



INFORMATION MANAGEMENT

Joint Doctrine Note
4/06

JOINT DOCTRINE NOTE 4/06
INFORMATION MANAGEMENT

Joint Doctrine Note (JDN) 4/06 dated June 2006,
is promulgated
as directed by the Chiefs of Staff



Director General
Development, Concepts and Doctrine

CONDITIONS OF RELEASE

1. This information is Crown copyright and the intellectual property rights for this publication belong exclusively to the Ministry of Defence (MOD). No material or information contained in this publication should be reproduced, stored in a retrieval system or transmitted in any form outside MOD establishments except as authorised by both the sponsor and the MOD where appropriate.
2. This information is released by the United Kingdom Government to a recipient Government for defence purposes only. It may be disclosed only within the Defence Department of a recipient Government, except as otherwise authorised by the MOD.
3. This information may be subject to privately owned rights.

AUTHORISATION

The Development, Concepts and Doctrine Centre (DCDC) publishes Joint Doctrine Publications (JDPs)/Joint Warfare Publications (JWPs) and maintains the hierarchy of these publications. Users wishing to quote JDPs/JWPs as reference material in other work should confirm with the DCDC Doctrine Editor whether the particular publication and amendment state remain extant. Comments on factual accuracy or proposals for amendment should also be directed to the Doctrine Editor at:

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

Telephone number: 01793 314216/7
Facsimile number: 01793 314232.
E-Mail: doctrine@dcdc.mod.uk

DISTRIBUTION

Distribution of JDPs/JWPs is managed by DSDC(L), Mwrwg Road, Llangennech, Llanelli, Carmarthenshire, SA14 8YP. Requests for this publication, or amendments to its distribution, should be referred to DSDC(L). All other DCDC publications, including a regularly updated CD '*Joint Doctrine Disk*' (containing both JDPs/JWPs and Allied Joint Publications (AJPs)), can also be demanded from DSDC(L).

Telephone number: 01554 822368
Facsimile: 01554 822350

All publications (including drafts) are available for viewing/download on the Defence Intranet: <http://chots.mod.uk/jointwar/index.htm>

PREFACE

1. **Purpose.** Joint Doctrine Note (JDN) 4/06 '*Information Management*' (IM) codifies emerging best practice and provides guidance on the management and exploitation of information resources to deliver operational advantage.
2. **Context.** 'Inform' is a key component of the Defence Capability Framework and Information is now recognised as a Defence Line of Development. The management of information to enable decision superiority¹ is essential. IM is a combination of procedures, training, behaviours and technology that, implemented efficiently, will deliver improved planning and execution of operations. The quantity of new information placed on systems increases by 30% annually, effectively doubling the available information resource every 3 years. Within Defence there is wide recognition of the need for IM but a risk of divergent approaches. This JDN is a step towards IM coherence.
3. **Structure.** This JDN comprises 7 sections. Section I introduces IM and expounds the context. Section II draws together a series of definitions and principles to bring a common language to the subject. Section III explores the output of IM, effective exploitation, and its lead of the IM process. Section IV deals with IM planning and framing information needs. Section V looks at information flow and Section VI the practices that underpin IM. Section VII looks at potential future developments.

LINKAGES

4. JDN 4/06 enhances the understanding of IM expressed in Joint Warfare Publication (JWP) 3-00 (2nd Edition) '*Joint Operations Execution*', JWP 5-00 '*Joint Operations Planning*', JWP 6-00 '*CIS Support to Joint Operations*' (2nd Edition) and Joint Discussion Note 4/05 '*The Comprehensive Approach*'. It sits alongside the Defence IM Handbook which provides more detailed understanding of information and IM.

¹ The UK Joint High Level Operating Concept (JHLOC) introduces the core concept of Inform to be 'decision superiority through shared situational awareness within task-orientated communities of interest that exploit collaborative processes in a single information domain'.

(INTENTIONALLY BLANK)

INFORMATION MANAGEMENT

CONTENTS

Title Page		i
Authorisation & Distribution		ii
Preface		iii
Contents		v
Joint Doctrine Publications		vi
Section I	Operating Environment	1
Section II	Information	1
Section III	Exploitation	8
Section IV	Information Needs and Planning	8
Section V	Information Flow	10
Section VI	Information Administration	14
Section VII	Future Developments	16

JOINT DOCTRINE PUBLICATIONS

The successful conduct of Joint operations requires intellectually sound, clearly understood and accepted doctrine that can be exploited by a nation and its likely partners, particularly in those situations associated with crisis and conflict. It is UK policy that national doctrine should be consistent with NATO doctrine, terminology and procedures (other than when the UK has elected not to ratify NATO doctrine). However, national doctrine should always cater for those areas not adequately covered by NATO doctrine, as well as influence the development of Allied doctrine. These requirements are met by the hierarchy of Joint Doctrine/Warfare Publications (JDP/JWPs).²

Interim Joint Doctrine/Warfare Publications (IJDP/IJWPs) are published to meet pressing new short to medium-term requirements for fully staffed and agreed Joint doctrine, often to deal with unexpected or unfamiliar circumstances and gaps in guidance. More short-term, urgent requirements for doctrine are published 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 establish the basis for further development and experimentation and provide a doctrinal basis for operations and exercises.

The Joint doctrine development process and the associated hierarchy of JDP/JWPs are to be found in Defence Instructions and Notices (DINs).

² JWPs are in the process of being renamed JDPs, as part of the review cycle.

SECTION I – OPERATING ENVIRONMENT

101. **Historical Environment.** Information, whether about own force dispositions, enemy intentions, meteorological predictions or orders, has always enabled command and control. Historically, commanders and their staffs have fought to obtain actionable information and hierarchical J1-J9 stove-piped staff procedures have evolved to deconflict, exploit, present and disseminate information in demanding operational environments. These legacy staff procedures have not yet been matched by equally disciplined procedures for the Information Age, characterised by massive volumes and flows of accessible and actionable information. In 2002, around 800 megabytes of new recorded information was produced per person in the world, equivalent to 100 books of written word, data and imagery. 92% of this information is stored on computer media.¹

102. **Network Enabled Capability.** Network Enabled Capability (NEC) should transform the means by which information can be exchanged, exploited and presented and enable more precise risk assessment and decision-making – by everyone.² It is intended to confer decisive advantage through the timely provision and exploitation of information, allowing effective decision-making and agile actions. Information flows over networks in ever-increasing volumes to wider audiences and in near-real time, offering both risk and opportunity; commanders need the right, assured, assessed and actionable information in time, and not simply an abundance of data. Above all, they should avoid the temptation of requiring too much data, leading to ‘analysis paralysis’.

103. **Technological Developments.** Currently, Defence uses a range of information systems, applications and platforms. Generally, interfaces have improved to the extent that information can flow directly between most systems, largely by e-mail with attachments. Developments should increasingly allow individuals on one system to have access to information across widely different networks.³ That said, security considerations and system constraints continue to prevent full connectivity and transparency being achieved within Defence, between Departments and between coalition partners.⁴ Ever-increasing Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) feeds, own-force tracking and tactical data links enable a near-real time operating picture, but the risk from Computer Network Attack is significant. The Information Age is far from mature and substantial management

¹ University of California, Berkeley, School of Information Management and Systems, ‘*How Much Information 2003*’.

² JSP 777 Edn 1, ‘*Network Enabled Capability*’, provides a coherent overview of NEC to a non-specialist reader.

³ DII(F) and (FD) should improve collaborative working and Meridio will improve electronic record management. The Joint Command and Control Support Programme (JC2SP) will enable real-time shared working and web browsing across the Joint Operational Command System (JOCS), the Royal Air Force Command and Control Information System (RAF CCIS) and the Royal Navy Command Support System (RNCSS).

⁴ Ongoing work on message and data exchange may lead to better automated information sharing across a coalition. At the same time, the use of a single mission language at the operational level will become essential.

challenges remain, including bandwidth availability, Information Management (IM) techniques and technologies, and Information Assurance (IA).

104. **Operational Environment.** The Effects-Based Approach⁵ (EBA) depends on the fullest achievable understanding and analysis of adaptive and complex situations. Collaborative working, supported by a Joint Operational Picture (JOP)⁶ and shared knowledge (in increasingly real time), should enable superior risk assessment and decision-making. Likewise, using rapidly accessed information, the tempo of decision-making at all levels may increase. The sheer breadth and depth of information available may, however, either facilitate or restrict freedom of action and the achievement of objectives in support of effects. Information sharing and effective IM should assist commanders in gaining and sustaining the initiative. Poor IM would contribute to increasing difficulty in discriminating actionable information from mounting clutter, the ‘e-fog of war’.

105. **Culture.** The best organisations consider information as a corporate resource, owned by the organisation, for use by all staff working towards a common goal. For NEC to deliver operational advantage, Defence should do likewise and accept that IM is a vital enabler for everyone from commander to ‘shooter’. With the volume of information available digitally expected to double every 3 years, the scale of the potential IM challenge will also demand a substantial change in organisational culture across Defence.

106. **Accountability.** The sinking of the Argentine cruiser General Belgrano in 1982, although lawful, prompted considerable debate on the lawfulness of such action. Since then, increasing Parliamentary and judicial scrutiny of the legality of UK Armed Forces’ activity, rebuttal, official inquiries and litigation have all demanded greater access to historical information. It follows that the information available to commanders should be preserved as part of our operational records and, eventually, public records. Although it may be exempt from subsequent disclosure on grounds of national security, such information may have to be disclosed under UK legislation such as the *Freedom of Information, Public Records and Data Protection Acts*. At the same time, due regard for the protection of intellectual property rights of others and the privacy of individuals, means that there will be circumstances where UK Armed Forces’ ability to gather and retain information will be closely regulated by law.

SECTION II – INFORMATION

107. **Information.** Data, information, knowledge and intelligence are inter-related manifestations of fact or perceived fact that have varying degrees of utility for

⁵ JDN 1/05 ‘*The UK Military Effects-Based Approach*’.

⁶ The JOP comprises JOPWeb and the Common Operations Picture. The former is web-enabled access to files. The latter is graphical in representation and includes environmental information and information that can be portrayed by position.

commanders and their staff. Data is the basic building block of information and comprises basic facts and statistics that can be manipulated by individuals or machines. 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 use of the information, in decision-making for example. One individual's knowledge becomes another's information, and thus information and knowledge, when presented, require managing through the same IM processes.⁷ In parallel, intelligence is an ability to acquire and apply knowledge. In military terms intelligence normally refers to information and knowledge on adversaries or potential areas of operation.⁸ Management of this intelligence is no different to the management of any other information.

108. **Definitions.**⁹ IM and its associated terms 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 (IX).** 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 (IAdmin).** 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 protection of information and information systems against attack, failure and compromise.

109. IM encompasses the joint enabling activity that underpins effective information exploitation and common situational understanding by commanders and staffs. Figure 1.1 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 itself comprises 3 parts:

- a. Determining information needs.

⁷ 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 JDN.

⁸ AAP-6 'NATO Glossary of Terms and Definitions' defines intelligence as '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'.

⁹ These definitions will be submitted for inclusion in JDP 0-01.1. 'United Kingdom Glossary of Joint and Multinational Terms and Definitions'.

- b. Managing information flow.
- c. Administration of information.

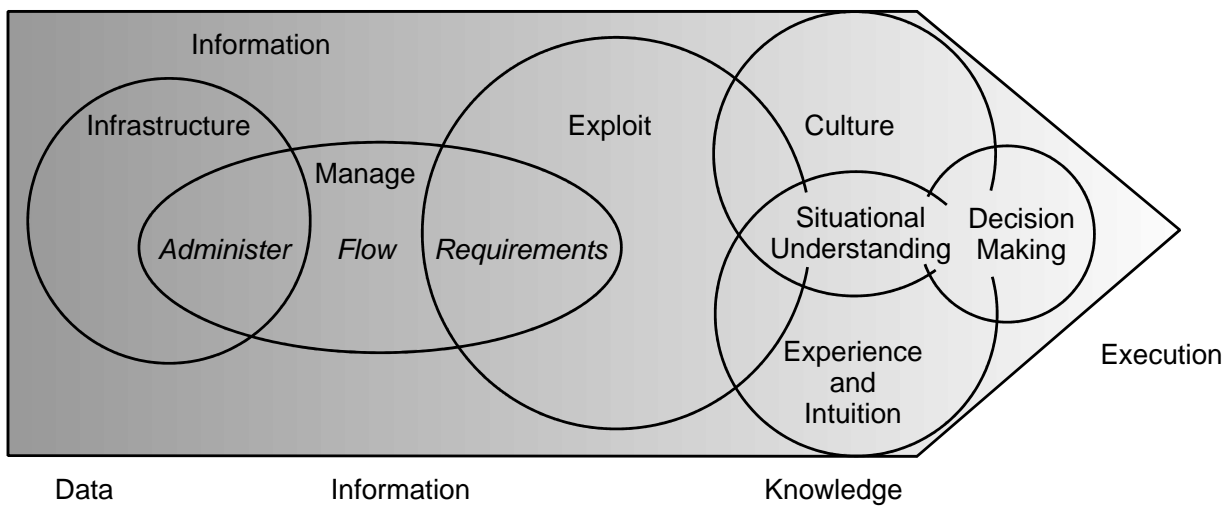


Figure 1.1 - The place of IM in Decision-making

110. **Information Life-Cycle.** Information, like any other commodity, has a life-cycle, demonstrated in Figure 1.2. On its journey, it can be exploited by a wide range of users, systems and platforms for differing reasons, many of which are not known to the originator. The cycle is not complete until information is discarded, archived or released into the public domain.

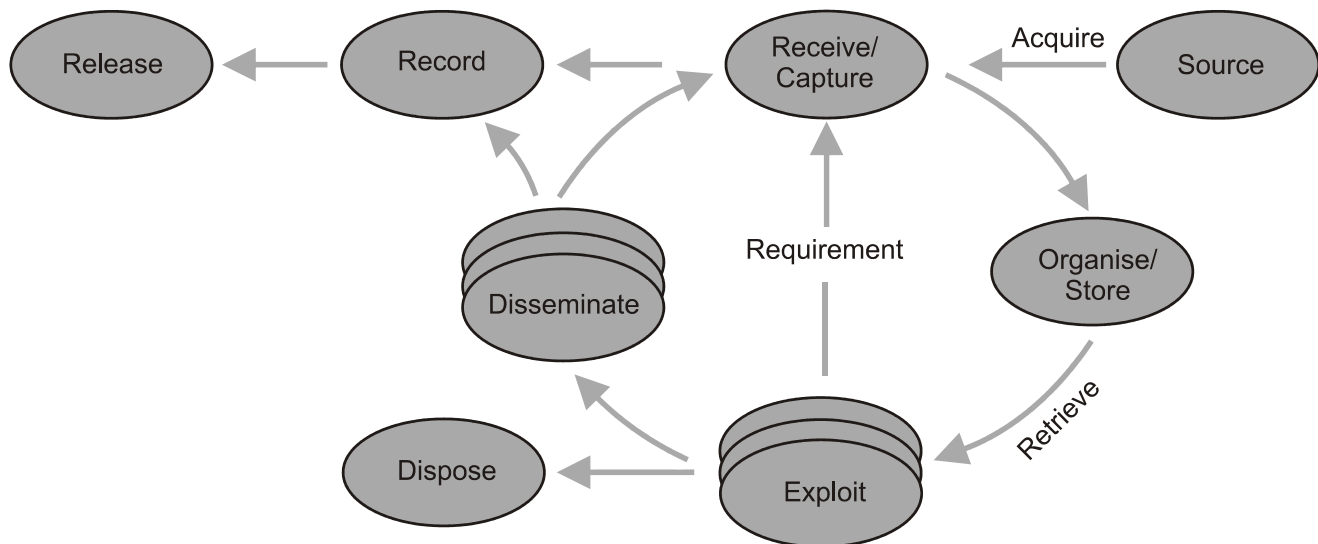


Figure 1.2 - The Information Life-Cycle

111. **Components of Information Management.** Figures 1.1 and 1.2 demonstrate that successful IM comprises a range of activities and behaviours. These are illustrated in Figure 1.3 and are applicable at all levels of warfare.

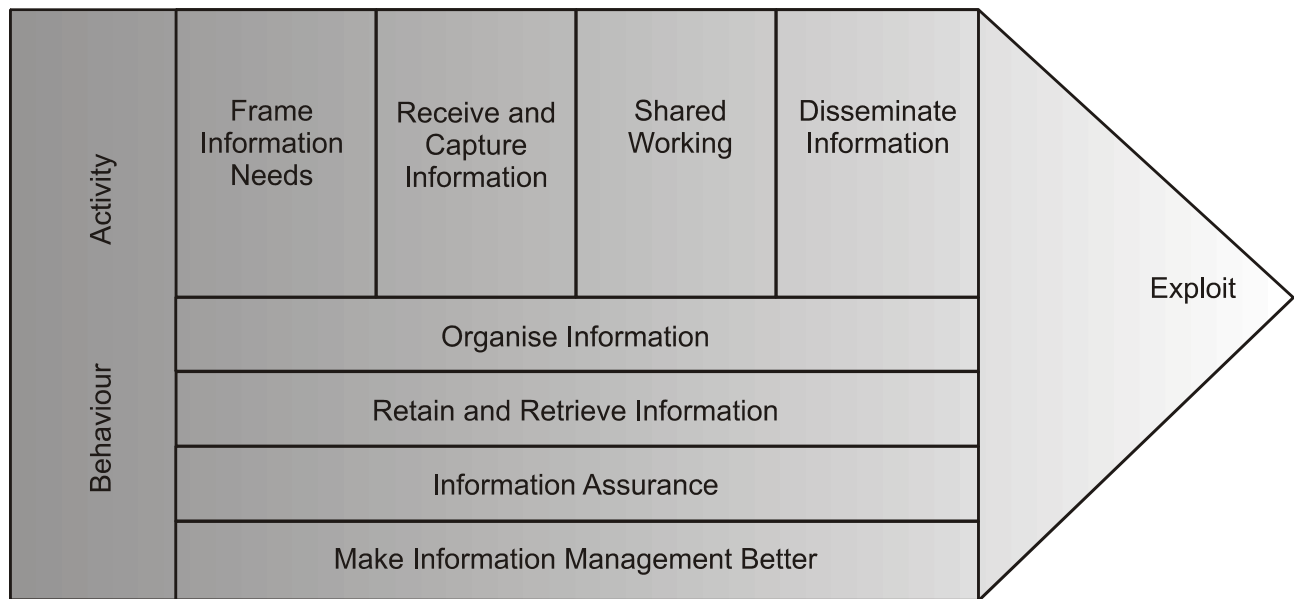


Figure 1.3 - Components of IM

112. **Information Categories.** Operational information covers a wide variety of subjects, including opposition forces, friendly forces, non-aligned/neutral forces, governance, administration, commercial, economic, humanitarian and health, environment, history and culture, law, infrastructure and information constituents of a society. Common information categories, which are not mutually exclusive, are:

- a. **Reference Information.** Reference Information is information that changes slowly over time, such as equipment support manuals or establishments.¹⁰
- b. **Environmental Information.** Environmental Information is the underlying or collated basic data that describes the physical environment, such as aeronautical, bathymetric, geospatial, hydrological, meteorological and oceanographic. Reference and Environmental information need to be coherent across Defence and be authoritative.
- c. **Mission Support Information.** Mission Support Information (MSI) is information that assists a commander and staff in planning and executing a mission.
- d. **Mission Critical Information.** Mission Critical Information (MCI) is information without which a commander cannot execute effective command. Rules of Engagement (ROE), answers to Commanders Critical Information Requirements (CCIRs), orders, tracking information and operational directives

¹⁰ The nascent Joint Reference Information Management Capability, FLEET Information Management Unit and Air Warfare Centre are examples of reference information providers. Their output has grown considerably in recent years.

are normally MCI. Intelligence, environmental information and other MSI may become MCI as appropriate.

e. **Record.** Documents or collections of documents produced, received, used or retained by organisations as evidence of their activities or to support decisions. A Record cannot be changed.

113. **Principles.** 12 principles reflect current thinking and provide a basis for IM:

a. Exploitation is enhanced by dynamic collaboration across organisational, geographical and national boundaries.

b. IM should be driven top-down and is everyone's responsibility.

c. Information needs should be identified against intended effects and objectives.

d. Information should be managed as a corporate asset and exploited to the advantage of the organisation not the individual.

e. Current information and records must be clearly distinguishable.

f. Information should have clearly defined ownership.

g. Information should be as widely available as possible.

h. Information should be created once and used many times.¹¹

i. Information should be managed in accordance with legal obligations and extant security requirements.

j. Common procedures and practices for the effective handling of information should, as far as practicable, be standardised across Defence, driven by the operational requirement.

k. Information that supports or disseminates operational decisions should be archived.

l. Information should be clearly labelled for subsequent retrieval.

114. **Governance Structure.** IM is a core staff activity requiring leadership and specialist support. A 4-tier structure in an organisation will enable this.

¹¹ In the deployed environment, integrity of information is important, the challenge of its maintenance across a wide range of systems, platforms and HQs across the Joint Operations Area (JOA) and the UK being considerable. A singular point of storage improves maintenance, but reduces assurance of availability.

a. **Senior Information Officer.** 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.

b. **Information Manager.** The Information Manager (IMgr) works to the SIO and sets in place the processes necessary to deliver the information requirements of the organisation. The IMgr writes and maintains the operational IM plan, manages information flow and coordinates and enforces IM activities on behalf of the SIO. Assistant information managers across an organisation will ensure local coherence with the plan and could double as branch watchkeepers providing local situational awareness.

c. **Information Hub.** An organisation's Information Hub (IHub) is the focus for IAdmin and exercises governance on behalf of the SIO and IMgr. It conducts a wide range of tasks including supporting users and team sites,¹² managing Electronic Ways of Working (EWoW), maintaining a guaranteed access point for messages, transferring information to the Record, providing local search expertise and managing profiles and accounts. An IHub is run by Information Support Officers (ISO) who understand the business of the organisation and are responsible for the administrative tasks that underpin IM. ISOs are information professionals in the same manner that registry and Communications Centre (COMCEN) staff have been previously, but are not system administrators. No single IHub construct will suit all scenarios; some organisations will opt for a centralised model, others dispersed.¹³

d. **Information Management Board.** An organisation's Information Management Board provides the means to bring J2, J3 and J6 staffs together with subordinate organisations to resolve IM issues across a Force during planning and the conduct of operations. A Board will continually look to improve IM.

115. **Culture and Training.** Maximising the benefits of information requires a culture of sharing and collaboration, and individual training in IM and the many tools available to assist situational understanding and IX. Operational IM procedures should be reflected in office procedures, allowing optimal connection and transition between the front line and supporting organisations.

¹² The terms 'team' and 'team sites' in this JDN are not system specific but refer to teams drawn together for a specific function. Often a team will be a staff branch or department.

¹³ IHub development is in its infancy and the competencies and training required to develop the skills are yet to be identified. It is clear that the competencies are different to those required by current registry staff.

SECTION III – EXPLOITATION

116. **Exploitation.** Exploitation is achieved by individuals and teams, supported by technology, who have a thorough understanding of the mission, commander's intent and desired end-state. Conceptually, exploitation can be broken down into a number of overlapping activities, to meet concurrent operational and tactical requirements:

- a. Analysis will result in the identification of information, tools and the team required to complete the task. The team will generate a shared understanding of the situation and desired end-state in order to work together towards a common purpose.
- b. Information will be assessed, fused, transformed and presented during the planning process. Decisions will provide the trigger for subsequent dissemination of direction and information for others to act upon.
- c. During execution, shared situational awareness will be instrumental to controlling activities and realising effects.
- d. Assessment will be continuous, providing information to support rolling analysis and planning.

117. **Situational Understanding.** The improved interaction of information, people, processes, experiences and culture, together promote shared situational awareness (for example the JOP), which in turn benefits situational understanding. Management of all JOP information across a Force is the primary IM function, aiming to ensure optimum data integrity at all levels of command whilst understanding its shortfalls and latency.

SECTION IV – INFORMATION NEEDS AND PLANNING

118. **Information Management Planning.** An IM Plan is derived from the Operational Estimate, the Permanent Joint Headquarters (PJHQ) 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 1.4. As IM becomes a core activity, properly reflected in Joint SOPs, so the IM Plan will increasingly focus on any necessary variations to these practised procedures. IM planning will specifically:

- a. Determine the information needs and outputs of the organisation, leading to a Joint Operations Area (JOA) information flow analysis. This in turn enables production of the Joint Information Exchange Requirement (IER)

and identifies changes to Reports, Returns and Responses (R3).¹⁴ Many information needs are standard and should be captured in Standing Operating Procedures/Instructions (SOPs/SOIs) but others will be operation-dependent and will need to be identified specifically.

- b. Provide input to the CIS estimate and to national/international system interface requirements, whilst taking account of CIS constraints.
- c. Determine changes to the IAdmin regime, particularly for coalition operations and taking account of the planned battle rhythm.

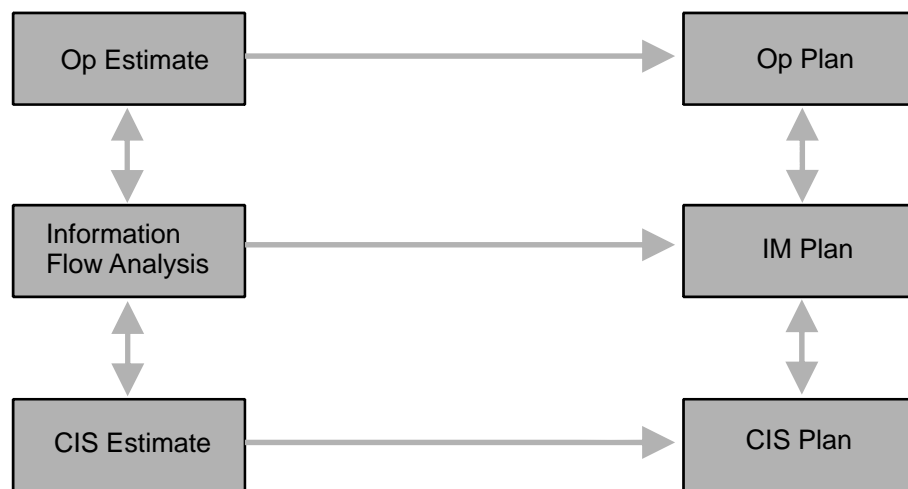


Figure 1.4 – Plans and Estimates

119. **Information Needs Analysis.** Information needs will 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 must 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 will require identification of:

- a. The content, format and timeliness of outputs necessary to deliver the effect, from formal directives through R3 to the JOP. Maintaining output currency may be a prime consideration, in which case modularity or use of databases may be preferable to single long documents.
- b. The membership of teams to deliver these outputs. Increasingly these will be cross-organisational rather than J1-J9 focused, in order to bring best expertise to bear.

¹⁴ R3 provide information to meet battle rhythm decision-making requirements. They are directed by the chain of command and increasingly can be automated or achieved through maintenance of common databases or publishing to the web.

- c. Information needs to service the 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.

120. **Agility.** Unresponsive operational plans, information clutter and lack of relevant actionable information will 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 to information and is fundamental to the achievement of agility.

121. **Coalition.** Information flow within a Coalition is constrained by immature system interfaces, language difficulties and security concerns. A Coalition will aim to operate a tiered structure of network domains interfacing through gateways that ideally allow information to be transferred automatically between partners. Particularly on enduring operations, a coalition network may be established for this purpose. Sharing information should only be limited by national security or release constraints. National SIOs must engage early with coalition partners to determine how and what information will flow across coalition interfaces. Where UK provides the operational lead, the senior deployed UK SIO takes responsibility for combined joint force information flow.

122. **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.

SECTION V – INFORMATION FLOW

123. **Information Flow.** This section examines the activities that individuals, teams and organisations need to undertake to acquire the information, receive and capture it within the organisation, work collaboratively and then disseminate tailored output effectively.

124. **Acquisition.** Once information needs have been determined (see Section IV), any information not to hand will have to be acquired in one of 3 ways:

- a. Retrieve information through searching and browsing available systems, whilst making use of contacts and subject matter expertise within an organisation or community of interest.
- b. Tasking subordinate organisations through standard processes, normally seeking a particular report or product including ISTAR outputs.
- c. Submission of formal Requests for Information (RFI). The established J2 CCIRM model¹⁵ provides effective management for Intelligence requirements; a force will need a similar process for non-intelligence RFIs. The IMgr must ensure the establishment and operation of an effective RFI process, including the extent to which RFIs can circumnavigate the chain of command to rear-based Mission Support Capabilities to access information and specialist advice quickly. RFI responses should normally be posted onto an accessible website and linked to the RFI register so that a wider audience can use the information.

125. **Receive.** Procedures must be in place to receive information into a headquarters, whether paper, voice or electronic. Timely notification of action addressees is essential and thus monitored group mailboxes should be the norm for e-mail in all operational organisations, and logs should be maintained for voice communications. MCI should be passed through IHubs to optimise tracking.

126. **Capture.** Received information must be captured and stored for subsequent exploitation. Paper documents should normally be digitised and records made of key information received by voice communications, maximising digital information availability. Headquarters staff will usually have access to 3 drives in each security domain: a personal drive, the use of which must be restricted to personal files only; a shared working drive on which all work in progress is conducted; a Record drive which is read-only and contains authorised, released files.

127. **Information Assessment.** NEC will provide access to sometimes contradictory information, particularly with increasing volumes of information over time and the use of the Internet. Information completeness, currency, accuracy, timeliness and relevance must be assessed by staff officers as part of its exploitation. Normally these assessments are based on experience and trust in the source, although in some cases measurements are applied, particularly to Intelligence.

128. **Shared Working.** Human interaction and shared working achieve 2 benefits: common situational understanding and tempo. Shared working is not restricted to a team within a single organisation but extends to intra-organisation teams.

¹⁵ JWP 2-00 (2nd Edition) 'Intelligence Support to Joint Operations' describes the CCIRM process.

a. **Collaborative Working.** Collaborative working is significantly enhanced by the use of information systems to share and exploit information whilst working with others in a team, potentially across many boundaries. Collaboration progressively adds value and deepens understanding and trust between participants. Meetings, voice, chat and Video Teleconferences (VTCs) are all part of process, but NEC provides greater opportunity to collaborate virtually with new tools being introduced to aid this. Collaborative working teams may be permanent or formed for a specific task, and each should have a shared working area on an appropriate system.

b. **Communities of Interest.**¹⁶ Communities of Interest provide sub-sets of the ‘share widely’ principle by enabling individuals to communicate within a functional area and have easy access to functional information. They also allow for compartmentalisation to meet security requirements by providing protected repositories of information from which appropriately authorised teams can draw. Communities may be drawn from differing levels of command, across Components and mission support capabilities, and could include ISTAR, Targeting, Media Operations, Information Operations, Battlespace Management, Airspace Control and Explosive Ordnance Disposal.¹⁷ Communities should be moderated¹⁸ and IM, security and CIS plans should take them into account.

129. **Information Sharing.** Information will be of use to a wide range of users, potentially for exploitation in a variety of unanticipated ways, and must be shared within the bounds of necessary security. The cultural corollary of this duty to share is that superior headquarters should avoid ‘the long handled screw-driver’. If increasing situational awareness produces a tendency for interference then information flow may quickly be limited by restrictive access permissions. It is helpful to consider 5 different potential users of information. The *involved* are those individuals and teams directly using the information. The *interested* will have oversight of the work or will contribute to it in some way. Others need to be *informed* as it may impact on other workstrands, and greater situational understanding can be provided to the *inquiring*. Lastly, there are those that must be *excluded*. Team leaders must balance sharing with security, and also avoid potential confusion between access to information still ‘in-work’ and completed, authorised, output. During planning activity, access might be limited to the involved and interested. Once approved and published, a plan for example might be released to the informed and then during execution also to the *inquiring*.

¹⁶ Joint HLOC Chapter 5 introduces the concept of Communities of Interest.

¹⁷ There are many examples of communities of interest on the internet. Perhaps the best known within the military are the ‘British Army Rumour Service’, ‘Rum Ration’ and the pilots professional community, ‘PPRuNe’.

¹⁸ A Community of Interest may extend from strategic to tactical level. The moderator will police the community, ensuring that information is relevant and maintained and does not abuse accepted freedom from the formal chain of command.

130. **Disseminate.** The owner is responsible for ensuring that information reaches the appropriate audience in an exploitable format, on time and taking account of communications availability, the need for acknowledgement, timeliness and replication means. Format requires thought; good presentation of information enables its use whilst poor design may prevent its use. Dissemination can take several forms:

- a. Publishing to the organisation's web supported by a message to those that must action it.
- b. Message with attachment or hyper-link.
- c. Electronic media¹⁹ and paper graphics or documents, particularly when passing information to civilian communities, Non-Governmental Organisations (NGOs) and across some parts of a coalition or when file sizes are particularly large.
- d. Voice.²⁰
- e. Databases²¹ or spreadsheets that are treated as any other electronic file but ownership of information can be widespread. The updating of such files can constitute dissemination.

MCI requires delivery assurance through manual or automatic acknowledgement and should be either sent directly, or pushed, to appropriate addressees or made available through a web-portal²² supported by an acknowledged message. MSI would normally be published to the web.

131. **Web Portals.** Access to information at the operational level should normally be through web portals, with links to documents in shared working and Record drives. Several ground rules will help the retrieval of information from web sites:

- a. Intuitive web design based around the operation should take users quickly to team or community of interest pages.
- b. MCI should be accessed easily through the organisation's front-page with changes being flagged up and therefore immediately obvious. Generally MSI and MSI changes will be accessed through subordinate team-sites.

¹⁹ This includes broadcast communication systems such as the Pilot Digital Broadcast System.

²⁰ The power of the spoken word in command will remain fundamental. To quote General Walker in '*RUSI Journal February 2001*' 'While talking they can convey passion, sarcasm, equivocation, subservience, and exhaustion all with the exact same words'.

²¹ Joint databases might include J3 Targets, J2 CCIRM, infrastructure, RFIs, and the Joint Lessons Identified Database (JLID).

²² JOPWeb and Allied Rapid Reaction Corps Web (ARRCWeb) use web technology to support the dissemination of information for specific operations in web form.

- c. Users should make use of automated alerts for content change of key web pages, where facilities allow.
- d. Team sites must have a site manager responsible for policing content for the team and all web pages should have an owner detailed on the page.
- e. Currency must be maintained if confidence in the site is to be retained.

SECTION VI – INFORMATION ADMINISTRATION

132. IAdmin encompasses all the staff processes necessary to organise, store, maintain, access, communicate and facilitate the use of information in a collaborative environment. Software tools may make IAdmin increasingly user-friendly, but organisational and individual culture and discipline, and structured procedures, will remain essential cornerstones. All individuals have IAdmin responsibilities.

133. **Organise.** Information should be organised in accordance with widely understood and enforced IM rules. Some of these will be mandated by Joint Service Publications (JSPs),²³ others mandated in local SOPs.

a. **Labelling.** Labelling is the single most important IAdmin action. All information, whether held as a Record, as a working document or within a database, must be labelled to allow subsequent retrieval using search tools. The information in such labels, known as metadata, must include title, creator, date, subject and protective marking. It may also include other information including release constraints, required retention period and version control. Subject metadata comprises key words, selected from a controlled vocabulary known as taxonomy, against which retrieval searches can be conducted. The UK Defence Taxonomy provides a start point, supplemented by standard operational writing abbreviations, JDP 0-01.1 '*United Kingdom Glossary of Joint and Multinational Terms and Definitions*', and Geographic Gazetteers. Where new words are needed for local taxonomies, the IHub must record these and ensure onward passage to MOD DG Info for inclusion in the Defence Taxonomy. To be clearly understood in comprehensive and coalition environments, taxonomies should use Concise Oxford English Dictionary words and definitions.

b. **Structure.** The organisation's information storage capacity must be structured to ensure maximum accessibility to information both internally and externally, provide necessary security controls and be resilient. Drive and folder structures should be intuitive to use, adaptable and differentiate between

²³ JSP 717 provides policy for managing, maintaining and using metadata (labels) as defined by the MOD Metadata Standard. JSP 441 gives guidance on Records management.

team working areas and the read-only Record. Design of the structure is an IMgr responsibility with maintenance and policing provided by the IHub.

c. **Track.** Tracking ensures that information is in the right place at the right time. For MCI the originator has responsibility until a receiving organisation acknowledges receipt, at which point internal tracking procedures must ensure it is actioned by appropriate individuals. RFIs also should be managed and tracked by designated RFI managers.

134. **Retrieve.** To retrieve information, users must be able to use labelling schemes and search engines. The use of subject matter experts, communities of interest and IHubs can help locate information when individuals cannot or where greater clarity or additional value is required.

135. **Retention.** Once work on a task is complete and the output authorised, the information becomes a Record along with any information supporting a commander's decision that has led to the output. It is transferred to the organisation's Record where it can no longer be amended. Periodically the Record must be reviewed and information disposed of or transferred to the Defence Archive under rules laid out in JSP441. Once in the Defence Record, it will also remain available to those on operations and for operational analysis.

136. **Ownership.** Information is a corporate asset but for reasons of trust, maintenance and accountability must have an owner. The owner is responsible for maintenance of the information (its currency, ensuring that it is shared, stored and labelled correctly) and observation of security and release constraints. Ownership can transfer. Prior to designation as a Record, working information is owned by the individual, team leader or branch head, who retains responsibility for its authority and for sharing it appropriately. Once in the Record the IMgr takes ownership on behalf of the SIO although the original owner retains responsibility for ensuring relevant updates are available. In the Defence Archive, it is owned corporately by the MOD.

137. **Operational Record.** Commanders at all operational levels must retain an operational record, effectively the diary. This is best achieved as a rolling document listing key events and decisions with linked supporting files. Responsibility for production of the operational record must be clear and the nominated individual have full access to the decision-making process.²⁴ This is particularly applicable to UK Resilience Operations where much information will become a legal record or evidence. Legal and police advice will be required in the preservation of such evidence to prevent the loss of this information to commanders and staffs.

²⁴ Single Service direction covers command-led RN, Army and RAF Operational Record procedures. Similar formal procedures do not exist in the Joint arena, although the Chief of Joint Operations and Joint Task Force Commanders are responsible for keeping operational records and receive support from DG Info staff to accomplish this.

138. **Assurance.** IA requires a management process to ensure that the systems and networks employed to manage the critical information used by an organisation are reliable and secure, and that measures and processes are in place to counter malicious activity in order to support the business needs of the organisation. It encompasses the related discipline of information security management and relies on effective risk and business continuity management. Organisations must plan IA against the criticality of information and plans be coordinated across J2, IM and J6 functions.

- a. Protection of systems and information is an established security function,²⁵ with appropriate actions the responsibility of all users.
- b. Availability is assured through effective IM and robust CIS processes including IMgr-directed back-up policy, frequently updated local copies of web sites, local storage of MCI and redundancy in the CIS architecture.
- c. Confidentiality is achieved through a mixture of security procedures, system gateways and by restricting access to information, especially during planning.
- d. Integrity is achieved through avoidance of information-corruption. Corruption could be malicious or through use of poor quality source information. Risk of the latter is minimised by using trusted sources and seeking subject matter expertise should clarification be required. Information assessment by individuals is the first line of defence.
- e. Organisations must maintain a planned and tested reversionary capability to ensure access to information necessary for the conduct of operations should systems fail.

SECTION VII – FUTURE DEVELOPMENTS

139. **Comprehensive Approach.** Defence will need to establish an approach to developing IM capability to meet the demands of strategic, operational and tactical levels within a CA. It will need to breach inter-Department and agency cultural and technical boundaries and take account of the discrete characteristics of systems,²⁶ capacity (both human and technical) and sophistication of each individual area.

140. **Technology.** Computer-processing power in 2018 is predicted to be around one thousand times greater than in 2006 and the volume of information available digitally will be about 15 times greater. In the short-term, current systems will transition to applications hosted on a common infrastructure. This rationalisation and

²⁵ JSP 440 *'The Defence Manual of Security'*.

²⁶ Systems interoperability is restricted by the protective level at which different Departments work. Effective system interfaces to allow information sharing and collaborative working must be seen as an early goal, requiring a Cabinet Office lead.

the development of core Defence IM capabilities will enable more effective IX. Increasingly automated IM capabilities should then deliver common, application-independent services over a seamless infrastructure.²⁷ Smart IM services could maximise automation and improve search capabilities, perhaps automatically serving relevant information to individual users all of who have a personalised ‘home page’. The NEC Transitional Epoch is characterised by improved integration in which, from the user’s perspective, the whole system functions as if it were a single unit. IM techniques will increasingly encompass new, IM-specific, technology applications.²⁸

141. **Culture.** Culturally there is still much to change. The IM doctrine set out in this JDN is a beginning but can only be fully realised and developed further if IM is embraced comprehensively across Defence. It requires top-down commitment, universal adoption of staff procedures at every level,²⁹ and the integration of IM into routine individual staff and headquarters training.

142. **Information Exploitation Programme.** DG Info’s current IX Programme will deliver a set of Defence IM Policies and Protocols and identify IM-specific competencies and associated training requirements, such as the new IM/IX Courses at the Defence Academy.

143. **Role of Development, Concepts and Doctrine Centre.** The Development, Concepts and Doctrine Centre (DCDC) views IM as a critical part of delivering operational success. To develop this theme, DCDC intends to:

- a. Produce an Inform Interim Concept expanding on the high level operating concepts in ‘*UK Joint High Level Operational Concept*’ (JHLOC).
- b. Include IM in the relevant 2, 3, 5 and 6 series Joint Doctrine Publications (JDP). Feedback to this JDN will help determine the need for a stand alone IM JDP.
- c. Observe and influence development of IM at the operational level on operations and exercises, and to develop doctrine accordingly.
- d. Capture and exploit multi-national and cross-Department thinking, including through the Multinational Experiment series.

²⁷ The Equipment Capability approach to realising an IM capability places the organising of information at the core of the IM process. An Information Catalogue should provide this core element through the application of common metadata standards to all information. Surrounding this core, common information requirements management, information repositories and information maintenance services are all essential. However, equipment alone will not result in an IM capability unless there is a corresponding contribution across other Lines of Development.

²⁸ As a commercial example, Google is the World’s most used search engine. Google also develops and markets a wide range of other IM/IX technologies and services to meet its mission, ‘*to organise the World’s Information*’.

²⁹ JSP 101 ‘*Defence Writing Guide*’ could be amended to include the basics of metadata, as a documents label must be seen as part of the document not an optional extra.

(INTENTIONALLY BLANK)