAL) INTEROPERABILITY

28. This section covers both Joint and multinational interoperability of systems and services at all levels of command (Strategic, Operational and Tactical). A detailed Interoperability Matrix is included at Annex G.

TASKS

29. **Jt NETCEN**.

30. **JTFHQ**.

31. **All Component Commands**. *To remove repetition, tasks that apply equally to all CCs should be described here.*

32. **MCC**.

33. **LCC**.

34. **ACC**.

35. **JFLogCC**.

36. **Joint Force Support**.

37. **To include CIS supporting and supported commanders**.

CO-ORDINATING INSTRUCTIONS

38. **Timings**.

39. **Risks**. Annex H.

40. **Restoration Priorities**. Annex I.

41. **Battlespace Spectrum Management Plan**.

42. **INFOSEC Measures (such as CND) and information services Security**.

43. **Personal Equipment and HN CIS usage policy**.

44. **Engineering Recovery Plan**. Annex J.

45. **Formal Messaging Plan**. Annex K.

SUSTAINABILITY PLAN

46. **Sustainment Concept**.

47. **Level 3 Support**.

48. **Critical Spares**.

49. **Commercialisation (ISS Plans) and Enabling Works**.

50. **CSO**.

MISSION ESSENTIAL AND CRITICAL EQUIPMENT

51. Identify equipment (Annex L) that is fundamental to the successful achievement of a mission (*Mission Essential*) and equipment that, if lost, would cause the loss of mission-essential capability (*Mission Critical*). Detail how such equipment is to be allocated and controlled.

COMMAND AND SIGNAL

52. **Appointments and Locations**.

53. **Alternative Comd/Headquarters**.

54. **Information Services R2**.

55. **Information Services Liaison**.

56. **EMCON**.

Ack: Authenticate:

NAME
Rank
JTFC

NAME
Rank
Comd JFCIS

Annexes:

A. JTF C2.
B. JTF Liaison Matrix.
C. Task Organisation.
D. IXR.
E. Core Information Services Architecture.
F. Services Delivery Plan.
G. Interoperability Matrix.
H. JFCIS Risks.
I. Restoration Priorities.
J. Engineering Recovery Plan.
K. Formal Messaging Plan.
L. Jt Mission Essential and Critical Equipment.

Distribution:

JFMCC
JFLCC
JFACC
JFLogCC

AmphibFor
11 Sig Bde
90 SU
J3 Ops Sp
Jt NETCEN
JFEngr

Copy to:

CIO/J6-Ops
PJHQ
JTFHQ
FLCs (via PJHQ)
HQ DSF
ISS

(INTENTIONALLY BLANK)

ANNEX 3D – SECURITY AND INFORMATION GOVERNANCE

3D1. Authoritative Communications and Information Services (CIS) Security Policy is detailed in Joint Service Publication (JSP) 440, *Defence Manual of Security*. This Annex sets out the high-level approach to security and its application to the governance of CIS capability. It is a guide to the factors considered on operations. This Annex describes constituent elements of information governance, particularly those within the scope of Information Assurance (IA) and how they relate to equipment and services so that appropriate measures may be taken before, during and after an operation. IA is a contributor to Operations Security (OPSEC)[1] and hence to force protection.

SECTION I – SECURITY CONSIDERATIONS

3D2. **Security**. Information services are of little use to a commander if they compromised or delayed. The threat to information services, articulated in Comd JFCIS CIS Directive, defines the appropriate security requirements.

3D3. **Aggregation of Information**. Throughout an operation, there is a risk of an opponent intercepting seemingly unimportant pieces of information which, when aggregated, lead to the deduction of important intelligence about friendly operations. Therefore, the timely accreditation[2] of information services and the application of IA measures are at the forefront of information services planning.

3D4. **Protection**. Information services are protected to survive physical and electronic attack or failure according to the value of the information held and its importance to users. If protection is breached, recovery measures should be available to restore capacity. Diversity and redundancy are both used to enhance network protection.

3D5. **Risk Management**. The Joint Task Force Commander (JTFC), advised by Comd JFCIS, balances the implications of reduced IA against the required operational tempo. The establishment of an IA Officer enables Comd JFCIS to provide appropriate risk management advice. Effective Security Risk Management (SRM) ensures that risk owners are aware of the level of risk they are holding and the impact should an incident occur.

3D6. **Vulnerability Analysis**. Specialist units, with engineering, information services security and intelligence communications professionals, undertake an

[1] OPSEC is *the process which gives a military operation or exercise appropriate security, using passive or active means, to deny an enemy knowledge of the dispositions, capabilities and intentions of friendly forces*. (AAP-6).
[2] A formal statement confirming that the use of a system meets extant security requirements and that its use does not present any unacceptable risk. (JSP 440, *Defence Manual of Security*).

Information Security (INFOSEC) Vulnerability Analysis for the Commander,[3] which includes:

a. Defensive Monitoring (DM),[4] which may be used to monitor unencrypted forms of communication (unencrypted radio (voice), static telephone, service mobile telephone and facsimile transmissions) at fixed and deployed sites.

b. DISS will deliver TEMPEST inspections and assessments to help minimise compromising emanations from computer and communications systems.

c. Technical Security Countermeasures Assessment (TSCMA) to identify the presence of clandestine eavesdropping devices.

d. Computer Security (COMPUSEC), monitoring and audit tasks to identify the vulnerabilities of networked and distributed Information Technology (IT) systems, and to recommend remedial measures.

3D7. **Allied and Coalition Communications**. When UK and allied forces operate together, secure communications are usually provided in accordance with Allied Communications Publications (ACPs). For coalition operations, the lead nation generally determines appropriate INFOSEC. National CIS remains subject to national CIS Security Policy.

3D8. **Application of Security Policy**. Information services security policy applies to all military and civil information services used in the Joint Operations Area (JOA). To avoid confusion with single-Service procedures, information services Security Policy is detailed in the CIS Directive.

3D9. **Operations Security**. OPSEC is a J3 lead, but has close ties to J6:

a. **Planning**. During planning for an operation, there is an increase in communications traffic between headquarters and nominated force elements. Information services used during the planning process requires appropriate protection. Subsequent force element preparation requires practise in OPSEC techniques, usually through exercises or mission rehearsals. Consideration should be given to disguising these events by deception techniques where practicable. INFOSEC is used to prevent any indication that force elements preparation is tied to a particular operational plan or geographical area.

[3] Depending on the risks identified and the prevalent threat to CIS, Comd JFCIS may request a Force INFOSEC Team (FIT) to deploy as part of the JTFHQ J6/JFCIS for all or part of an operation.
[4] An IA technique formerly known as 'COMSEC Monitoring'.

b. **Force Assembly**. Irrespective of whether the operation is mounted from the UK, or from a forward mounting base, force assembly generates significant traffic over strategic information services links. Increased communications traffic to, or from, an assembly area may focus an adversary's interest, and result in an increased hostile intercept effort. Political events may indicate UK interest, but only the interception of communications may provide information about the timing, location and scope of any future operation. Transmission security in modern systems significantly improves protection against an adversary intercepting and analysing friendly communications. INFOSEC during this phase is enhanced by the use of only approved information services.

c. **Deployment**. Communication increases markedly during the deployment phase, particularly on information services supporting maritime and air assets. OPSEC is critical during this period, and the imposition of radio and electronic silence should be considered to deny information to the adversary. It is vital that OPSEC is maintained during deployment, and under no circumstances should insecure means be used to pass sensitive deployment information.

d. **Force Entry**. Radio silence is often appropriate during force entry and compliance with the Emission Control (EMCON) plan is essential.

SECTION II – INFORMATION GOVERNANCE

Information Security

3D10. Figure 3D.1 illustrates the links between security disciplines.[5] Within the framework of information governance and IA, information security describes the security measures taken to safeguard information in any form. It provides an important connection between traditional security staffs embedded within the J2/3 community and those directly charged with the protection of information services and its products. The information services community has a particular INFOSEC responsibility, given its ownership of the provision and maintenance of CIS equipment, to ensure that the risks to information are identified and appropriately managed.

3D11. The INFOSEC measures required are determined by a Vulnerability Assessment and/or Risk Analysis, and implemented with the appropriate Criticality Level (CL) of the CIS and/or Protective Marking (PM) of the information being handled, stored, processed or transmitted. This process ensures that confidentiality, integrity, availability and accountability concerns are addressed.

[5] DGInfo/CBMJ6/CND Policy 1.5 dated 14 May 2007 *MOD Policy for Information Assurance in the Deployed Environment*.

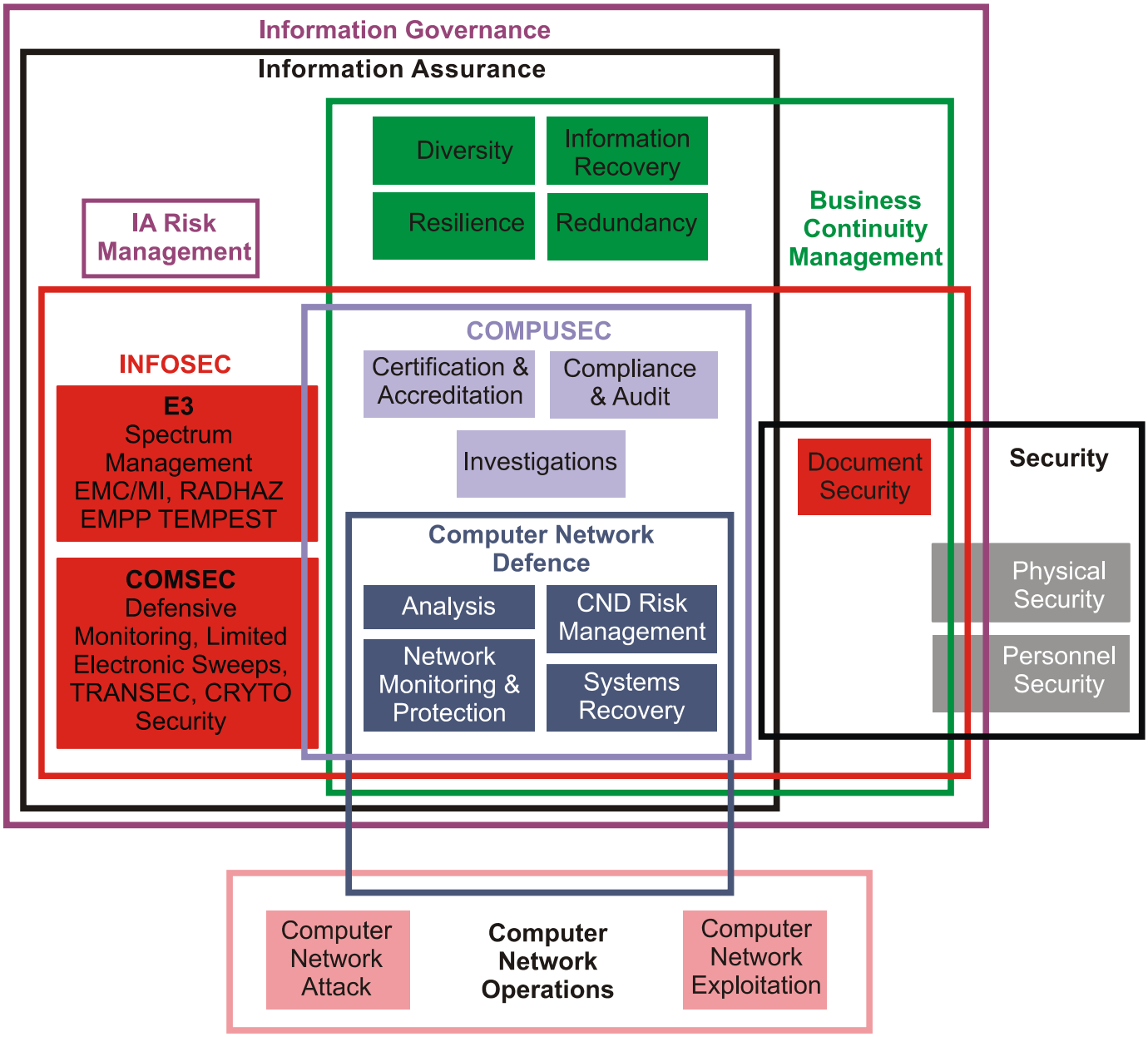


Figure 3D.1 – Linkage between Security Disciplines

Computer Security

3D12. COMPUSEC covers all facets of computer security to ensure the confidentiality, integrity and availability of IT systems, and is applied to both hardware and software. Deployed information services staffs should be aware of the significant risks that exist through the lack of accreditation of some legacy systems, standalone equipment and small systems as advised by each system's accreditor and risk owner. Accreditation advice should be taken prior to deployment or after any subsequent significant system changes, including all proposed changes to connectivity. Compliance with system security policies and any additional local policies (particularly in a multinational environment) is a vital element of COMPUSEC.

Communications Security

3D13. Communications Security (COMSEC) measures are specialised protective security measures taken to ensure the confidentiality, authentication, non-repudiation and integrity of information in communications channels. On operations, COMSEC procedures are designed and issued as JTF-level instructions, particularly if they differ from Standard Operating Procedures (SOPs). Most COMSEC procedures are detailed in the CIS Directive, but it may be appropriate to produce a specific instruction on COMSEC depending on the scale and classification of the operation. Such an instruction covers the duties and responsibilities for COMSEC, but emphasises:

a. Arrangements for the distribution of cryptographic material.

b. Transportation of cryptographic material.

c. Handling and storage of protectively marked material.

d. Transmission of plain language communications.

3D14. Measures that indicate the levels of information leakage and that help deny an opponent the opportunity to electronically eavesdrop include:

a. **Defensive Monitoring**. DM is essential to reinforce OPSEC training and to act as a deterrent against poor COMSEC, including EMCON. DM equipment is used to monitor all unencrypted forms of communication.

b. **Technical Security Countermeasures Assessment**. Eavesdropping uses clandestine listening devices to overhear and transmit or record conversations. An electronically-safe working area is critical in deployed environments where information is processed in unfamiliar locations. This is particularly important early in an operation or during a reconnaissance phase where un-trusted facilities may have to be used. The provision of an electronically safe working area requires an inspection comprising both a physical check and a TSCMA. Specialist units[6] and staff within deployed headquarters hold deployable TSCMA equipment.

3D15. COMSEC procedures also provide protection against Electronic Attack, including any defensive measures against search, interception and direction finding, jamming and deception. These procedures are produced as a JTF-level instruction - Protection against Electromagnetic Attack (see Section III).

[6] For example, 591 Signals Unit at RAF Digby and ISS DE3A EST at Blandford.

Cryptographic Security

3D16. Specially devised methods or processes, usually called cryptosystems, are used to protect information in communications channels. Cryptosystems are used to conceal the content of communications and their effectiveness depends on the strength of the cryptologist used, the overall protection given to the cryptosystem and the correct use of operating procedures. Specific guidance on cryptographic security is published in BMD/0001/0001 the *Defence Cryptosecurity Operating Instructions* and JSP 440. UK national instructions are compatible with the corresponding NATO Cryptographic Security Instructions published in Allied Military Security General (AMSG) 293 and Allied instructions contained in ACP 122(E) *Information Assurance for Allied Communications and Information Systems*.

3D17. Most modern UK and North Atlantic Treaty Organization (NATO) cryptosystems are highly resistant to cryptoanalysis, but a determined and capable adversary could obtain details of the cryptology either by theft or by suborning a UK/NATO national. Cryptographic material is safeguarded by enforcing a comprehensive security policy, articulating physical, personnel, and communications security (including Radiation Security (RADSEC) and TEMPEST). Comd JFCIS directs which protective measures are applied to information exchanges and information storage, including online and offline cryptographic systems, secure speech equipment and authentication and code systems.

Radiation Security

3D18. RADSEC manages the risk associated with radio signals, both intentional and unintentional. Compromising emanations, when intercepted and analysed, may disclose protectively marked information. An essential element of RADSEC is TEMPEST, the investigation and study of unintentional emanations. In addition, it is important to conceal the radio frequencies to be used by UK forces, normally conducted in conjunction with the Battlespace Spectrum Management (BSM) Plan.

Computer Network Defence

3D19. Information services relies heavily on computer networks, and the risk from Computer Network Attack (CNA) and Computer Network Exploitation (CNE) is increasing due to a proliferation of increasingly sophisticated opponents and techniques. Countermeasures are essential to provide IA. Alert, Warning and Response (AWR) is vital to the Computer Network Defence (CND) effort and JSP 541*MOD Alert Warning and Response Policy and Procedures Manual* describes the procedures for implementing CND measures across Defence networks.

3D20. Networks are susceptible to attack from a wide range of opponents: directly from individuals, terrorists and Foreign Intelligence Services (FIS); and indirectly from malicious code such as viruses. The risk of attack becomes more acute as frontline capability becomes increasingly network enabled.

3D21. The most likely method of electronic attack against information services is through gateways with other systems. Access could be made via the information systems of third parties, such as allies, industry or other government departments, which are connected to military systems. Indirect attacks may be made against services upon which military activities depend. CND is used to counter attacks and is defined as *actions taken within an overall IA framework to deter, protect from, react to and recover from a CNA or CNE on MOD's computer networks*. Threats to information hosted on the MOD's computer networks are categorised in Figure 3D.2:

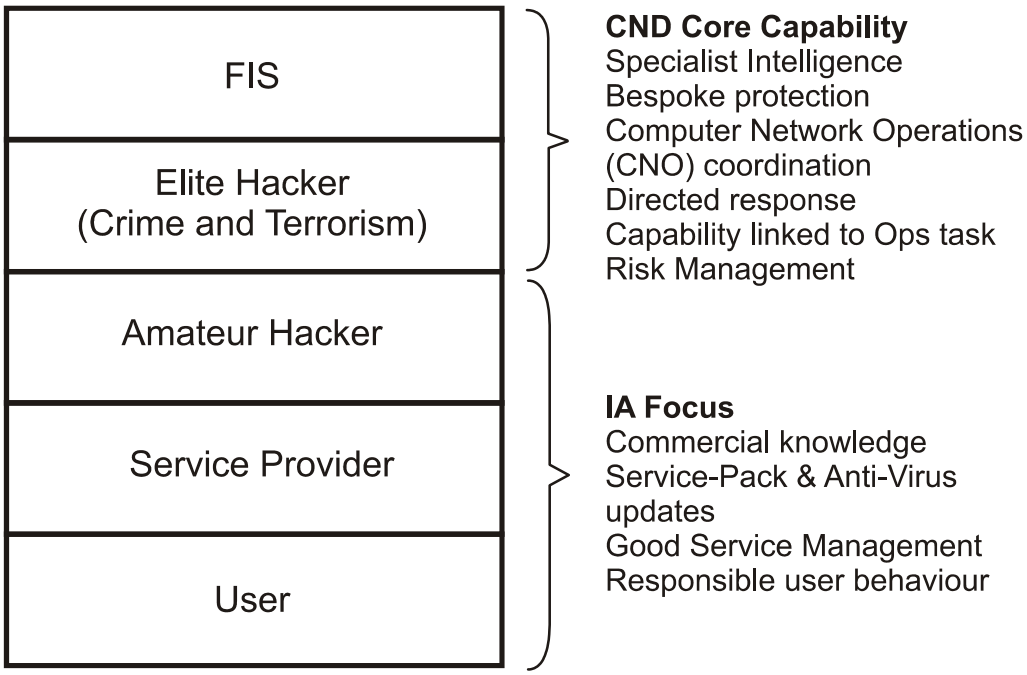


Figure 3D.2 – MOD CND 'Threat Stack'

3D22. Although CND can detect and respond to threats from the lower 3 categories in Figure 3B.2, its operational focus is on the top 2 categories of FIS and elite hackers. A balanced and cost-effective mix of CND measures is deployed to counter these threats to provide credible defence against CNA. These measures are:

a. **Deter**. A well-defended installation with an effective guard force is likely to deter a physical attack. An information system or network well protected against CNA is similarly likely to deter an electronic attack.

b. **Protect**. Protection is provided through a combination of physical and electronic security measures. The cost of absolute protection is usually prohibitive; therefore, the residual risk is identified and managed, striking a

balance between technical and non-technical information security procedures. The sensitivity of the information to be protected, resources available and the likely operational impact of compromise influences the degree of proactive risk management.

c. **Detect**. Detection is used to gain evidence of attacks or methods. This alerts staff to attacks and triggers countermeasures. Detection measures include malicious code detection, system audit and accounting, network monitoring, hardware and software configuration management, detection of unauthorised system configuration changes, detection of unauthorised actions by personnel and the provision of appropriate training. CND Intrusion Detection Systems (IDS) are deployed, in particular at network boundaries, key nodes and gateways, to maximise the potential of attack detection.

d. **React**. Reaction consists of:

(1) Preventing further damage by immediate response.

(2) Implementing counter-compromise actions.

(3) Assessing information lost, corrupted or compromised.

(4) Ameliorating the damage already sustained by reconfiguration of systems or pathways.

(5) Restoring the system service, possibly at a degraded level.

(6) Initial measures to locate the source of the attack by initiating an investigation including the forensic safeguarding of evidential data.

e. **Recover**. Recovery includes analysing and applying the lessons from an attack, and establishing protective measures to generate a more robust IA posture.

SECTION III – PROTECTION AGAINST ELECTROMAGNETIC ATTACK

3D23. All electromagnetic emissions are vulnerable to exploitation by an adversary conducting Electronic Warfare (EW). With the appropriate equipment, signals can be detected, intercepted, sourced, analysed and disrupted. The ideal result of effective Electromagnetic Protection (EP) is preventing an opponent from detecting friendly electromagnetic radiation. Full prevention may be unachievable, so the principal objectives of EP are to:

a. Minimise emissions and thereby reduce an opponent's intelligence collection.

b. Minimise all other types of electromagnetic transmissions, such as radar and infrared lasers, which may compromise friendly operations.

3D24. Effective EP is achieved in 2 ways:

a. **Active Electronic Protection**. This consists of detectable measures to ensure effective use of the Electromagnetic Spectrum (EMS), such as changing frequencies and changing modes of operation.

b. **Passive Electronic Protection**. This consists of undetectable measures, such as operating procedures and technical features of the equipment, to ensure the unhindered use of the EMS as well as counter Electronic Surveillance (ES) and counter Electronic Attack (EA) measures.

3D25. EMCON is complex, given the plethora of CIS involved. A JTF depends heavily on the EMS for communications, surveillance, target acquisition and weapons guidance. The benefits of radio silence are balanced against the need for effective Command and Control (C2).

(INTENTIONALLY BLANK)

ANNEX 3E – BATTLESPACE SPECTRUM MANAGEMENT

3E1. Battlespace Spectrum Management (BSM), a subset of Battlespace Management (BM), is *the planning, co-ordination and management of the electromagnetic spectrum (EMS) through operational, engineering and administrative procedures; it enables military electronic systems to perform their functions within intended environments without causing or suffering harmful interference*.[1] Efficient and effective use of the EMS by the Joint Force provides an operational advantage to the Commander and enables optimal spectrum use through de-confliction, protection, exploitation and denial of this valuable resource within the Joint Operations Area (JOA).

3E2. BSM is primarily a J3 function[2] and the process through which the EMS, within the Electromagnetic Environment (EME), is controlled. BSM is discussed in JDP 3-70 *Joint Battlespace Management*[3] and supporting Joint Force Operating Procedures (JFOPS) for Joint (Jt) BM. The following information relates to BSM within the context of Joint Force Communications and Information Services (JFCIS) and Frequency Management.

Battlespace Spectrum Management Function

3E3. BSM is conducted through a BSM Cell within the Joint Task Force Headquarters (JTFHQ), normally part of J3/5 but it can also be a J6 role. BSM requires close engagement and liaison with key spectrum stakeholders within a Joint Task Force Headquarters (JTFHQ) and beyond, including:

a. JFCIS/Joint Network Centre (Jt NETCEN) Frequency Manager (FMAN) for CIS requirements.

b. J2 (Intelligence, Surveillance, and Reconnaissance (ISR) for Unmanned Aerial Systems (UAS) Common Data Link (CDL) downlink, Tracking, Telemetry and Control (TT&C) uplinks and Restricted Frequency List (RFL).

c. Electronic Warfare Co-ordination Cell (EWCC), to co-ordinate Electronic Attack (EA), Electronic Surveillance (ES) and Electronic Defence (ED).

d. Force Protection Electronic Countermeasures (ECM(FP)).

e. Tactical Data Links Authority (TDLA), for example Links 11 and 16.

[1] Allied Communications Publication (ACP) 190(B) *Guide to Spectrum Management in Military Operations*.
[2] J5 or J6 can also undertake the BSM role depending on the operation in hand.
[3] Programmed for promulgation in early 2008.

f. Government Communications Officer (GCO) for Signals Intelligence and Electronic Intelligence (SIGINT/ELINT) requirements.

g. J3 for kinetic/non-kinetic effects on the EMS or its users.

h. Other Government Departments (OGDs) for CIS or other requirements.[4]

i. Media Operations and Information Operations (Info Ops) for support to broadcast requirements.

j. Maritime, Land and Air Components for requirements including navigation radar, ground-to-air communications, tactical mobile radar, Missile Approach Warning Systems and EA (including attacks on navigation systems (Navigation Warfare (NAVWAR)).

3E4. Additionally, there may be a requirement to liaise and co-ordinate with Non-Governmental Organisations (NGOs), International Organisations (IOs) or Private Military Security Companies (PMSCs), who characteristically use radio communications and commercially available ECM(FP) equipment.

3E5. In a multinational operation, the Lead Nation establishes a Combined BSM Cell (CBSMC). Participating nations deploy a national BSM Liaison Officer (LO) to work in the CBSMC as well as a national BSM Cell within their own senior national HQ. For non UK-led multinational operations, a UK BSM LO is deployed in the CBSMC.

3E6. Initial planning for a Joint Force identifies the information exploitation requirement. Those elements of the information exchange requirement that require EMS allocation are co-ordinated and consolidated into the force spectrum bill or EMS resource requirement. This requirement is passed to the BSM Cell to consolidate all spectrum requirements and liaise with the host nation (HN) civil spectrum management authority to gain approval. In a multinational operation, consolidation of all multinational force spectrum requirements and liaison with host nation is done by CBSMC on behalf of all participating nations' military forces.

3E7. In an operation where there is no civil spectrum management authority, or the political/strategic situation prevents liaison from taking place, anecdotal spectrum records, together with spectrum situational awareness derived from real-time spectrum monitoring, provides a best-estimate spectrum resource from which to provide assignments and allotments.

3E8. Once a host nation issues spectrum assignments or allotments, they are sub-issued to the appropriate requesting authority. For example, assignments and

[4] Such as the Foreign and Commonwealth Office or Department for International Development may be deployed with a JTFHQ, separately, or as an Inter-agency Planning Team (IAPT), as part of an integrated approach.

allotments to support JFCIS (including components) are issued to the JFCIS/Jt NETCEN FMAN, who in turn issues them to the relevant system manager or component FMAN.

3E9. The BSM organisation depends on the size and scale of each operation; however, Figure 3C.1 offers generic guidance on the BSM organisational structure within a medium or large scale JTFHQ. BSM is based on interpretation of the Commander's Intent, operational priorities and an intelligence assessment of the EME. BSM, therefore, requires significant coordination with the J2, J3 and J6 staff branches. In this example, the Joint Task Force Commander (JTFC), through Jt BM staff and BSM Spectrum Working Group (SWG), empowers the BSM Cell to manage the EMS throughout the JOA in order to ensure minimal restrictions are applied to friendly forces. BSM SWG composition and BSM Command and Control (C2) structure diagrams are at Figures 3E.2 and 3E.3 respectively.

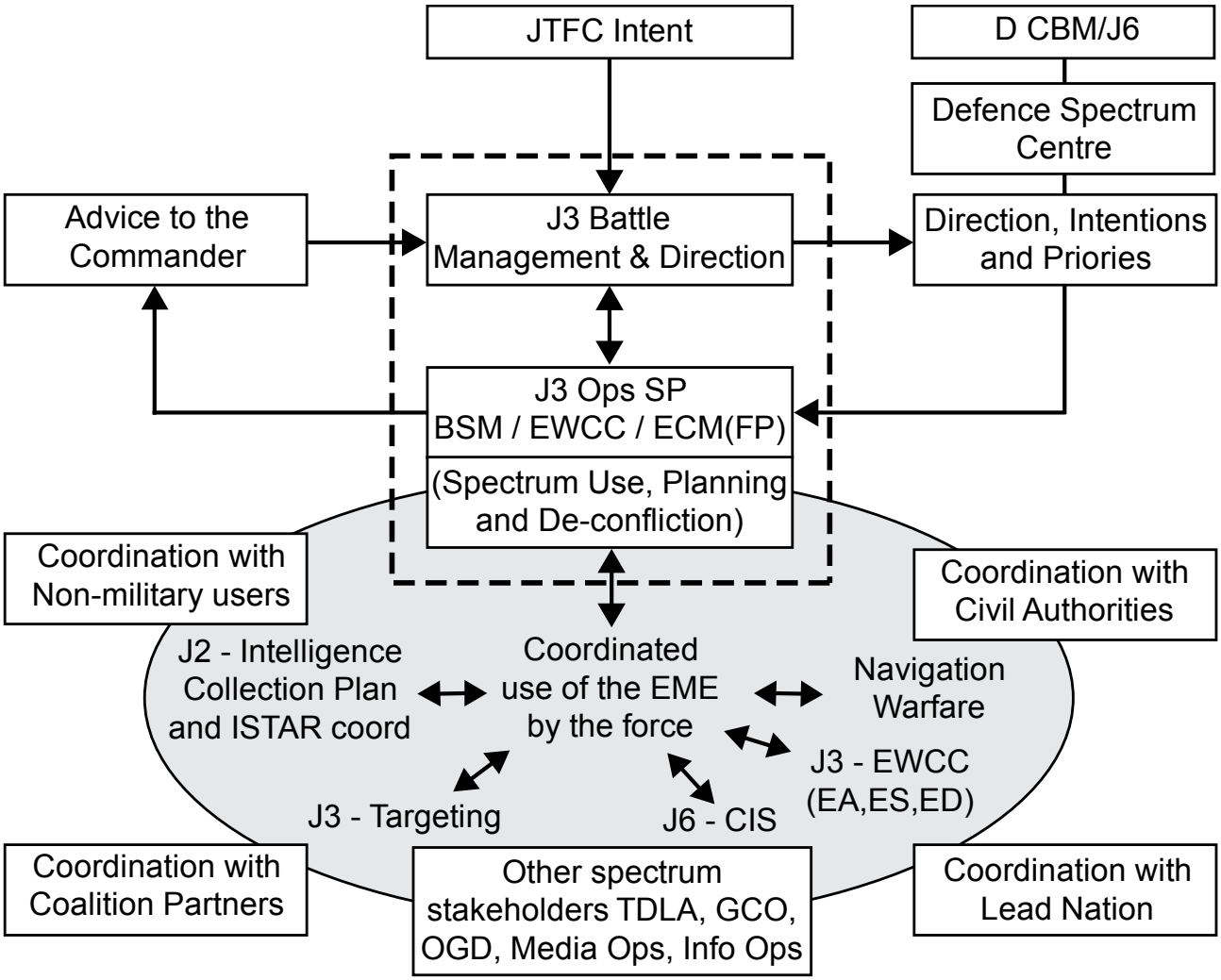


Figure 3E.1 – JTFHQ BSM Organisational Structure

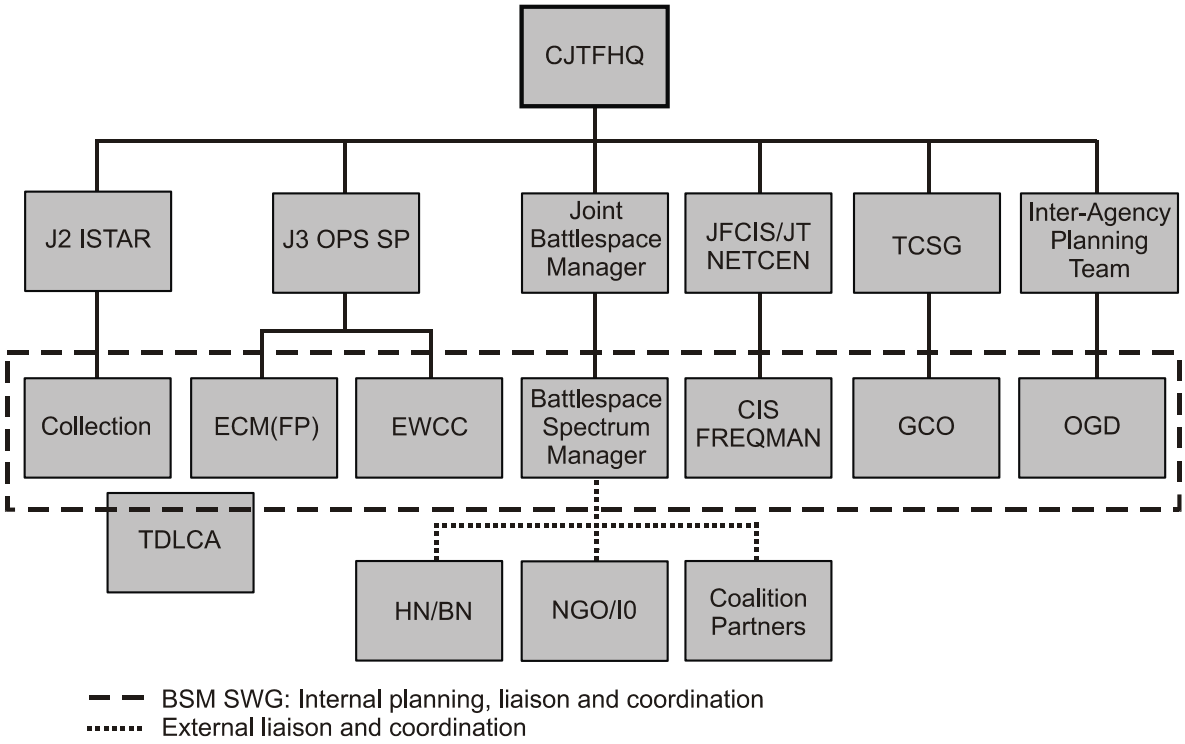


Figure 3E.2 – JTFHQ BSM C2-SWG Composition

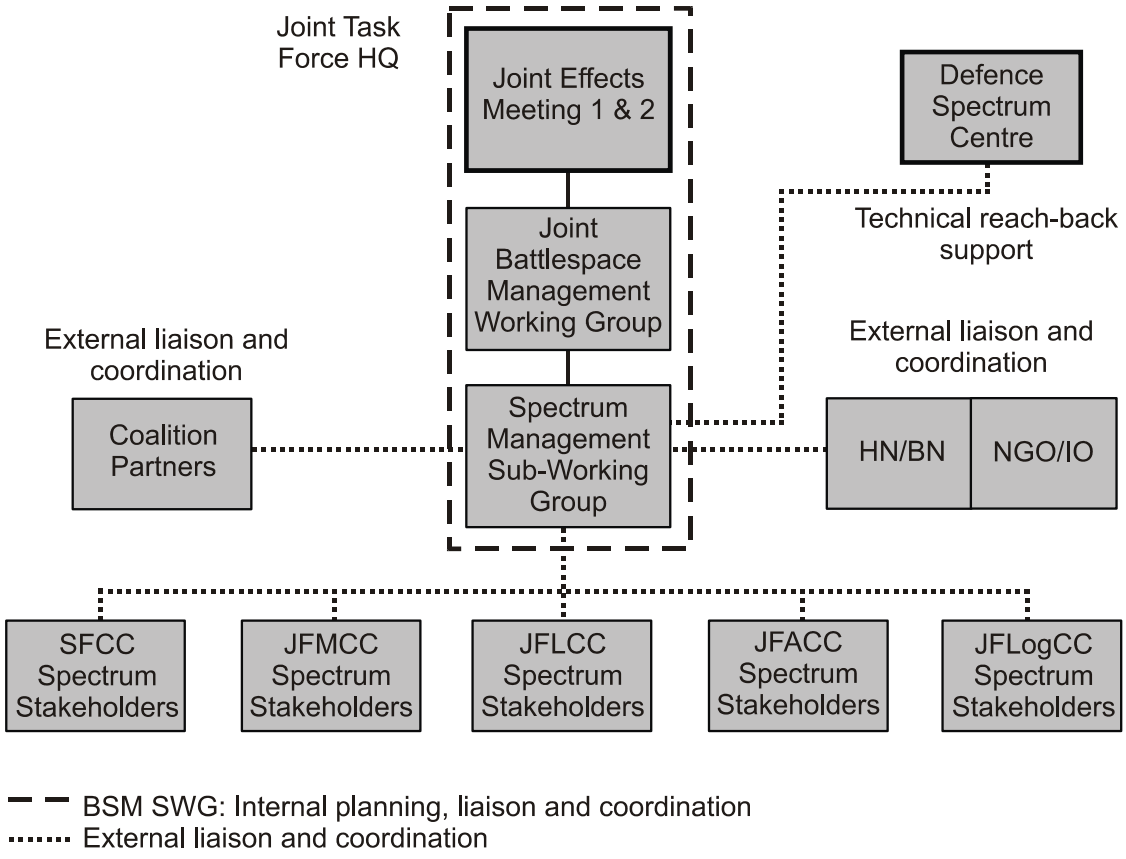


Figure 3E.3 – JTFHQ BSM C2 Structure

CHAPTER 4 – INFORMATION SERVICES SUPPORT TO THE CONDUCT OF OPERATIONS

401. During operations, Commander Joint Force CIS's (Comd JFCIS) staff ensure that information services deployed within the Joint Operations Area (JOA) satisfies the Joint Task Force Commander's (JTFC) information needs. Information services should be sufficiently agile to respond to changes to the commander's plan, as well as changes in tempo and posture, which may alter the information exchange requirement. Comd JFCIS should also consider in advance the information services support required during the roulement of forces, the transition to a follow-on force and redeployment from the JOA. Following on from the *prepare* phase articulated within Chapter 3, this Chapter focuses on *deploy*, *operate* and *recover*.

SECTION I – DEPLOY PHASE

402. **Deployment**. Upon arrival in theatre, the primary focus of the J6 staff will be delivering the priority services identified during the *prepare* phase. This will enable the deploying force to begin exploiting information services upon arrival in the JOA. The CIS Directive defines the Initial Operating Capability (IOC), which will deliver mission-essential C4, intelligence, surveillance and reconnaissance (ISR), logistics and medical information services capability as early as possible. It will also identify and prioritise the critical services needed for setting-up and commissioning the headquarters. Once critical services are established the information services delivery teams will focus on delivering the full information exchange requirement in order to achieve FOC. The CIS Directive will define the requirements and expected completion dates of both IOC and Full Operating Capability (FOC)[1]. However, the operational tempo may force an adjusted timeline which will need to be planned as a contingency and managed. Once FOC has been declared information services enter the *operate* phase.

403. **Command and Control**. The command states of all information service assets are detailed in the CIS Directive. Normally Comd JFCIS assumes operational command of all strategic assets[2] and theatre information services capabilities assigned to the operation (SF excluded[3]). Tactical information services assets usually remain under operational command of their assigned formations. In effect Comd JFCIS acts as a service provider of strategic and operational level information services to a range of customers; who may then have their own bespoke tactical systems. The key

[1] IOC will be the minimum CIS required for the headquarters to commence work. FOC will be the fully resilient solution identified within the information exchange requirement to meet the JTFC's requirements.
[2] With the exception of strategic satellite communications (SATCOM) capability remaining OPCOM with CIO/J6-Ops and CJO retaining OPCON.
[3] However, Special Forces (SF) and other government departments requirements will be investigated during the planning stages to identify if consolidation of IS is feasible. There will be a requirement to deliver SF LO specific VOICE and DATA capability within the Joint Task Force Headquarters (JTFHQ).

principle for discharging this responsibility is that unless Comd JFCIS specifically issues any constraints, subordinate commanders have the freedom to configure and operate information services to meet their local needs (provided that the capability is not part of a wider network or forms part of the joint force information exploitation effort). It should also be noted that maritime-based operations will be supported in a different way due to the additional limitations associated with maritime platforms; however, the principles outlined throughout the *deploy*, *operate* and *recover* phases should be adhered to.

404. **Governance**. The Network Authority (NA) is responsible for the coherence, performance and integrity of all aspects of the Defence network, and the information flows it enables, to support the operational and business needs of Defence. The Network Authority comprises the following three sub-authorities:

a. **Network Capability Authority**. The role of the Network Capability Authority (NCA) is to manage the coherent development of requirements for new services, systems, platforms and applications that require support from the Defence Network; this includes prioritisation of funding. The NCA captures these requirements in order that the network is designed, built, maintained and configured accordingly.[4]

b. **Network Technical Authority**. The Network Technical Authority (NTA) has authority over the entire Defence network and will ensure technical compliance for the development and integration of changes to, introduction and disposal of, all services, systems, applications and platforms.

c. **Network Operating Authority**. The Network Operating Authority (NOA) has authority for the operation of the whole of the Defence network through 2 separate delegations: first from the Chief Information Officer (CIO) on behalf of the Defence Board for routine operation and second, from Chief of the Defence Staff (CDS), via Chief Defence Materiel (CDM), for those activities specifically associated with defending the network. The NOA can reshape the network to meet priorities and, if required, to isolate services or users. The NOA provides assured end-to-end (E2E) information services to all users less SF and users on non-assured services. The day to day responsibilities of the NOA are largely directed and guided through the operation of the Global Operations Security Control Centre (GOSCC) and Comd JFCIS as specified in the CIS Directive.

[4] The intention is for the NCA to engage with other capability sponsors on a 'green card' basis i.e. collaboratively account for information needs from the outset. The NCA reserves the right to adopt a 'Red Card' approach in the event of wilful non-conformity by which it will articulate risks present in a particular course of action or programme/project through its relationship with the scrutiny group and Secretariat Equipment Capability.

405. **Building Information Services Capability in Theatre**. The first priority is to commence delivery of the information services capability to a support the IOC services.[5] This must be achieved quickly as headquarters staff arriving in theatre need information services immediately. As each service is tested and commissioned and declared operational it is captured on the network operating picture. Comd JFCIS uses the network operating picture to judge when IOC and FOC are achieved. In doing so Comd JFCIS must ensure that the Jt NETCEN and the DISS GOSCC have agreed that all services are operational, subject to agreed support arrangements, and are being managed in accordance with extant policy.

406. **Business Continuity of Information Services**. Mission critical information flows are identified as part the information exchange requirement process. Business continuity plans must consider alternative methods for delivering mission critical information, including the need to establish and test reversionary modes of service delivery. The resilience of non-mission critical services depends on the prioritisation of resources.

407. **Prioritisation**. Information services staff, at each level of command, maintain priorities for their area of responsibility,[6] reflecting the operational impact of service loss. These priorities, updated on a regular basis to reflect changes in the JTFC's plan, should be clearly understood by all service providers to ensure the timely restoration of essential capability.

408. **Service Management**. Service providers should be clear about how to apply technical direction and escalate issues. Comd JFCIS is responsible for producing service management and assurance concept of operations (CONOPS) for the operation in line with standing ISS publications. The CONOPS will be outlined in the CIS Directive that will assign specific service management and assurance responsibilities in the JOA for the Jt NETCEN and Component J6 staffs. Service assurance policy and direction is provided by DISS, via the Network Operating Authority (NOA) issued by CIO/J6-Ops, and is reflected in DISS Publications. Information service users are provided with procedures to report faults and service providers should have instructions on how to manage and report service delivery.

SECTION II – OPERATE PHASE

409. To declare FOC, Comd JFCIS must ensure that information services deployed within the JOA satisfies the commander's information needs. Following FOC, the Jt NETCEN focuses on sustaining current in-theatre information services to meet the commander's extant information needs allowing Comd JFCIS to focus on planning for

[5] This should be conducted as soon as possible and may involve assets being set up and utilised in a location other than their planned final location. If this is the case, then JFCIS and Jt NETCEN must mitigate against their potential movement during the testing and commissioning phase.
[6] For example, at the strategic level, the CIO/J6-OPS CIS Restoration List prioritises strategic assets such as SATCOM.

future requirements. The historical J6 focus purely on the provision of a communications network is no longer sufficient. J6 staff must have a detailed understanding of how information is managed and exploited, the C4ISR, logistic and medical applications and core services, how information flows to enable the services, and the network design and capabilities over which the information is collected, transmitted, stored and retrieved. This understanding enables the Jt NETCEN to prioritise services, diagnose and rectify faults, and manage reversionary modes. Comd JFCIS's planning will include new requirements, enhancements, reductions and technical upgrades of information services, support to the roulement of forces, the transition to a follow-on force and termination of the operation.

410. To sustain information services an E2E service management and assurance approach is used that enables quick identification and rectification of any failures. Each system or capability will have a Through-Life Capability Management (TLCM) plan detailing the level of support that has been procured. Additional considerations for Comd JFCIS are:

a. **Level 3 Support Organisations**. This support sits between that available at Front Line Command (FLC)/formation level and any in (or out of) theatre support provided by contractors. Tasking will be directed by the Jt NETCEN, via the respective Level 3 liaison officer normally located within the Jt NETCEN. The liaison officer will act as the conduit to any contractor support, whether in-theatre or via the Level 3 reach-back facilities. The size and composition of this deployed support will be decided during the information services estimate.

b. **Surge Personnel**. Surge personnel may be required to install, restore or maintain information services in support of the E2E approach. Comd JFCIS agrees the need for, and allocation of, surge personnel (who may be military, civil service or contractors) with PJHQ, ISS and the FLCs as required. Deployment of surge teams, including Contractor Support to Operations, is co-ordinated by PJHQ.

c. **Logistic Support to Information Services**. Comd JFCIS should consider logistic support as part of the information services estimate and keep the requirement under review as the campaign develops. Prioritisation, tracking and management of spares helps maintain information services capability. If applicable, local purchase of spares should be considered to improve availability. However, this is only feasible for some equipment and should be detailed prior to deployment. Non-military information services can attract significant commercial rental or call charges. Local purchase may also be used for consumable items that form a critical element in information services capability. Delegation of financial authority to Comd JFCIS and Component J6 staffs provides local control over operational usage and costs.

These arrangements are subject to formal delegation of financial authority agreed with the relevant J8 finance organisation.

d. **Environmental Support**. Following delivery of the information exchange requirement an assessment of environmental issues related to information services should be kept under frequent review. Some commercial off-the-shelf (COTS) products may not be designed for use in extreme environments and may be prone to degradation or failure due to temperature extremes, vibration, water and foreign particles ingress. COTS equipment may, therefore, require environmental protection, additional power, as well as physical and electronic protection.

411. **Reports, Requests and Returns**. The requirement for Reports, Requests and Returns (R3) is articulated in directives and instructions issued by headquarters at every level of command, with Comd JFCIS' requirements set out in the CIS Directive.[7] JFCIS R3 should be fully aligned with the theatre battle rhythm. Comd JFCIS' staff should pay particular attention to the information services contributions to the JTFHQ Assessment Report and JTFHQ Down Report.

412. **Situational Awareness**. During the campaign, Comd JFCIS seeks to gain and maintain the situational awareness[8] required to react rapidly to changing situations, which should include a detailed view of the information services situation and of the campaign as a whole. Integration into the JTFHQ Campaign Rhythm, as well as the reports and returns process, augmented by other tools and techniques, serves to improve Comd JFCIS' staff's situational awareness. Additional tools include:

a. **Video Teleconference and Conference Telephone Calls**. Component headquarters are often remote from the JTFHQ and Comd JFCIS. VTC and conference calls are used to ensure close liaison is maintained between Comd JFCIS and Component J6 staff as well as connection back to PJHQ and UK-based organisations. Agendas for these exchanges may include:

(1) An update from Chief of Staff (COS) JFCIS on recent developments.

(2) Back briefs from component J6 staffs.

(3) A review of the Risk and Issues registers.

(4) A summary of key events and tasks over the next 24 hours.

[7] ASSESSREPS, DOWNREPS, Logistics Reports, Personnel Reports, Operational Record Reports, Serious Incidents Reports.

[8] Situational Awareness is *the understanding of the operational environment in the context of a commander's (or staff officer's) mission (or task)*. (JDP 0-01.1, *UK Supplement to the NATO Terminology Database*, 8th Edition)

(5) Comd JFCIS' intent and guidance for the next 96 hours.

b. **Joint Operations Picture**. Comd JFCIS and component J6 staffs contribute to the Joint Operations Picture (JOP)[9] by incorporating detail on information services activity affecting the JOA.

c. **Mission Rehearsal and 'Red Teaming'**.[10] Mission rehearsal and *red teaming* are used to run through likely operational tasks. The process involves selected personnel from Comd JFCIS' and component command headquarters' staff testing the robustness of plans, identifying risks and developing contingency plans.

413. **Operations Documentation**. Comd JFCIS' staff contributes to all operations documentation, especially the CIS Annex of the JTFC's Mission Directive. Documents with a CIS contribution are:

a. **Campaign Directive**. The JTFC's Campaign Directive provides an overview of the conduct of the campaign and is the keystone document for the JTF and component commands. Comd JFCIS' staff provides a short paragraph outlining how they will support the campaign.

b. **Force Instruction Document**. The Force Instruction Document supports the Campaign Directive and provides supplementary instructions and information from across the JTFHQ. The CIS Directive will normally be published as an annex to the Force Instruction Document.

c. **Operations Plans**. As the design of the operation is refined, an Operations Plan (OPLAN) is written by J5 to outline the envisaged Concept of Operations (CONOPs) including the JTFC's intent and could potentially draft Component mission statements. Comd JFCIS' staff completes the CIS contribution to this OPLAN.

d. **Warning Orders**. Warning Orders (Wng Os) are produced in advance of a formal task to ensure that the personnel and equipment are ready, and capable, to deploy and meet the task timelines on order.

e. **Operation Orders**. The J3/5 cell drafts Operation Orders (OPORDs) including component mission statements and detailed coordinating instructions. Comd JFCIS' staff completes the CIS contribution to this

[9] The Joint Operations Picture (JOP) is *the total set of shared information on a particular operation, or Joint Operations Area, available through a secure information environment on CIS networks to support situational awareness and decision-making by UK commanders, and facilitate information sharing with allies and partners*. (JDP 0-01.1,8th Edition)

[10] DCDC Guidance Note, *A Guide to Red Teaming*, 2010 refers. A red team is an enabled cell, discrete from the main staff, that serves to develop opponent, neutral, cultural and contextual perspectives in order to challenge the perceived norms and assumptions of the commander and staff.

OPORD.Fragmentary Orders. Fragmentary Orders (FRAGOs) are significant modifications to previous orders or direction. Comd JFCIS contributes to JTFHQ's FRAGOs as appropriate, but may also issue FRAGOs to subordinate CIS organisations to accomplish specific tasks.

f. **Lessons Identified**. Throughout all phases of an operation, on roulement or at major transitions in a campaign there is a requirement to capture any lessons that will enable improvement. Part of the lessons process is the creation of a post event report which will be produced by all Force Elements. However, a single post event report from Comd JFCIS is required by PJHQ J6, which will be followed up by a post event interview to allow for expansion and in-depth discussion of any of the points raised within the formation's post event report. The post operational interview will be led by ACOS J6 in line with PJHQ J7 guidelines.

Enduring Campaigns

414. **Planning During an Operation**. Under the direction of Comd JFCIS his staff conducts planning throughout a campaign; a planning process that follows the same stages described in Chapter 3. The commander's information needs are continually reviewed. If required Comd JFCIS will direct a review of the information services estimate to deliver an updated information exchange requirement thereby ensuring that changes to the JTFC's scheme of manoeuvre, main effort and force laydown are supported by an appropriate information services plan. Comd JFCIS and his staff within the JOA lead the planning in consultation with PJHQ J6, FLCs and DISS, supported by the service providers and their staff. DISS, as the Network Authority, in consultation with Comd JFCIS, approves the information services solution's design, although PJHQ retains ownership of the requirement and associated risk. DISS, as the design authority, is then responsible for assuring E2E connectivity and service delivery. This condensed information services planning environment requires close coordination and active risk management to underpin operational success.

415. **Management of the Information Exchange Requirement**. As the operation develops the information exchange may change to incorporate new user requirements into the information services design and architecture. Accordingly, the information exchange requirement evolves under Comd JFCIS' configuration control.

416. **Changes to Force Structure**. As the operational theme changes between major combat operations, stabilisation and peace support activities or a campaign footing is desired, the force structure and tasks will change and engagement with multinational and multi-agency actors will increase. These changes in posture, purpose and operational theme will all alter the JTFC's information needs and must be planned for, and resourced, in advance. Any drawdown of forces associated with an improving security environment may offer the opportunity to commercialise and

contractorise military information services in order to regenerate a contingent capability.

417. **Commercialisation and Contractorisation**. While commercialisation and contractorisation of CIS capability may offer considerable benefits, including the potential regeneration of military capability,[11] and a more cost-effective and capable solution, they can, however, create additional operational risk. Commercial solutions are unlikely to be suitable in mobile, hostile or austere environments, and contractorised solutions may impose an additional force protection burden. The feasibility of a commercial or contractorised solution depends upon operational circumstances and a detailed assessment of the potential risks and benefits.

418. **Multinational Aspects**. In multinational operations, command and control and situational awareness are normally supported by a coalition network infrastructure. Comd JFCIS should develop a clear understanding of how contributing nations are supporting the overall information exchange requirement. In complex and rapidly changing operational situations however, national postures and contributions may change suddenly and disrupt the cohesion of the multinational information services contribution. Services provided by individual nations may be withdrawn, reducing the capability and integrity of the network. Comd JFCIS' staff must be prepared to react to these changes by developing and rehearsing contingency plans and subsequently taking action to deal with unexpected events.

419. ***Roulement* of Forces**. The *roulement* of forces is likely to lead to a change in the commander's information needs. If J6 forces are subject to *roulement*, which may be initiated by the JTFC, CIO/J6-Ops, PJHQ J6 or Comd JFCIS it may provide the opportunity to consider contractorisation and commercialisation to release military assets and provide a more cost effective enduring solution. In either case these changes to the force require deliberate planning to:

a. Capture new information exchange requirements.

b. Redesign the information services solution.

c. Issue new directives, such as a revised CIS Directive.

d. Manage the changeover of personnel.

Continuity of information services is aided by engaging with the incoming commander, his staff and specialist information services staff as soon as practicable. This enables information services planning to both meet any new information needs and to develop the incoming staff's appreciation of how current information services

[11] Commercialisation replaces military 'green' equipment with commercial 'white' equipment; this only frees up the military equipment for redeployment, but does not negate the need for military manpower to operate it and therefore does not regenerate the full operating capability. However, contractorisation releases both military equipment and manpower.

contributes to the overall mission. A key challenge will be maintaining the information services during the change of personnel; Comd JFCIS should investigate the early deployment of key liaison officers to act as the continuity to bridge any gaps in staff capability.

SECTION III – RECOVER PHASE

420. The completion of the operation or a significant change in the tasks undertaken by the components (such as a move from focussed intervention to peace support) may require major force restructuring including the requirement for formations to depart from the JOA. This requires the J6 staff to develop appropriate plans to drawdown the information services. The plans will ensure that: operational information is correctly annotated and archived to assist with the formal operational record keeping process; equipment is returned and regenerated (if appropriate); and UOR equipment will be either taken into core or disposed of. Throughout, drawdown information services must continue to meet the remaining force element's information needs until final departure.

421. **Handover of Responsibility**. As the campaign develops, the JTFC may need to transition responsibilities to an indigenous force or multinational follow-on force. Careful planning and co-ordination with the incoming nation's information services staff will ensure capability is sustained during the transition phase. CIO/J6-Ops and PJHQ J6 should assess whether it is appropriate to leave UK CIS equipment in place to assist the follow-on force, which may require gifting policy direction from PJHQ and MOD.

422. **Recovery**. The recovery of forces from theatre involves significant logistic effort, changes to information services capability, potential contractorisation or commercialisation and the drawdown or cessation of services. Comd JFCIS' staff require early and close engagement with J4 staff to achieve a full appreciation of the JTFC's recovery plan to ensure that capability is maintained at the appropriate level throughout. Areas that should be considered are:

a. **Data Management**. Contemporary operations have highlighted that the amount of data produced during an operation, across various systems and security domains, requires consolidated effort to: capture the data, transfer it to a system that enables the records to be accessed; cleanse the data (remove duplicates); and produce the Historical Record. To mitigate some of these data challenges, regular deployment of surge information management/information exploitation teams, particularly if the operation has been enduring, will ensure that data management is continuously reviewed. The requirement to deploy surge capability should be captured as early as possible in order to fully understand and consider the benefits of deploying an information management/information exploitation surge team.

b. **Urgent Operational Requirement Disposal**. Any equipment procured under the operation's UOR process will require a review to clarify its future utility, prior to cessation of its capability. DISS, as the Network Authority, working with MOD Comd JFCIS, PJHQ and the FLCs will conduct a review to identify if the capability is to be taken into core, disposed of locally, transferred to another operational theatre or alternate options considered.

c. **Maintaining Information Services until Final Drawdown**. As forces drawdown, the information exchange requirement will change as less users, from fewer locations, require access to core services and applications. However a significant surge in logistic information services should be expected and this may require the deployment of addition capability to meet the demand . To ensure sufficient information services are maintained throughout the period, consideration should be given to the order of departure, surging expeditionary capability to release less mobile or fixed infrastructure, and transfer of responsibilities to either the host nation or to another troop contributing nation.

d. **Asset Management**. Comd JFCIS must be fully involved in the J4 draw-down process during the *recover* phase. Information services constitute a significant part of the asset management process and as such will probably be the last service to be de-commissioned.

e. **Recuperation**. Following the recovery of the equipment, there will be a FLC-led requirement to reconstitute (and rehabilitate) the capability. Consideration of the enduring financial requirement and any follow-up investigation into significant capability losses can be mitigated by ensuring that regeneration is an integral part of the *recover* plan.

LEXICON OF TERMS AND DEFINITIONS

The primary references for terms and their definitions are indicated in parentheses.[1] Those marked (JDP 6-00) are new and will be incorporated in JDP 0-01.1 '*UK Glossary of Joint and Multinational Terms and Definitions*' following ratification and subsequent promulgation of this publication.

Computer Network Defence
Actions taken to protect against disruption, denial, degradation or destruction of information resident in computers and computer networks or the computers and networks themselves. (JDP 0-01.1)

Concept of Operations
A clear and concise statement of the line of action chosen by a commander in order to accomplish his mission. (AAP-6)

Control
That authority exercised by a commander over part of the activities of subordinate organisations, or other organisations not normally under his command, which encompasses the responsibility for implementing orders or directions. All or part of this authority may be transferred or delegated. (AAP-6)

Coordinating Authority
The authority granted to a commander or individual assigned responsibility for co-ordinating specific functions or activities involving forces of two or more countries or commands, or two or more services, or two or more forces of the same service. He has the authority to require consultation between the agencies involved or their representatives, but does not have the authority to compel agreement. In case of disagreement between the agencies involved, he should attempt to obtain essential agreement by discussion. In the event he is unable to obtain essential agreement he shall refer the matter to the appropriate authority. (AAP-6)

Host Nation
A nation which, by agreement:

a. Receives forces and materiel of NATO or other nations operating on/from or transiting through its territory;
b. Allows materiel and/or NATO organizations to be located on its territory; and/or
c. Provides support for these purposes. (AAP-6)

[1] JDP 0-01.1 '*United Kingdom Glossary of Joint and Multinational Terms and Definitions*', AAP-6 '*NATO Glossary of Terms and Definitions*'.

Host-Nation Support
Civil and military assistance rendered in peace, crisis or war by a host nation to NATO and/or other forces and NATO organizations which are located on, operating on/from, or in transit through the host nation's territory. (AAP-6)

Information
Information is the meaning that an individual associates with data, presented in context. Information combined with experience, interpretation and reflection, generates knowledge and thereby enables effective us of the information, in decision-making for example. (JDP 6-00)

Information Assurance
The confidence that the information within the Defence Community is maintained reliably, accurately, securely and is available when required. (JSP 440)

Information Exchange Requirements
Those categories of information that must be exchanged between operational facilities in order to provide commanders with essential information for decision-making. (JDP 6-00)

Information Exploitation
The use of information to gain advantage and improve situational awareness to enable effective planning, decision-making, and coordination of those activities required to realise effects. (JDP 6-00)

Information Management
Integrated management processes and services that provide exploitable information on time, in the right place and format, to maximise freedom of action. (JDP 6-00)

Information Superiority
Possessing a greater degree of information about the battlespace, being able to exploit the information more rapidly and preventing the adversary from obtaining or exploiting information which could give combat advantage. (JDP 0-01.1)

Integration
In CIS usage, the act of putting together, as a final item, various components of a system in such a way that the combination of separate systems, capabilities and functions can operate effectively, singly or in concert, without adversely affecting the other elements. (JDP 6-00)

Intelligence
The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organization engaged in such activity. (AAP-6)

Interoperability
The ability to operate in synergy in the execution of assigned tasks. (AAP-6)

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

Joint Operations Area (UK)
An area of land, sea and airspace, defined by 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. (JDP 0-01.1)

Joint Operations Area (NATO)
A temporary area defined by the Supreme allied Commander Europe, in which a designated joint commander plans and executes a specific mission at the operational level of war. A joint operations area and its defining parameters, such as time, scope of the mission and geographical area, are contingency-or mission-specific and are normally associated with combined joint task force operations. (AAP-6)

Joint Operations Picture
The total set of shared information on a particular operation, or Joint Operations Area, available through a secure information environment on CIS networks to support situational awareness and decision-making by UK commanders, and to facilitate information sharing with allies and partners. (JDP 0-01.1)

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

Mission
A clear, concise statement of the task of a commander and its purpose. (AAP-6)

Mission Critical Information
Mission Critical Information (MCI) is that information which is deemed critical to the business or operational needs of an organisation, requiring guaranteed delivery within a particular timescale, an audit trail, acknowledgement of receipt and alternate means of passing the information. MCI must be pushed to the action addressee and an acknowledgement of receipt must be achieved. The most likely method for dissemination, is published to the Web plus e-mail link, however, e-mail plus attachment with acknowledgement of receipt may be required when crossing system boundaries. (JDP 6-00)

Mission Support Information
Mission Support Information (MSI) is that information which is used to support the organisation, but does not require to be delivered within a specific timescale or require an acknowledgement of receipt. MSI should also be published to the Web to provide shared situation awareness. (JDP 6-00)

Operation
A military action or the carrying out of a strategic, tactical, service, training, or administrative military mission; the process of carrying on combat, including movement, supply, attack, defence and manoeuvres needed to gain the objectives of any battle or campaign. (AAP-6)

Operational Command
The authority granted to a commander to assign missions or tasks to subordinate commanders, to deploy units, to reassign forces, and to retain or delegate operational and/or tactical control as the commander deems necessary. Note: It does not include responsibility for administration. (AAP-6)

Operational Control
The authority delegated to a commander to direct forces assigned so that the commander may accomplish specific missions or tasks which are usually limited by function, time or location; to deploy units concerned, and to retain or assign tactical control of those units. It does not include authority to assign separate employment of components of the units concerned. Neither does it, of itself, include administrative or logistic control. (AAP-6)

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)

Situational Awareness
The understanding of the operational environment in the context of a commander's (or staff officer's) mission (or task). (JDP 0-01.1)

Standardisation
The development and implementation of concepts, doctrines, procedures and designs in order to achieve and maintain the compatibility, interchangeability or commonality which are necessary to attain the required level of interoperability, or to optimise the use of resources, in the fields of operations. (AAP-6)

Tactical Command
The authority delegated to a commander to assign tasks to forces under his command for the accomplishment of the mission assigned by higher authority. (AAP-6)

Tactical Control
The detailed and, usually, local direction and control of movements or manoeuvres necessary to accomplish missions or tasks assigned. (AAP-6)

TEMPEST
The investigation and study of unintentional emanations from classified systems. (JSP 440)

(INTENTIONALLY BLANK)

LEXICON OF ABBREVIATIONS

ACP	Allied Communications Publication
ACPT	Agency Contingency Planning Team
APOD	Airport of Disembarkation
ASSESSREP	Assessment Report
AWR	Alert Warning and Response
BM	Battlespace Management
BSM	Battlespace Spectrum Management
C2	Command and Control
CA	Comprehensive Approach
CBM	Command and Battlespace Management
CBSMC	Combined Battlespace Management Cell
CC	Component Commander
CCII	Command, Control, Information and Infrastructure
CCIR	Commanders Critical Information Requirement
CCT	Current Commitments Team
CDL	Common Data Link
CDM	Chief Defence Material
CDS	Chief of the Defence Staff
CESG	Communication Electronic Security Group
CIDA	Coordinating Installation Design Authority
CinC(s)	Commander in Chief(s)
CIS	Communications and Information System (s)
CJFO	Chief Joint Force Operations
CJO	Chief of Joint Operations
CJTF	Combined Joint Task Force (NATO)
CJTFC	Combined Joint Task Force Commander
CIMIC	Civil Military Co-operation
CLS	Contractor Logistic Support
CM(IS)	Capability Manager (Information Superiority)
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CoA(s)	Course(s) of Action
CoG	Centre of Gravity
Comd JFCIS	Commander Joint Force CIS
COG	Current Operations Group
COMPUSEC	Computer Security
COMSEC	Communications Security
CONLOG	Contractor Logistic

COS	Chief of Staff/Chiefs of Staff (MOD)
COTS	Commercial off the Shelf
CPT	Contingency Planning Team
CSO	Contractor Support to Operations
DA	Design Authority
D CBM	Director(ate) Command and Battlespace Management
DCDS(C)	Deputy Chief of Defence Staff (Commitments)
DCDS(EC)	Deputy Chief of Defence Staff (Equipment Capability)
DCIRT	Defence Computer Incident Response Team
DCMC	Defence Crisis Management Centre
DCMO	Defence Crisis Management Organisation
DCN	Defence Communication Network
DCM	Defence Crisis Management
DEC	Directorate of Equipment Capability
DE&S	Defence Equipment & Support
DFID	Department for International Development
DG Info	Director General Information
DG ISS	Director(ate) General Information Systems and Services
DG ISSP	DG ISS Publication
DIS	Defence Intelligence Staff
DM	Defensive Monitoring
DOA	Desired Order of Arrival
DOAST	Desired Order of Arrival Staff table
DOP	Defence and Overseas Policy
D Ops	Director Operations
DOWNREP	Down Report
DSF	Director Special Forces
D Strat Plans	Director Strategic Plans
EA	Electronic Attack
EBA	Effects-Based Approach
ECM	Electronic Counter Measure
ECM(FP)	Force Protection Electronic Counter Measure
ED	Electronic Defence
EEFI	Essential Elements Friendly Information
ELINT	Electronic Intelligence
EMCON	Emission Control
EME	Electromagnetic Environment
EMS	Electromagnetic Spectrum
EP	Electronic Protection
EPM	Electronic Protection Measure

ES	Electronic Support
ESM	Electronic Support Measure
EU	European Union
EW	Electronic Warfare
EWCC	Electronic Warfare Coordination Cell
FCO	Foreign and Commonwealth Office
FE	Force Element
FID	Force Instruction Document
FIS	Foreign Intelligence Services
FIT	Force INFOSEC Team
FLC(s)	Front Line Command(s)
FMB	Forward Mounting Base
FofS	Foreman of Signals
FOC	Full Operational Capability
FP	Force Protection
FRAGO	Fragmentary Order
FSG	Forward Support Group
GCO	Government Communications Officer
GII	Global Information Infrastructure
GOSCC	Global Operations Security and Control Centre
GSM	Global System for Mobile Communications
HF	High Frequency
HN	Host Nation
HNS	Host-nation Support
HQ	Headquarters
IA	Information Assurance
ICS	Information and Communications Services
IDS	Intrusion Detection System
IER	Information Exchange Requirement
IFA	Information Flow Analysis
IM	Information Management
INFOSEC	Information Security
Info Ops	Information Operations
IO	International Organisation
IOC	Initial Operational Capability
IP	Internet Protocol
IPT	Integrated Project Team
IS	Information Systems

ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
IX	Information Exploitation
JCB	Joint Coordination Board
JCP	Joint Contingency Plan
JCS	Joint Command System
JCISI	Joint Communications and Information Systems Instruction
JDP	Joint Doctrine Publication
JDLMO	Joint Data Link Management Organisation
JFAC	Joint Force Air Component
JFACC	Joint Force Air Component Commander
JFCIS	Joint Force CIS
JFHQ	Joint Force Headquarters
JFLC	Joint Force Land Component
JFLCC	Joint Force Land Component Commander
JFLogC	Joint Force Logistic Component
JFLogCC	Joint Force Logistic Component Commander
JFMC	Joint Force Maritime Component
JFMCC	Joint Force Maritime Component Commander
JFSFC	Joint Force Special Forces Component
JFSFCC	Joint Force Special Forces Component Commander
JHQ	Joint Headquarters
JOA	Joint Operations Area
JOCS	Joint Operations Command System
JOP	Joint Operations Picture
JOP	Joint Operational Standards
JPG	Joint Planning Guide
JRRF	Joint Rapid Reaction Force
JSyCC	Joint Security Coordination Centre
JSP	Joint Services Publication
Jt Comdr	Joint Commander
JTFC	Joint Task Force Commander
JTFHQ	Joint Task Force Headquarters
JTFHQ(A)	Joint Task Force Headquarters (Afloat)
KV	Key Variable
LO	Liaison Officer
MARBAT	Maritime Battlestaff
MCI	Mission Critical Information
MN	Multinational

MOD	Ministry of Defence
MODCERT	Ministry of Defence Computer Emergency Response Team
MOU	Memorandum of Understanding
MRC	Monitoring and Reporting Centre
MSE	Military Strategic Estimate
MSI	Mission Support Information
NATO	North Atlantic Treaty Organisation
NAVWAR	Navigational Warfare
NEC	Network Enabled Capability
NCC	National Contingent Commander
NETCEN	Network Centre
NGO	Non-Governmental Organisation
NSE	National Support Element
NSID	National Security, International Relations and Development
NTM	Notice to Move
OGD	Other Government Department
OLRT	Operation Liaison and Reconnaissance Team
OPCON	Operational Control
OPCOM	Operational Command
OPLAN	Operational Plan
OPORD	Operational Order
OPSEC	Operations Security
ORBAT	Order of Battle
OT	Operations Team
PFI	Private Finance Initiative
PM	Prime Minister
PME	Political/Military (Pol/Mil) Estimate
PMSC	Private Military Security Companies
POC	Point of Contact
PJHQ	Permanent Joint Headquarters
PSA	Political Strategic Analysis
R3	Reports Returns and Responses
RADSEC	Radiation Security
RATT	Radio Automatic Tele-Type
RFI	Request for Information
RFL	Restricted Frequency List
ROE	Rules of Engagement
RSOI	Reception, Staging, Onward movement and Integration

SA	Situational Awareness
SATCOM	Satellite Communications
SF	Special Forces
SFCC	Special Forces Component Commander
Sig Bde	Signal Brigade
SIGINT	Signals Intelligence
SIO	Senior Information Officer
SOFA	Status of Forces Act
SOI	Standing Operating Instructions
SoM	Scheme of Manoeuvre
SOP	Standard Operating Procedure
SOR	Statement of Requirement
SofS	Secretary of State
SPG	Strategic Planning Group
SPOD	Seaport of Disembarkation
SRM	Security Risk Management
TACOM	Tactical Command
TACON	Tactical Control
TDA	Theatre Distribution Authority
TDLA	Tactical Data Link Authority
TLMP	Through Life Management Plan
TSCMA	Technical Security Countermeasures Assessment
TTC	Telemetry Tracking and Control
UAV	Unmanned Aerial Vehicle
UKSF	United Kingdom Special Forces
UOR	Urgent Operational Requirement
USSO	Unified System Support Organisation
USUR	Urgent Statement of User Requirement
VTC	Video Teleconference
WAN	Wide Area Network
WARP	Warning and Reporting Point