MINISTRY OF DEFENCE

Joint Doctrine Publication 2-00

Understanding and Intelligence Support to Joint Operations

Third Edition

DCDC

Development, Concepts and Doctrine Centre

JOINT DOCTRINE PUBLICATION 2-00

UNDERSTANDING AND INTELLIGENCE SUPPORT TO JOINT OPERATIONS

Joint Doctrine Publication 2-00 (JDP 2-00) (3rd Edition), August 2011
is promulgated as directed by the Chiefs of Staff

Assistant Chief of the Defence Staff (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
Military Network: 96161 4216/4217
Facsimile number: 01793 314232
Military Network: 96161 4232
E-mail: dcdc-doceds@mod.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 on the Defence Intranet (RLI) at: www.dcdc.dii.r.mil.uk

This publication is available on the Internet at: www.mod.uk/dcdc

PREFACE

'*Nothing is more worthy of the attention of a good general than to endeavour to penetrate the designs of the enemy*.'[1]

Niccolo Machiavelli

1. The traditional military focus for understanding was identifying and knowing about adversaries in order to neutralise or defeat them. Militaries are generally very good at developing this knowledge, particularly identifying capabilities, military infrastructures, human geography, patterns and types of forces. What modern militaries are not good at is understanding the psychological and cognitive aspects that shape the fears, motivations and perceptions of an adversary and the plethora of other surrounding actors who influence them or they influence. The reality of the contemporary operating environment is that although it remains their primary mission, it is no longer sufficient for the military to focus on adversaries in isolation. Modern operations demand a broader understanding of the operating environment, sub-environments and various networks that exist within them.

2. JDP 2-00 (3rd Edition) *Understanding and Intelligence Support to Joint Operations* emphasises the increasingly cross-governmental nature of intelligence and the need to inculcate a spirit of collaboration, including with partners and allies. It assumes that in the 21st Century, we will conduct intelligence in an inter-departmental and inter-agency context. This will involve integration and co-operation between government departments and the UK intelligence community. An enduring aspect of this approach is that commanders at all levels will still need accurate and timely intelligence to inform their decision-making, but they must know and understand their own role and that of their staff in developing and delivering it.

3. This document is written with 4 audiences in mind. Primarily, it informs senior commanders how their intelligence staff should work to support their decision-making. Secondly, it provides the opportunity for commanders at all levels to gain an understanding of the value of intelligence and the intelligence process. Thirdly, it provides a principal reference document for intelligence specialists on which subordinate documents can be based. Finally, it provides external readers an explanation of MOD intelligence functions.

4. JDP 2-00 (3rd Edition) outlines the theory, principles and guidelines for intelligence using 6 core themes throughout the document:

---

[1] *The Historical, Political, and Diplomatic Writings,* Volume 2, Chapter XVIII *The Prince, Discourses on the First Ten Books of Titus Livius, Thoughts of a Statesman* 1513.

The centrality of influence and understanding
The importance of cultural awareness
The importance of intelligence exploitation
Interagency co-operation and common operating procedures
The relationship between the commander and the intelligence staff
Intelligence in the contemporary operating environment

5. **Structure**. JDP 2-00 is divided into 6 chapters:

a. Chapter 1 provides the strategic context and describes a contemporary approach to understanding and intelligence.

b. Chapter 2 explains the fundamentals of intelligence and their application.

c. Chapter 3 explains the development of intelligence and the application of the intelligence cycle.

d. Chapter 4 explains intelligence support to joint operations.

e. Chapter 5 explains how understanding and intelligence support is enabled.

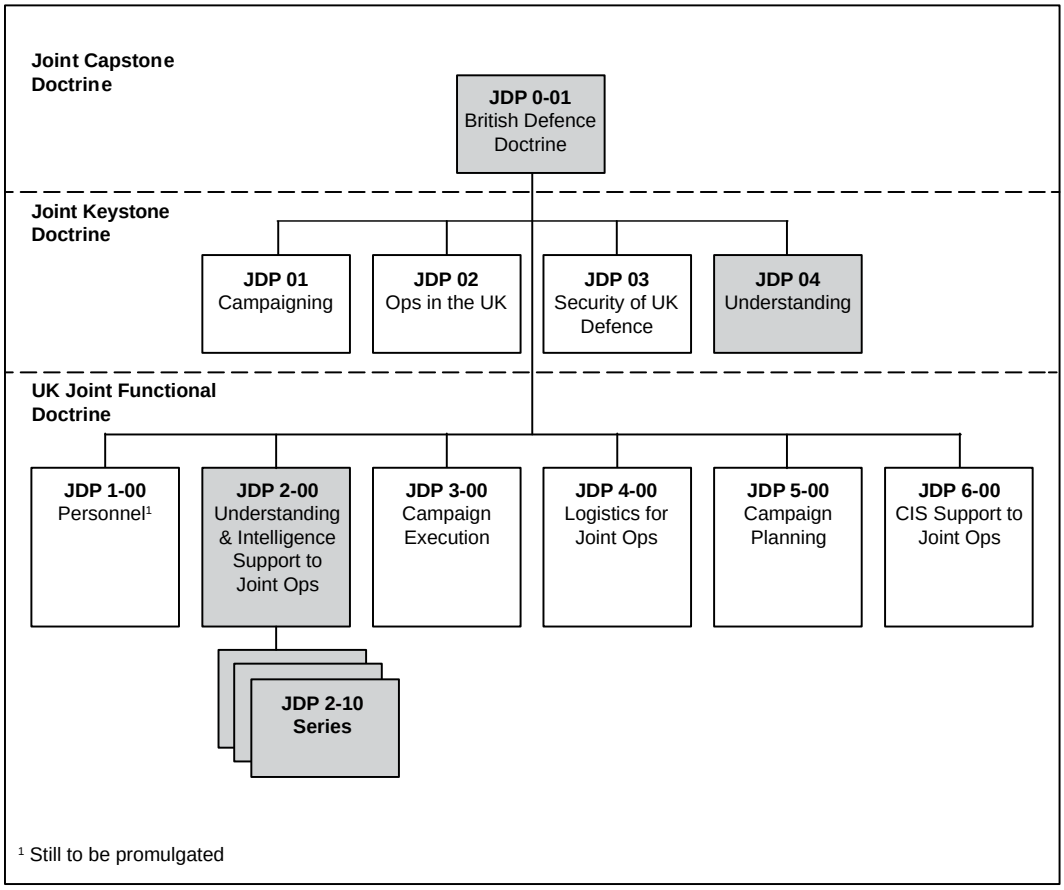
f. Chapter 6 explains intelligence support to the joint operational planning process.

LINKAGES

6. JDN 1/10, *Intelligence and Understanding* has been subsumed into this edition of JDP 2-00 and is therefore withdrawn. JDP 2-00 is intended to be read in conjunction with JDP 0-01 *British Defence Doctrine* (3rd Edition) which it supports and JDP 04 *Understanding*. It should also be read in conjunction with NATO Allied Joint Publication-2 *Joint Intelligence, Counter Intelligence and Security Doctrine*. It is linked with JDPs 01 *Campaigning* (2nd Edition), 3-00 *Campaign Execution* (3rd Edition), 5-00 *Campaign Planning* (2nd Edition), as well as JDNs 2/09 *Materiel and Personnel Exploitation* and 3/11 *Decision Making and Problem Solving: Human and Organisational Factors*. JDP 6-00

Communications and Information Systems Support to Joint Operations (3rd Edition) provides additional detail on information management as well as communications and information systems. While JDP 3-40 *Security and Stabilisation: The Military Contribution* provides guidance on the application of understanding within the stabilisation and counter-insurgency environments.

7. **The JDP 2-10 Series**. JDP 2-00 is written primarily for generalists. It should be understood by commanders, staff officers and personnel working within the joint operational staffs. It is impossible to convey all of the complexities of intelligence for specialists in JDP 2-00. Therefore, a supporting series of specialist intelligence documents, the JDP 2-10 series, provides this specialist guidance. Shown below is the hierarchy of intelligence doctrine and JDP 2-10 series:



JDP 2-10 Series			
2-10.1	Intelligence Requirements and Collection Management	2-10-6	Materiel and Personnel Exploitation
2-10.2	Counter-Intelligence	2-10.7	Measurement and Signature Intelligence
2-10.3	Human Intelligence		
2-10.4	Signals Intelligence	2-10.8	Open Source Intelligence
2-10.5	Geospatial Intelligence and Imagery Intelligence	2-10.9	All Source Intelligence
		2-10.10	Cultural Capability

(INTENTIONALLY BLANK)

CONTENTS

CHAPTER 1 – A CONTEMPORARY APPROACH TO UNDERSTANDING AND INTELLIGENCE

'*All the business of war, and indeed all the business of life, is to endeavour to find out what you don't know from what you do*.'

The Duke of Wellington

Chapter 1 explains the strategic context and the challenges for intelligence in the contemporary operating environment. It also explains the understanding and intelligence framework used throughout this publication.

SECTION I – THE STRATEGIC CONTEXT

101. The changing character of conflict emphasises the need to place intelligence within the wider concept of understanding, where commanders must seek a deeper penetration of the human domain in which adversaries and other actors will compete with and confront each other.[1] Intelligence is not only a tool for counting the forces of adversaries or assessing their preparedness to engage in conflict. Intelligence is an enabling capability whose value is largely realised through the activities of the whole of Defence from *Whitehall to War-fighter*.[2] It enables the focused application of military power in support of the UK's national interests.

102. Intelligence is crucial to the development of understanding. It requires systems, architectures and practitioners flexible enough to operate in complex environments and a command climate that promotes collaboration and creates the organisational structures required to achieve fusion at the point of need.

103. The National Security Strategy (NSS) defines the UK's strategic context that drives the nature and scope of that intelligence support. It provides the strategic vision and defines our national interests. The UK's interests centre on the security of our nation (the first duty of government) as the foundation of our freedom and prosperity.[3] The quinquennial Strategic Defence and Security Review (SDSR) informed the military tasks, size, shape and preparation of our armed forces,

[1] The term *commander* describes the authority at any level for whom intelligence is produced.
[2] *Intelligence Sub-Strategy for Defence* dated 23 April 2010.
[3] National Security Strategy 2010: *A Strong Britain in an Age of Uncertainty*, 18 October 2010.

including how they develop their understanding and operate with other agencies to support national interests. The NSS and SDSR define the operating environment, priorities, where the main effort should be, priorities for capability development and the planning assumptions. Most importantly, they provide the military tasks outlined in Figure 1.1.

Providing strategic intelligence	Support to horizon scanning Support to the development of situational awareness Support to policy and strategy formulation as well as contingency planning
Providing nuclear deterrence	Maintenance of the UK's nuclear deterrence: the ultimate guarantor of the UK's security in a nuclear world
Defending the UK and its Overseas Territories	Steady-state and crisis joint operations in the UK and overseas territories Defence contribution and support to homeland security Homeland defence
Supporting civil emergency organisations in time of crisis	Support under the framework of Military Aid to the Civil Authorities (MACA)
Providing a Defence contribution to UK influence	Support to national influence goals and operations
Defending UK interests by projecting power strategically and through expeditionary interventions	Strategic and operational intelligence Maintenance and development of the appropriate military capability
Providing security for stabilisation	Provide the military contribution to stabilisation within the context of the *JIIM*[4] environment

Figure 1.1 – The UK Military Tasks from NSS and SDSR

[4] Joint, Inter-Agency, Intergovernmental and Multinational.

The Nature of Adversaries in the 21st Century

'*Hezbollah is not your father's terrorist organisation. This is not a group of loosely affiliated cells of would-be hijackers or suicide bombers. Hezbollah is a terrorist army, trained like an army, organised like an army, funded and equipped like an army.*'

Israeli Officer's Assessment after the July War 2006

SECTION II – THE IMPLICATIONS FOR UNDERSTANDING AND INTELLIGENCE IN THE CONTEMPORARY OPERATING ENVIRONMENT

104. **The Contemporary Operating Environment**. The Development, Concepts and Doctrine Centre's (DCDC's) report on Global Strategic Trends and the Future Character of Conflict explains in detail the nature, character and perceived future challenges of the contemporary operating environment.[5] Commanders should recognise that developing understanding based on intelligence is still critical for effective decision-making, needing careful allocation of resources to achieve the mission.

105. **Key National Challenges**. The likely challenges in the first half of the 21st Century are:

a. **Terrorism**. Terrorism is defined as *the unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives*.[6]

[5] For further details, see MOD's Strategic Trends Programme *Future Character of Conflict* (FCOC) and *Global Strategic Trends-Out to 2040* (4th Edition) promulgated by DCDC.
[6] Allied Administrative Publication (AAP)-6 the *NATO Glossary of Terms and Definitions*.

b. **Hostile States**. Hostile states are those states characterised by enmity or ill-will towards the UK, its allies or the balance of international order. Hostility can be either open (verbal or violent aggression or belligerence) or disguised and can be conducted by proxy.

c. **Fragile and Failing States**. States that cannot adapt to the changing global context risk collapse and for many such failures are likely to be accompanied by substantial outbreaks of violence. Poor governance, economic deprivation and inequality that characterises failed and failing states is likely to spread to neighbouring states.[7]

d. **Hybrid Adversaries and Threats**. Hybrid threats occur where conventional, irregular and high-end asymmetric threats are combined in the same time and space.[8] Conflict could involve a range of trans-national, state, group and individual participants operating both globally and locally. In some conflicts, concurrent inter-communal violence, terrorism, insurgency, pervasive criminality and widespread disorder are likely.

This list is not exhaustive, but it represents the most challenging operations. The military contribution to understanding, at both the national and military level, is to help develop the *insight* and *foresight* to interpret and anticipate the nature of these challenges, being prepared to deploy the right military capability at the right time.

106. **Operating in Complexity**. While state-versus-state conflict is still possible, contemporary operations are likely to be more complex and adversaries could be more difficult to identify. Increasingly we live in a world of *wicked problems*, which are so complex that they defy process-driven, management or scientific approaches.[9] This does not mean that they are unsolvable, but the approach must be open-minded, agile, flexible and adaptable to work through the complexities. Joint Doctrine Publication (JDP) 04 *Understanding* Chapter 4 describes this complexity and forms the basis of the principles of intelligence in Chapter 2.

107. **The Single Information Space**. Information is unprocessed data of every description that is used in our normal Defence business and on operations, and specifically in the production of intelligence. Within

[7] FCOC, page 5.
[8] *Ibid*, page 13.
[9] The term *wicked problem* was introduced by Horst W J Rittel in a 1967 lecture, and subsequently elaborated more fully in collaboration with M W Webber in their *Dilemmas in a General Theory of Planning*, Policy Sciences, Volume 4, 1973, pages 155-169.

Defence, there is only one information space: the world in which we live. Defence makes no artificial distinction between the business and operational domains. It achieves access to the information space by a combination of people, processes and technology.

108. **The Requirement to Understand**. It is no longer sufficient just to know about adversaries and their capabilities, although identifying, neutralising or defeating adversaries remains the primary military focus. There is a need to understand the context within which our adversaries operate, the institutions within which they live and detailed information about their cultures, fears, perceptions, motivations and history. Described within JDP 04, the human domain framework includes the totality of the human sphere of activity or knowledge, and concerns the interaction between humans and their broader environment. The focal point for understanding is the role of people as actors on the global stage in their identities as states, non-state actors, populations, organisations, groups or individuals. At the very least, actors must be considered within their cultural, institutional, technological and physical environments to provide the context for developing understanding. The challenge for commanders is to develop the structures and networks that allow us to understand the totality of the human domain. This sets a requirement for contextual intelligence and a dynamic approach to developing and using networks. Chapter 4 considers the concept of the human domain in more detail.

109. **The Requirement for Contextual Intelligence**. The complexity of modern operations produces a greater need for contextual intelligence, which uses a wide range of sources to develop understanding of the operating environment. This relies upon geospatial, cultural and linguistic capabilities for information collection and the subsequent processing into intelligence. The implications for commanders are that some intelligence staff may need context-specific training and that continuity within the intelligence staff is a prerequisite to effective intelligence assessments.

110. **A Dynamic Understanding and Intelligence Network**. Dynamic and flexible networks, which can adapt to changing requirements, are required to produce contextual intelligence. This requires intelligence staff to consult with subject-matter experts and a variety of specialists, including those living within the affected nation. Examples include:

a. Anthropologists and sociologists who can provide assistance in understanding tribal dynamics and human factors.

They can also support key leadership engagement or the building of relationships.

b. Geographers, academics or other government departments, which have a detailed or long-standing knowledge, can provide advice on a particular region or country.

c. Industry experts who can provide insight into particular industrial processes that underpin an adversary's capability.

d. Economics or financial experts who are able to give advice on the movement of funds as well as the processes for tracking and identifying such movements.

e. Historians who can provide information that is invaluable when attempting to understand the lineage, background, cultural or tribal issues and their historical allegiances, including the way that the various actors conduct war.

111. **The Orchestration of Intelligence**. The way that we orchestrate intelligence will increasingly need to become more agile and dynamic. There are 2 approaches: the *conventional* and the *adaptive*:

a. **Conventional Approach**. The conventional approach has fixed lines and boundaries between departments that include rules for inter-agency co-operation. In effect it is a closed system. This system will become more difficult to sustain in the 21st Century and, while useful for certain problems, it is not flexible enough to deal with problems that are more complex. The current intelligence process is a product of the conventional approach. It does have utility as the bedrock of intelligence activity, but it must become more flexible to make it suitable for dealing with asymmetric problems.

b. **Adaptive Approach**. The adaptive approach requires a flexible and more open system, where agencies work together in a way that 'resembles jazz musicians improvising on a theme' to focus their efforts at the point of need.[10] The requirement for common protocols between agencies remains, but these should be agile and based upon the principle of collaboration: *how can we work together rather than articulating the obstacles to working together*. This spirit or ethos should be enshrined in intelligence

[10] US Marine Corps Pamphlet, *Countering Irregular Threats – A Comprehensive Approach*, June 2006.

operators to create the trust that promotes sharing at the lowest possible level.

Commanders need to provide clear direction on the establishment of intelligence networks that reflects both the nature of the operation and the need for collaboration. Such networks will include the arrangements for the integration of intelligence provided by other government agencies, responsibilities for fusion and the inclusion of intelligence from non-traditional sources. This direction should prevent the exclusion of any government agency or single-Service intelligence unit from the fusion of intelligence and the building of understanding.

112. **Other Factors Influencing the Intelligence Staff**. A variety of other factors will influence the way that intelligence staff operate in the contemporary environment. Primarily, the nature of adversaries is different in that they may have no fixed infrastructure, uniforms and tangible military assets or they may operate in cyberspace. Secondly, intelligence methods must change to reflect the greater availability of data, the growing sophistication of intelligence capabilities and the impact of network capability on working practices. Intelligence staff must be educated and trained to operate in the face of these challenges. Chapter 4 discusses the need for education and training for intelligence staff to enable them to cope with these challenges.

SECTION III – UNDERSTANDING AND INTELLIGENCE

113. **The Relationship between Understanding and Intelligence**. Understanding is one of the 3 key components of statecraft: understanding; power; and influence. It provides the context for the decision-making process, which informs the application of power to achieve national objectives by enabling us to develop and maintain a global view. This includes a detailed view of our national interests, our strategic partners and our international obligations (e.g. the UN and NATO). Intelligence plays a critical role by providing the processed information required to develop understanding. This includes answering the main intelligence question of what, where, why, how, who and when, and providing the context and narrative of events.

114. **The Importance of Insight and Foresight**. Whatever the context, understanding refers to the acquisition and development of knowledge to enable insight (*knowing **why** something has happened or is happening*) and foresight (*being able to identify and anticipate what **may** happen*). Developing understanding relies initially on gaining the

situational awareness to identify the problem.[11] Analysis of this situational awareness provides greater comprehension (insight) of the problem. Judgements based on this comprehension provide understanding of the problem (foresight). This is summarised as:

Understanding

Situational awareness + analysis = **Comprehension** (Insight)

Comprehension + judgement = **Understanding** (Foresight)

The distinction between situational awareness and understanding is the level of analysis and depth of comprehension that allows judgement to be applied effectively.[12]

115. **Definition of Understanding**. Within a military context, understanding is defined as *the perception and interpretation of a particular situation in order to provide the context, insight and foresight required for effective decision-making*.[13]

116. **Developing Understanding**. Understanding flows from developing the most inclusive perspective of an actor, group, environment or situation. Building understanding takes time; rarely will understanding of an area of interest be available at the outset of a potential crisis. Accessing information and processing it into intelligence is, by its very nature, a cross-governmental, multi-agency and multi-source activity. The approach must be sufficiently inclusive, flexible and adaptive to accommodate a wide range of experts, both within and external to the formal structure of a state's national agencies. Such experts may hold the key to understanding within the contemporary operating environment. Developing understanding is based upon:

a. Clear articulation of the requirement by commanders.

b. The development of networks and systems.

c. A detailed knowledge of the human domain.

d. Situational awareness derived from a common picture of the operational environment.

[11] In intelligence, situational awareness is *the ability to identify trends and linkages over time, and to relate these to what is happening and not happening*. (JDP 04 *Understanding*).
[12] Situational awareness is the appreciation of what is happening, but not necessarily, why it is happening.
[13] JDP 04.

e. The coherent integration of:

(1) Information management, exploitation and assurance.

(2) Communications and information technology.

f. Education and training.

117. **The Implications of Understanding for Commanders and Intelligence Staff**. Understanding is as much an attitude of mind as an activity. This has implications:

a. A change of ethos and philosophy: a duty to share proactively.

b. There is a greater requirement to understand our allies, adversaries, neutral actors and ourselves.

c. A change in how we produce our vision and intent, our thought and planning processes and in the way we make decisions.

d. We must be comfortable working with complex and ambiguous problems.

e. We must monitor and evaluate the effects and consequences of our decisions in order to learn, adapt and make better decisions in the future.

118. **Definition of Intelligence**. The MOD definition of intelligence is *the directed and co-ordinated acquisition and analysis of information to assess capabilities, intent and opportunities for exploitation by leaders at all levels*.[14] Information is defined as *unprocessed data of every description that may be used in the production of intelligence*.[15]

[14] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.
[15] AAP-6.

Derivation of *Intelligence* Definition

The new definition of intelligence is generic. It explains intelligence and its purpose across all levels from the strategic to the tactical for both civilian and military personnel within Defence. The term *leaders* has been used instead of *commanders* to explain this wider utility. The focus of intelligence product and process does, however, differ at each level of warfare and there are 3 extant definitions, given in Chapter 2, which describe the function of intelligence at these levels. They sit within the overall definition and are focused on commanders.

119. **The Roles of Intelligence**. The primary roles of intelligence are to: develop understanding; support decision-makers; support joint action; and support monitoring and evaluation. Chapter 4 describes these roles.

SECTION IV – NATIONAL UNDERSTANDING AND INTELLIGENCE

120. The national understanding and intelligence network connects intelligence agencies and other government departments with our global partners, allies and other key sources of information (such as academia and occasional intelligence partners). Maintaining and sustaining the network is ultimately a human activity and personal relationships are vital. These relationships must develop continuously to engender the trust and co-operation that is essential to enable the fusion of intelligence across multiple sources at the point of need. The national understanding and intelligence network also supports strategic and operational commanders through the MOD (Defence Intelligence), Permanent Joint Headquarters (PJHQ) and frontline commands. It also allows access to other Government agencies and institutions. Intelligence staffs must have a clear appreciation of the intelligence network and the capabilities of specific agencies assigned to their operations.

121. **State Intelligence Institutions and Associates**. The intelligence institutions of a democratic state broadly align with the elements of national power: diplomacy; military power; and economic power. Information, and the intelligence derived from it, is the lifeblood of the state when it comes to taking action through diplomatic, military or economic means. Without information and the ability to interpret it, none of these state institutions can operate effectively in pursuit of the national interest. Intelligence staff must constantly strive to maintain co-operative working and liaison. Commanders and intelligence staff must therefore forge, nurture, guard and sustain effective relationships to ensure a

reliable flow of information. In the context of wider state security, Figure 1.2 shows examples of intelligence institutions and associates:

Generic Intelligence Agencies	National intelligence Defence intelligence Police intelligence
Other Government Departments	The Cabinet Office Foreign and Commonwealth Office Department for International Development Department of Trade and Industry The Home Office
Occasional Intelligence Partners (Internal and External)	Private intelligence companies Host or friendly nation agencies
Other Potential Information Sources (National and International)	Academia Journalists Cultural experts International organisations (e.g. United Nations, International Committee of the Red Cross) Regional organisations (e.g. the European Union and African Union) Non-governmental Organisations
Allied Intelligence Agencies and Government Departments	Allied and Coalition Political-Military Alliances (e.g. NATO, ABCA[16]) Inter-governmental Security Co-operation (e.g. OSCE[17])

Figure 1.2 – Examples of Intelligence Institutions and Associates

These links form the basis of a national understanding and intelligence network. The generic network is represented graphically in Figure 1.3.

[16] American, British, Canadian, Australian and New Zealand Armies Program.
[17] Organization for Security and Co-operation in Europe.

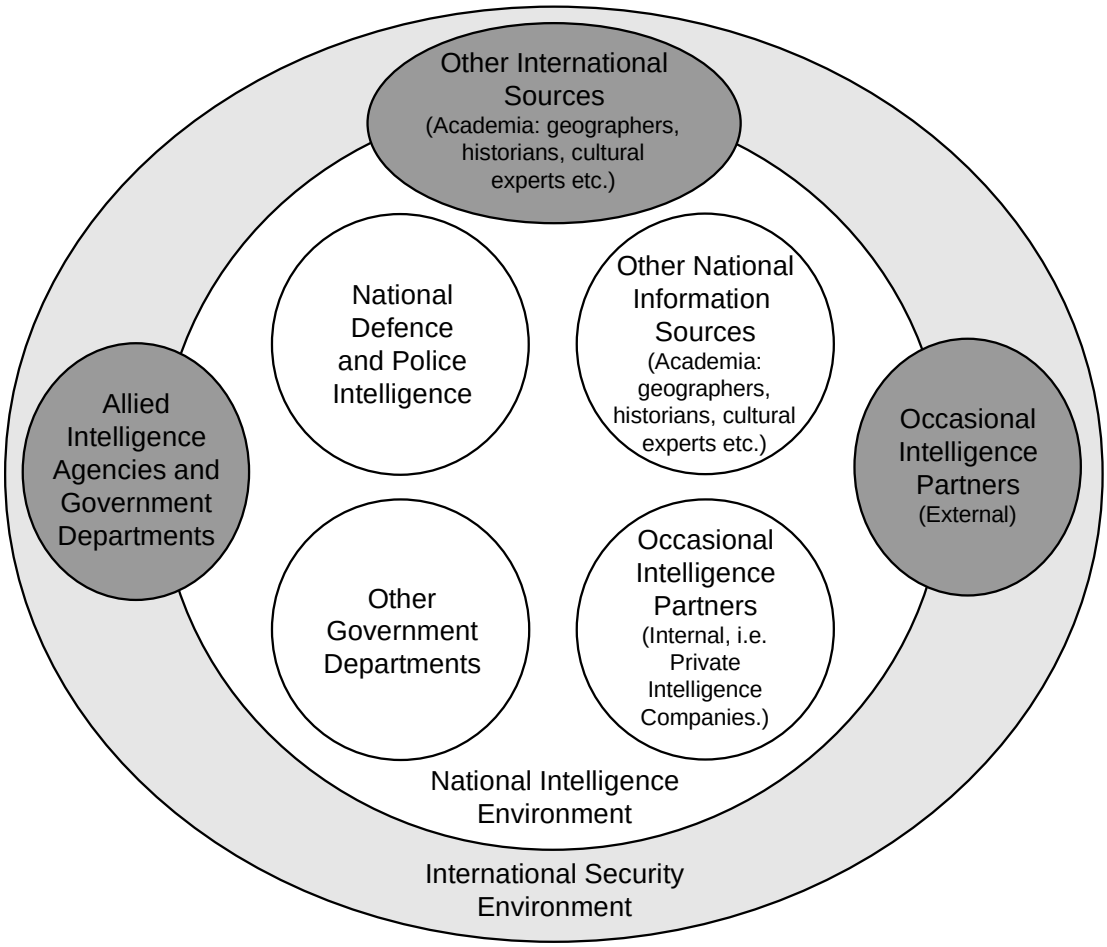


Figure 1.3 – The Generic National Understanding and Intelligence Network

122. **The Importance of a Generic State Model**. One of the principles of understanding is self-awareness. This demands an understanding of our networks, our operating principles and our interface with other states. When we look at our own understanding and intelligence network, there is a tendency to assume that other states operate with similar models. This is true with close allies and within formal structures such as NATO where there is already a high degree of collaboration and interoperability. However, with non-western, occasional intelligence partners and some host nations, this is often not the case. The generic state intelligence model is based on understanding how the nature of the state affects the way that we conduct intelligence activities. The people, the government and the military are products of their environment and have been shaped by their geography, history, culture, ethnicity, ideology and technological development. This shapes the unique way that they understand or respond to threats and whether they are aggressive, passive, neutral or peripheral players on the stage of war. It will also shape the way that

they organise and conduct intelligence activities to enable the wider security of the state. An important focus for intelligence staff is to compare our network and method of operating with that of our allies and adversaries. Commanders and intelligence staff need to consider these factors when designing their intelligence architecture and identify their interface with allies and be cognisant of the adversaries' architecture.

SECTION V – UK NATIONAL INTELLIGENCE AGENCIES

'*Intelligence is now big business, with a legal status and a public persona: it is no longer sensible to pretend that it doesn't exist. Democracies have to recognise it, and public opinion and those who form it, need some basis for informed views. Governments have to judge what to expect of it, how much to spend on it, and how to control it.*'[18]

Michael Herman

123. Once shrouded in secrecy, UK intelligence agencies are now in the public eye. During operations, intelligence staff must understand the organisations that constitute the UK intelligence community, what support they can provide and the protocols for contact, governance and assurance.

124. **National Security Council**. The National Security Council (NSC) is responsible for the co-ordination of responses to national threats. It integrates at the highest level the work of the foreign, defence, home, energy and international development departments, and all other arms of government contributing to national security. The NSC is responsible for the supervision and co-ordination of the national intelligence agencies and provides direction to MOD.

125. **The Joint Intelligence Committee**. The Joint Intelligence Committee serves 2 functions. It provides ministers and senior officials with co-ordinated interdepartmental intelligence assessments on a range of issues in the fields of security, defence and foreign affairs. In addition, it formulates and issues national requirements and priorities for intelligence. The Joint Intelligence Committee also has a warning and monitoring role. The Joint Intelligence Committee Assessments Staff supports the Joint Intelligence Committee by: drafting assessments; providing warnings of threats to British interests; and identifying and monitoring countries at risk of instability. It draws upon a range of reporting (primarily from the intelligence agencies, including UK

[18] Herman M, *Intelligence Power in Peace and War,* Cambridge University Press, page xii,1996.

diplomatic reporting and open source material) and thematic and country expertise (for example from Defence Intelligence, Foreign and Commonwealth Office or other government departments). The Chief of the Assessments Staff has an advisory oversight role for the programme of strategic assessments undertaken across Government in the security, defence and foreign affairs fields. The assessments staff maintains its own contacts with overseas intelligence organisations, allowing access to information and analysis that may otherwise not be available. In the case of countries with which the UK has military alliances or faces a common threat, the sharing of information enables decisions based on a more common understanding.

126. **Secret Intelligence Service**. The Secret Intelligence Service provides the Government with a global covert capability to promote and defend the national security and economic well-being of the UK. It is responsible under the Intelligence Services Act 1994 for the collection of intelligence on the actions or intentions of persons outside the UK. It conducts these actions as per the Joint Intelligence Committee's requirements and priorities.

127. **Government Communications Headquarters**. Government Communications Headquarters (GCHQ) is responsible under the Intelligence Services Act 1994 for the collection of signals intelligence to support Government policy-making and operations in the fields of national security, military operations, law enforcement and economic well-being. The intelligence collected includes crucial intelligence for the UK armed forces, wherever they are deployed in the world. GCHQ also undertakes information assurance to protect Government data (communications and information systems) from hackers and other threats.

128. **Security Service**. The Security Service is responsible under the Security Service Act 1989, for the protection of national security. In particular, it is responsible for protection against threats from espionage, terrorism and sabotage, and from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means. It is also responsible for safeguarding the economic well-being of the UK against threats posed by the actions or intentions of persons outside the UK. The Security Service also supports the activities of law enforcement agencies in the prevention and detection of serious crime.

129. **Joint Terrorism Analysis Centre**. The Joint Terrorism Analysis Centre is responsible for co-ordinating the analysis and dissemination of

intelligence in response to the international terrorist threat. The centre comprises of personnel from the MOD, Foreign and Commonwealth Office and Home Office staff.

130. **Defence Intelligence**. Headed by the Chief of Defence Intelligence, Defence Intelligence (formerly the Defence Intelligence Staff) is part of the MOD. The mission of Defence Intelligence is to provide intelligence products, assessments and advice to MOD which: guide decisions on policy and maintenance of operational commitment; informs defence procurement decisions; and supports military operations. Defence Intelligence also contributes to wider national collection and assessment efforts. It works closely with staff in other intelligence organisations and provides advice to other government departments (such as the Foreign and Commonwealth Office, the Department for International Development, and the Department for Business, Industry and Skills). Additionally, it works closely with NATO, the EU and other allies.

SECTION VI – FACTORS AFFECTING INTELLIGENCE IN THE CONTEMPORARY OPERATING ENVIRONMENT

131. **Intelligence with No Boundaries**. In the 21st Century, the traditional boundaries of the strategic, operational and tactical levels of warfare have less relevance when related to intelligence. Tactical military commanders may require access to strategic intelligence and tactical intelligence often has strategic importance. This has significant implications for security and the control and management of protectively marked material. In particular, it requires co-operation and collaboration between the intelligence agencies and across government departments. The MOD's vision is for a Defence-wide approach and environment, enabled by architecture and process, through which appropriate and timely intelligence reaches the user on time based on operational need, rather than their organisation, classification or method of collection. This approach, known as the *single intelligence environment*, is both an attitude of mind (i.e. embracing a collaborative environment) and the physical architecture to deliver it. Chapter 5 explains the single intelligence environment in detail.

132. **The Centrality of Influence**. In the military context, trying to achieve influence is central to our role. Intelligence provides the commander with the understanding on how best to achieve influence by either hard or soft power across a spectrum of potential civil and military activities. Figure 1.4 illustrates the spectrum of influence.

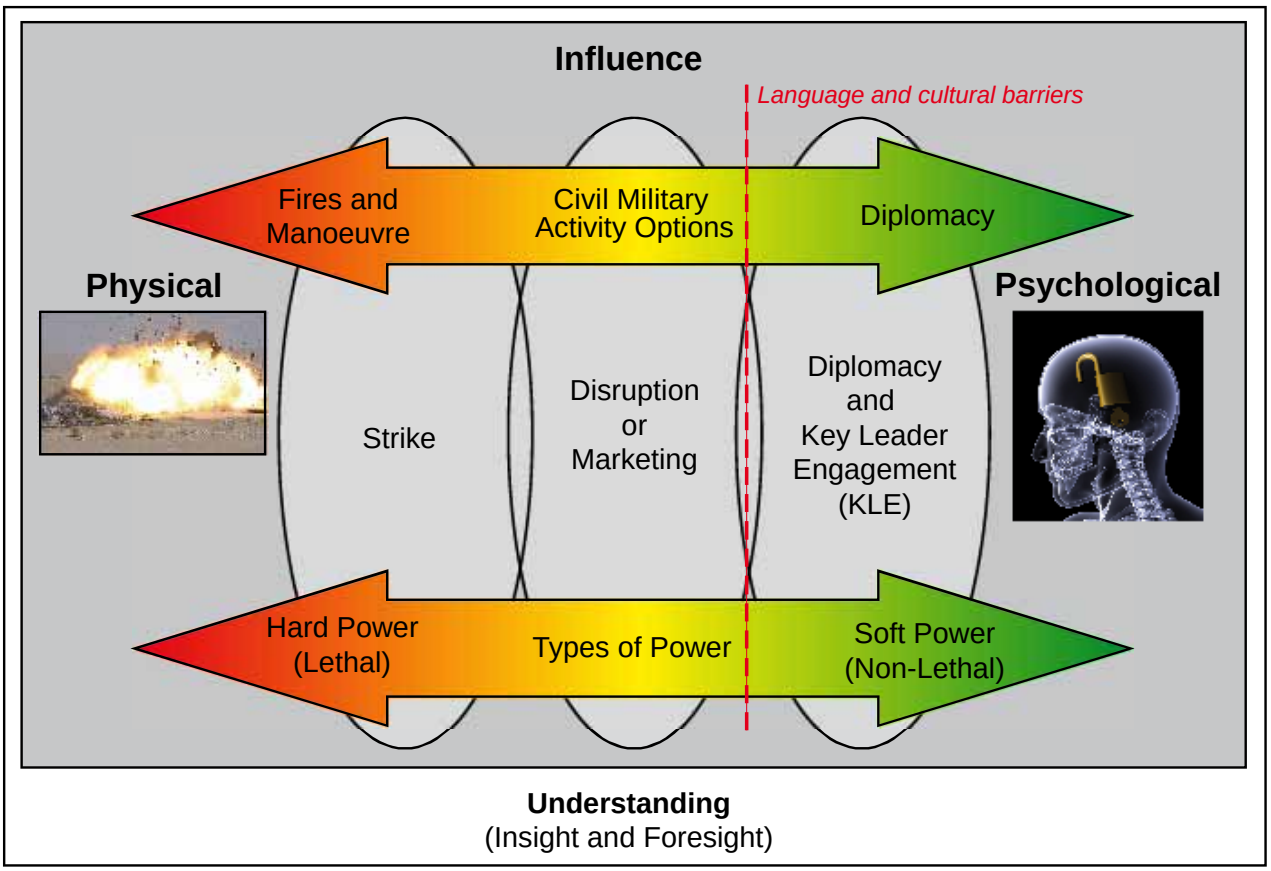


Figure 1.4 – The Spectrum of Influence

133. **Reach-back**. Reach-back is the ability to co-ordinate work between the operational theatre and external locations. It allows deployed forces to access additional expertise or services from dispersed intelligence centres and external organisations, including other UK-based military units, other government departments, academia and industry. Reach-back can reduce the number of deployed personnel, but requires the correct balance of resources and tasks between the echelons. Ideally, as much intelligence support and analysis as possible should be undertaken in the UK. Intelligence staffs that require access to national capabilities do so via Defence Intelligence, who co-ordinate, de-conflict and prioritise requests for information to national agencies.[19]

134. **Collaborative Working**. Collaborative working includes not only inter-service and inter-agency working, but also allies and partners. Traditionally, intelligence staffs have developed links with the militaries of other nations to strengthen key strategic alliances. This promotes both

[19] This is normally completed via the Intelligence Requirement Management and Collection Management Cell within Defence Intelligence.

burden sharing and the sharing of intelligence. This collaboration may need to extend to new non-traditional partners.

135. **Information Anarchy**. The increasing volume of information available and the increasing lack of any control over or provenance for it can create a condition known as information anarchy. This condition complicates commanders' abilities to identify and use the best information. Within headquarters, the ability to place relevant information quickly in its correct context should be the defining feature of an effective intelligence system. The widespread and clear articulation of command intent is a principal catalyst for shared context.

136. **Information Management and Exploitation**. Effective information management is the key to successful decision-making. Intelligence staff must continuously work with operations, plans and communications staff to ensure that processes are constantly developed, maintained and optimised to enable effective information flow and to maximise exploitation.

137. **Virtual Identity**. Virtual identity is an individual, common or collective persona in the information space that is different to that of the individual or organisation in the physical information space. An example of a virtual identity is the identity developed by an on-line gamer who is known on-line only by their cyber persona or where a group of gamers have a single virtual persona. Future adversaries may operate in this virtual world creating on-line identities to hinder tracing or pursuit. Over time, some adversaries may associate more with their virtual persona and conduct acts of subversion or terrorism in the real world in keeping with their on-line identities, effectively giving them the capacity to commit violent acts they would not normally have contemplated.

138. **Cultural Capability**. Cultural capability is the ability to understand culture and to apply this knowledge to engage effectively in different environments. Cultural capability is critical to understanding and requires the development of cultural expertise for the areas in which we are likely to operate, together with a general awareness of other cultures, and of how culture influences perceptions.

139. **Information Security and Protection**. Security will remain essential in ensuring the protection of individuals, organisations and intelligence sources. There is a tendency to over-classify intelligence which leads to reduced access when it is most needed. Defence Intelligence is responsible for establishing and promulgating common Defence guidelines for collaboration with other government agencies to

enable effective sharing of intelligence. Defence Intelligence guidelines are designed to strike the optimum balance between protection and timely exploitation. However, the protection of sources remains critically important and will continue to be a major driver for restricted access.

140. **The Importance of Geography and History**. Geography and history provide an authoritative foundation for placing intelligence within its correct context (for example, they can determine place names and known variants). They can enables the identification, visualisation, integration and fusion of multiple geographic, historic and other intelligence sources to support further analysis in order to identify patterns, trends, perceptions and interrelationships.

CHAPTER 2 – THE FUNDAMENTALS OF INTELLIGENCE

'*By intelligence we mean every sort of information about the enemy and his country – the basis, in short, of our own plans and operations*.'[1]

Clausewitz

Clausewitz's description of intelligence is as true today as it was in 1832. Intelligence enables commanders to understand their enemy and environment and then exploit that advantage. However, as Chapter 1 describes, it is no longer possible to focus only on our adversaries; we must understand the full context of the environment in which we operate. Chapter 2 considers a number of fundamental concepts that ensure commonality during MOD intelligence activities.

SECTION I – THE PRINCIPLES OF INTELLIGENCE

201. Intelligence at all levels is guided by 8 enduring principles (detailed in this section). These should govern the mindset, organisation and activities of those involved.

202. **Principle 1 – Command Led**. Setting the conditions for effective intelligence is a fundamental responsibility of command; intelligence failures are generally failures of command. Good intelligence flows from a command led process that constantly defines (and re-defines) what is important as well as what is urgent. Commanders should set priorities and direct the intelligence effort to meet operational requirements and to integrate intelligence with operations planning. Intelligence staffs are responsible for organising the collection and the production of intelligence. Unless intelligence staffs intimately understand the commander's intent, they will be unlikely to satisfy his requirements. Commanders should foster a command climate that empowers their staffs, particularly the intelligence staff, to work in a spirit of co-operation.

203. **Principle 2 – Objectivity**. Intelligence should always be unbiased, requiring staff with open minds. Intelligence staff should not distort their assessments to fit preconceived ideas to provide the answer that they think the commander wants, or conform to fit existing plans. A methodical and determined exploitation of all available information and intelligence will help

[1] Clausewitz, (edited and translated by Sir Michael Howard and Peter Paret), *On War*, Princeton, NJ: Princeton University Press, 1984.

objectivity.[2] However, objectivity can be threatened from outside or inside the intelligence staff:

a. Externally, the threat may come from above, through over-direction. This puts a considerable responsibility on the commander to give his intelligence staff room to disagree with him. Logical counter-arguments are vital, even though the commander reserves the right to take final judgements. However, wherever possible he should explain why he has disagreed with his staff.

b. Within the intelligence staff, co-operation can sometimes result in groupthink, which may distort analysis.[3] Overcoming groupthink requires an acceptance of authentic dissent, but it can be difficult when a group seeks to shun dissenters. Commanders must support the airing of dissenting views, even if they appear contrary to accepted wisdom.

204. **Principle 3 – Perspective**. Alternative perspectives reinforce objectivity. Even facts supported by strong evidence will be contested by others and understanding somebody's perception can be as important as understanding the facts. Intelligence analysts must seek to understand the likely perspective of adversaries and other key actors in the operational theatre. They must continuously refine their ability to think like them and to understand their fears, motivations, intentions, capabilities and narratives. There are 5 basic questions in the generation of perspective:

a. How do we perceive my adversary and other actors, including their actions?[4]

b. How do we perceive the actors?

c. How does the wider international community perceive the actors?

d. How do actors see themselves? Self-image plays an important part in narratives.

e. How will actors perceive my actions and what might be the other actors' probable responses?

[2] Joint Doctrine Note (JDN) 3/11 *Decision-Making and Problem Solving: Human and Organisational Factors* provides guidance on improving decision-making in all complex problems, by better understanding the factors that influence the way we think and behave as individuals, in groups and as organisations.
[3] Groupthink is created when the internal group dynamics will elicit conformity of opinion that is difficult for any individual to overcome, even when they believe that the opinion of the group is wrong.
[4] Understanding natural biases and pre-conceived ideas is implicit in this question.

Perspective also depends on mindset and personality. A key part of perspective is being open-minded and informed based on the ability to understand other peoples' views.

Perception

In the World War II, Field Marshal Montgomery kept a photograph in his caravan of Field Marshal Rommel, his principal antagonist, and asked himself daily what he would do if he were in Rommel's shoes. It is this perspective that is vital to understanding how to interact with adversaries and other actors.

Perspective – Mirror Imaging

Mirror imaging is when a person, group, organisation or nation is viewed through the lens of our own country or experience, rather from theirs. One example of this is the arms limitation discussions between Warsaw Pact and NATO officials in the 1980s concerning main battle tanks and their use as a weapon system. When both sides made qualitative judgements on main battle tanks there was a significant divergence of view. The result was that the capabilities of the same tank was judged by opposite sides of the discussions as being both the best in service and the worst. The reason for this was that each side of the meeting took a different view on how a tank should be designed and used, and therefore which attributes were more important. For NATO, a main battle tank was seen principally as a means of destroying an enemy's tanks. NATO placed particular emphasis on survivability on the battlefield and demanded high quality armour, speed and firepower. By contrast, the Warsaw Pact officials placed emphasis on the ability of a tank to work closely with their own infantry and as a vehicle to suppress enemy infantry. Accordingly, the most important consideration was the ability to carry quantities of ready to use ammunition in this role. Neither had tried to understand the different perspective of the other and had assumed that the use of the opposition's main battle tanks was a mirror image of their own.

205. **Principle 4 – Agility**. Agility is defined as *the physical and structural ability that allows forces to adjust rapidly and decisively, especially when operating in complex situations or in the face of new or unforeseen circumstances*.[5] It is a critical characteristic of effective intelligence. Intelligence staff should continuously adapt their activities to the changing environment and the requirements of their commanders. This implies mental and organisational agility in particular. Agility also exists in time; intelligence staffs need to deal with short notice requirements, while simultaneously continuing extant long-term work. Agility is not synonymous with speed; there are times when intelligence is required quickly, but agility is also the ability to exploit information at the correct tempo, implying trade-offs in speed, accuracy and cost. It is a myth that de-centralisation automatically creates agility; unregulated initiatives can reduce agility. Commanders must proactively risk manage, be clear about what is being de-centralised and establish effective control mechanisms. In intelligence, agility has 3 components:

a. **Resilience**. Not all intelligence activity will immediately be successful; it is essential to be persistent, adapt quickly and exploit opportunities when they arise. In particular, intelligence staffs must be sufficiently resilient to recover from intelligence failures or setbacks. An ethos of *learning and adapting,* coupled with a will to succeed after a serious setback, is vital.

b. **Adaptation**. Learning and adaptation can only occur through a comprehensive review of results. This enables reduction of negative unintended consequences, exploitation of positive unintended consequences and pursuit of those originally intended. Rigorous self-analysis by intelligence staff is critical and complacency is its enemy. Intelligence staff must test their assessments for continued relevance and adapt when circumstances change.

c. **Flexibility**. Flexibility allows the re-direction of effort to meet changing circumstances. It also shuns the notion that there is only one way of working. When applied correctly it enables new approaches to solve intractable problems and exploit opportunities.

206. **Principle 5 – Timeliness**. '*Knowledge a week too late is the same as ignorance*.'[6] Intelligence should be delivered in time. This will often produce tensions between speed, quality and comprehensiveness. However, even the best intelligence is rendered useless if it arrives after the event, so timeliness has a special importance. It is better to provide 80% of the intelligence on time rather than 100% of the intelligence too late. Similarly, the commander

[5] Joint Doctrine Publication (JDP) 0-01 *British Defence Doctrine*, paragraph 221.
[6] Friedman G, *The Intelligence Edge: How to Profit in the Information Age,* Crown Publishing, 1997.

must accept that when less time is available for an assessment, the uncertainty associated with it will inevitably increase. This is inextricably tied to the risks that a commander might wish to take. Quality assessments take time to produce and the commander should always aim to provide intelligence staff with the earliest notification of an intelligence requirement.

207. **Principle 6 – Collaboration**. Sharing individual understanding to achieve greater collective and common understanding is a powerful tool in joint and coalition operations.[7] The process includes collaboration with other nation's information and intelligence agencies. For operational security, the *need to know* principle endures, but a collaborative environment relies on a *duty to share* culture across and possibly outside government, underpinned by pragmatic risk-management. Without collaboration, attempts to develop a collective narrative are doomed to partial success or to failure.

208. **Principle 7 – Continuity**. Experience is gained slowly, but can be lost quickly. Some skills are enduring and transferable, particularly in enduring operations. Maintaining subject matter experts in post, both at home and on operations, is one way to achieve continuity of understanding. The commander should ensure that sufficient continuity of expertise is maintained within his intelligence staff, but also recognise the valuable insights sometimes gained from a fresh perspective. This may require being proscriptive about handover at the end of tour, maintaining an audit trail of judgements and decisions to allow new staff to pick up quickly, as well as enabling specialist on-the-job training at the commencement of a campaign or operation.

209. **Principle 8 – Security**. The advantages of collaboration in the production of intelligence are highlighted throughout this publication. Security permeates the entire intelligence enterprise. At the point of collection, techniques may be vulnerable to counter-measures if targets are alerted, the capabilities of sensors may be revealed and operators, handlers, sources and agents may be exposed to unacceptable risk. In the collation and analysis phases, unauthorised access to intelligence requirements or assessments may reveal intent, provide access for disruption of the intelligence process or illuminate gaps in knowledge. At distribution, inappropriate dissemination may provide useful information to an adversary, breach operational security by revealing plans or prejudice success through enabling counter-measures. All of these consequences could risk lives or mission failure. The risks are mitigated by technical measures, enforcement of rules and procedures, discipline (including self-discipline) and effective counter-intelligence operations.

[7] Individual understanding is our own personal interpretation of the facts. JDP 04, *Understanding*.

Command led	An inherent command responsibility: commanders provide the direction, resource the capability and create the right command climate.
Objectivity	Intelligence must be unbiased, undistorted, intellectually honest and free of prejudice.
Perspective	Get inside the mindset of the key actors, particularly adversaries; try to think like them.
Agility	Look ahead, identify threats and opportunities, develop the flexibility to react to changing situations and be ready to exploit opportunities as they arise. Agility is not about absolute speed: it is an ability to exploit information in context at the right tempo.
Timeliness	Providing intelligence on time, even if incomplete, to enable commanders to make decisions at a pace that maintains the initiative.
Collaboration	A duty to share as well as to protect.
Continuity	Develop and retain subject matter expertise.
Security	Security must permeate the entire intelligence enterprise, but should balance the need to share with the need to protect people and plans.

Figure 2.1 – Summary of the Principles of Intelligence

SECTION II – THE LEVELS OF INTELLIGENCE

210. Notwithstanding the ethos of intelligence with no boundaries, categorising intelligence into levels provides a helpful indicator of its function and helps to scope the resource requirements. Such a categorisation does not imply ownership or limit relevance and utility to a specific level of command. To achieve the best effect, it is wise to co-ordinate intelligence across the levels. The levels of intelligence are:

a. **Strategic Intelligence**. Strategic intelligence is defined as *intelligence required for the formation of policy, military planning and the provision of indications and warning, at the national and/or international levels*.[8] Gathered in response to government requirements, it focuses

[8] Allied Administrative Publication (AAP)-6 *NATO Glossary of Terms and Definitions*.

on national threats and supra-national issues, encompassing military, diplomatic, political and economic aspects. The nature of strategic intelligence means that a wide variety of intelligence sources and assets outside national capabilities are used. During coalition operations, the dominant coalition partner may own the assets employed in support of operations and may introduce caveats or limit availability of assets, which can restrict the collection and analysis of intelligence. It is important to develop the appropriate protocols to optimise the effectiveness of strategic intelligence.[9]

b. **Operational Intelligence**. Operational intelligence is defined as *intelligence required for the planning and conduct of campaigns at the operational level*.[10] Its primary users are operational level commanders and decision-makers with a specific area of responsibility.

c. **Tactical Intelligence**. Tactical intelligence is defined as *intelligence required for the planning and execution of operations at the tactical level*.[11] It normally supports specific activities by tactical level commanders or units. In most cases, intelligence assets providing tactical intelligence belong to the sending nation and may be part of the tactical headquarters involved.[12]

Levels of Intelligence and Responsibilities
Strategic ***Senior Military and Civilian Leaders***
• Assist in developing national policy and strategy • Monitor the international situation and maintain a global view • Maintain situational awareness • Identify likely adversaries • Assist the maintenance of key UK multinational alliances and strategic partnerships through defence diplomacy in support of other government activities • Assist in developing military plans in support of national plans: campaign planning; and contingency planning • Assist in determining the appropriate military capability to match the UK's global roles and aspirations – a key component of national and international credibility • Support the conduct of strategic operations

[9] For example in Afghanistan, the US controls some strategic collection assets that are accessible to the UK.
[10] AAP-6.
[11] *Ibid.*
[12] An example is those UK intelligence collection units that are assigned to support UK forces within the UK area of operations.

Operational ***Joint Force Commander***
• Focus on military capabilities and intentions of all key actors, enemies and adversaries globally and in the joint operations area • Monitor events in the commander's area of intelligence interest • Support the planning and conduct of joint campaigns • Identify adversary centres of gravity • Support the deployment, employment and recovery of joint forces in support of the campaign plan • Support operational security and force protection • Provide intelligence support to understanding, decision-making, joint actions (particularly targeting), monitoring and evaluation
Tactical ***Force Element Commanders***
• Support the planning and conduct of operations • Provide commanders with information on imminent threats • Provide commanders with intelligence to develop understanding

Figure 2.2 – Levels of Intelligence and Responsibilities

211. **Variations in Terminology**. Civilian agencies have different definitions of strategic, operational and tactical levels. Intelligence staff should expect variations in terminology, particularly at the tactical level and during homeland security operations.

The Civilian View of the Strategic, Operational and Tactical

'In military thinking, the distinction between tactical, operational and strategic is essentially spatial. It is a question of scale, roughly equivalent to the levels of the engagement. This ranges from tactical battles to the theatre or campaign level, and finally regional or global plans and posture in support of national aims. In civilian terms, the distinction is temporal; 'tactical' equates to short-term, whether it is in terms of days, weeks or months; 'strategic' refers to medium to long term, typically in terms of months or years; 'operational', by contrast, equates almost to the sub-tactical level of the melee, referring to techniques and specific actions whether it be contacting an agent, investigating a murder, policing a football match, observing an embassy or getting a story placed in the news media.'

Dr. Philip Davies and Dr. Kristian Gustafson
Brunel Centre for Intelligence and Security Studies

SECTION III – CATEGORIES OF INTELLIGENCE

212. Intelligence products reflect their intended use and include periodic intelligence summaries, specific intelligence reports and threat assessments.

213. **Basic Intelligence**. Basic intelligence is defined as *intelligence on any subject that may be used as reference material for planning and as a basis for processing subsequent information or intelligence*.[13] Basic intelligence includes details of orders of battle, equipment capabilities, personalities, infrastructure, socio-political, economic and environmental aspects. We derive basic intelligence through routine monitoring or on a contingency basis. Some UK intelligence agencies use the term 'building-block intelligence' when referring to basic intelligence.

214. **Current Intelligence**. Current intelligence is defined as *intelligence that reflects the existing situation at any level of command*.[14] It can offer greater granularity than basic intelligence, but generally reflects a moment in time and is perishable.

215. **Applied Intelligence**. Applied intelligence is defined as *intelligence which is tailored to provide direct support to the decision-making process*.[15] Exploitation of basic and current intelligence, to meet specific and normally predictive intelligence requirements, generates applied intelligence. It includes: an adversary's probable courses of action; how to influence local actors, including the general population of the host nation; specific reports on the capabilities of an adversary or neutral actors, which may influence the conduct of operations; and action by other agencies.

216. **Evaluation of Progress**. Intelligence can provide an evaluation of progress, based on levels of subjective and objective measurement to inform decision-making.[16] Intelligence contributes to an assessment of whether planned activities are successful by conducting battle damage assessments, accessing human intelligence and open sources, and analysing the actions of our adversaries over time to see if they have changed their approach because of our actions. In addition, intelligence can provide an assessment of the psychological effects of military activities and can support assessment and measurement for other civilian agencies.

[13] AAP-6.
[14] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.
[15] JDP 0-01.1 (7th Edition) *United Kingdom Glossary of Joint and Multinational Terms and Definitions*.
[16] JDP 01 (2nd Edition) *Campaigning*.

SECTION IV – THE LIMITATIONS OF INTELLIGENCE

217. **Management of Expectations**. Even when exploited fully, intelligence will not produce complete certainty. Intelligence staffs must be realistic about what can be achieved through intelligence activity especially when resources are limited. They must manage the expectations of their commanders while doing all they can to optimise available resources. Commanders should accept that intelligence can rarely be completely accurate.

218. **Incomplete Intelligence**. Intelligence may not meet the commander's requirements exactly and may not be entirely accurate, complete, or easily corroborated. Nevertheless, the commander will have to make judgements and decisions based on it. While there is the risk of misinterpretation or deception, exploiting information is critically important. Intelligence staff must articulate where there are gaps in knowledge. This will enable the commander to place appropriate weight on the assessments.

219. **Collection Assets**. All collection, exploitation and processing assets have limitations. Intelligence staff must provide the commander and all staff branches with a realistic appraisal of collection, exploitation and processing capability. This includes the limitations of each collection asset, its vulnerability to physical and electronic attack as well as deception, its coverage and the response time to meet requirements. Commanders should also understand the strengths and weaknesses of adversary collection assets. Additionally, commanders need to understand that the requirement for intelligence is likely to exceed the availability of collection or exploitation assets and they will have to prioritise their requirements ruthlessly to make best use of available intelligence resources.

220. **Source Protection**. Source protection is critical where covert collection capabilities are involved. However, source protection should not become a reason for withholding intelligence from those who need to know. This may require direction from the commander, if it is within his remit, on the balance between the need to protect the collection source and dissemination of the intelligence. Often, authority for release will be controlled through higher authorities at the national level.

221. **Capabilities and Intentions**. Historically, intelligence staffs have often determined an opponent's capabilities principally by the size, shape and quality of their military and the performance of their equipment. However, it has always been exceptionally difficult to determine an opponent's intentions. In the contemporary and future operating environments, where the size of an opponent's military capability may be less relevant due to unconventional or

hybrid tactics, intelligence staff should ensure that commanders understand the increased difficulty of determining adversaries' capabilities and intentions.

SECTION V – INTELLIGENCE DISCIPLINES

222. **Acoustic Intelligence**. Acoustic Intelligence (ACOUSTINT, sometimes ACINT) is defined as *intelligence derived from the collection and processing of acoustic phenomena*.[17] The term refers specifically to undersea intelligence gathered by submarines, sensors and passing ships. It is a sub-discipline of Measurement and Signature Intelligence (MASINT).

223. **Geospatial Intelligence**. Geospatial Intelligence (GEOINT) is defined as *the spatially and temporally referenced intelligence derived from the exploitation and analysis of imagery intelligence (IMINT) and geospatial information (GEOINF*[18]*) to establish patterns or to aggregate and extract additional intelligence*.[19] It may be complemented by other sources where they provide additional intelligence value. GEOINT is often a key enabler for multi-intelligence produced by the blending of multiple intelligence sources.[20]

224. **Imagery Intelligence**. IMINT is defined as *derived from imagery acquired by sensors that can be ground based, sea borne or carried by air or space platforms*.[21] The information conveyed by an image or textual report can corroborate intelligence derived from other sources. It may also be used in its own right, for example to support targeting or to map patterns of behaviour. Most IMINT is derived from aerial reconnaissance platforms and requires specialist analysis before use.

225. **Human Intelligence**. Human Intelligence (HUMINT) is defined as *a category of intelligence derived from information provided by, or collected on, human sources and individuals of intelligence interest, as well as systematic and controlled exploitation, by interaction with, or surveillance of, those sources or individuals*.[22] It is achieved through the observation of, or direct communication with, people. It encompasses debriefing, source handling, tactical questioning and interrogation all conducted by trained personnel.[23]

---

[17] AAP-6.
[18] GEOINF is defined as *facts about the Earth referenced by geographical position and arranged in a coherent structured. It describes the physical environment and includes data from the aeronautical, geographic, hydrographical, oceanographic and meteorological disciplines*. JDP 0-01.1
[19] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.
[20] Multi-intelligence is described in more detail in paragraph 325.
[21] JDP 0-01.1.
[22] *Ibid.*
[23] Any debriefing, tactical questioning and interrogation of such sources must comply with the applicable international and domestic law. See JDP 1-10 (2nd Edition) *Captured Persons* and Joint Service Publication (JSP) 383 *The Joint Service Manual of the Law of Armed Conflict*.

226. **Measurement and Signature Intelligence**. MASINT is defined as *the scientific and technical intelligence from the analysis of data obtained from sensing instruments for the purpose of identifying any distinctive features associated with the source, emitter or sender, to facilitate the latter's measurement and identification.*[24] Examples of MASINT information include, but are not limited to, intelligence derived from advanced processing of radar emissions, advanced electro-optical imaging and acoustic or seismic signatures. The applications of MASINT include, but are not limited to, the detection, tracking and identification of targets or systems, and description of distinctive characteristics of target sources.

227. **Open Source Intelligence**. Open Source Intelligence (OSINT) is defined as *intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access*.[25] Despite being open source, some official sources may have limited availability (such as limited print-runs of official reports that are not on the Internet), but they increasingly provide a rich source of information and should be sought. Collection of open source information for analysis and dissemination as OSINT is vital. Media monitoring, academic communities and industry all potentially provide examples of valuable open source resources while the Internet may provide material and insight into small, emerging and evolving adversarial groups.[26] OSINT and media monitoring in particular can be vital sources to support influence activities and for assessment. In complex operations, such material has an important part to play in achieving societal, cultural and ideological understanding. This is especially so when exploited by trained analysts to ensure the intelligence produced is unbiased and free of prejudice, open-source material is no less important than protectively marked material.

228. **Signals Intelligence**. Signals Intelligence (SIGINT) is defined as *the generic term used to describe communications intelligence and electronic intelligence when there is no requirement to differentiate between these 2 types of intelligence, or to represent the fusion of the two.*[27] SIGINT comprises:

[24] AAP-6.
[25] *Ibid*.
[26] This can, of course, refer to media of any kind; monitoring printed material has been commonplace for years, the BBC has monitored overseas broadcast media for a similar period. There will undoubtedly be increasing opportunities to exploit Internet publications and monitor social networks in the future.
[27] AAP-6.

a. **Communications Intelligence**. Communications Intelligence (COMINT) is *derived from electronic communications and communication systems by other than intended recipients or users.*[28]

b. **Electronic Intelligence**. Electronic Intelligence (ELINT) is *derived from electromagnetic non-communications transmissions by other than intended recipients or users*.[29] This includes the interception of radar emissions to identify an opponent's electronic order of battle.

229. **Materiel and Personnel Exploitation**. Materiel and Personnel Exploitation (MPE) is defined as *the systematic collection, information processing and dissemination of intelligence obtained by tactical questioning, interrogation and the extraction of data from recovered materiel*.[30] It is a multiple source, responsive process, which aims to maximise the intelligence value of detained individuals and recovered materiel. It contributes significantly to specific intelligence target development, as well as supporting wider thematic assessment. MPE ranges from the exploitation of recovered improvised explosive device components after an incident, to the systematic exploitation of a number of detained individuals. It can make extensive use of non-dedicated intelligence collection, including the harvesting of biometric and other forensic information, data recovered from computers and other digital systems, as well as hard copy documents. MPE comprises:

a. **Technical Intelligence**. Technical Intelligence (TECHINT) is defined as *intelligence concerning foreign technological developments, and the performance and operational capabilities of foreign material, which may have or could eventually, have a practical application for military purposes*.[31] TECHINT also encompasses exploitation of improvised explosive devices and can support counter-threat efforts.

b. **Weapons Intelligence**. Weapons intelligence is defined as *intelligence concerning components, manufacture, origin and method of employment of all foreign and domestic conventional and improvised weapons, munitions and devices*.[32] Weapons intelligence specialists provide the capability to understand the rapid technological development of adversary threats. Weapons intelligence establishes a picture of the adversary's technical capabilities and identifies their method of operation. It also contributes to network analysis and the prediction of future adversary intentions, as well as providing a further

[28] *Ibid*.
[29] *Ibid*.
[30] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.
[31] AAP-6.
[32] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.

dimension to the commander's intelligence picture from which he will plan and execute future operations.

c. **Forensic and Biometric Intelligence**. Forensic and Biometric Intelligence (FABINT) is defined as *intelligence derived from the application of multi-disciplinary scientific and technical processes and can often, although not exclusively, be collected to an evidential standard*.[33] Biometric intelligence is a sub-set of this, and refers to forensic intelligence related to specific individual.

d. **Chemical Exploitation**. Chemical Exploitation (CHEMEX) *provides chemical intelligence on IEDs, improvised weapons and unknown substances by processing, examining and analysing samples of materials*.[34] Technical outputs include identification of the substance, advice on the handling of the material should it be encountered again and comments on the material constituency or batch signatures.

e. **Financial Intelligence**. Financial Intelligence (FININT) is defined as *the gathering of information about the financial affairs of entities of interest, to understand their nature and capabilities and predict their intentions*.[35]

f. **Seized Media Analysis**. Seized Media Analysis (SMA) is defined as *the systematic exploitation of hard copy documents or electro-magnetically stored data, including that found on hard drives, data discs and personal communications systems*.[36]

g. **Medical Intelligence**. Medical intelligence (MEDINT) is defined as *intelligence derived from medical, bio-scientific, epidemiological, environmental and other information related to human or animal health*.[37] Being of a specific technical nature requires medical expertise throughout its direction and processing within the intelligence process.

[33] *Ibid*.
[34] *Ibid.*
[35] *Ibid*.
[36] *Ibid*.
[37] JDP 4-03 (3rd Edition) *Joint Medical Doctrine*, refers.

SECTION VI – COUNTER-INTELLIGENCE

230. **Definition of Counter-Intelligence**. Counter-intelligence is defined as *those activities that identify the threat to security posed by hostile intelligence services or organisations or by individuals engaged in espionage, sabotage, subversion, terrorism or other non-traditional threats*.[38] The main thrust of the counter-intelligence effort is to protect personnel, information, plans and resources, both in the UK and overseas. It aims to provide knowledge and understanding of the prevailing situation to keep privileged information secret, equipment secure and personnel safe.

231. **Purpose of Counter-Intelligence**. Counter-intelligence is an intelligence function that should provide commanders at all levels with a detailed understanding of threats, vulnerabilities and risks to enable them to make well-reasoned decisions on security measures. In reality, there are likely to be compromises between what is needed and what is feasible. Counter-intelligence should be proactive and preventative in its approach.

232. **Components of Counter-Intelligence**. Counter-intelligence has 3 components:

a. **Counter-Intelligence Activity**. Counter-intelligence activity can make a significant input to force protection and operations security. Primary activities are liaison, investigations, casework, screening of locally employed civilians and intelligence collection.[39] Liaison is conducted to obtain and corroborate information, develop sources of information and foster both goodwill and understanding. Investigations are conducted into the activities of an adversary and into personnel security matters. Counter-intelligence casework may exploit opportunities to develop greater understanding of security threats or weakness. Investigations and casework may employ interviews, record checks, technical measures, computer forensics, covert search and covert passive surveillance to develop understanding. Counter-intelligence activities require a high degree of integration with intelligence staff.

b. **Counter-Intelligence Analysis**. Counter-intelligence analysis is the fusion of multi-source information and intelligence on hostile intelligence services, terrorists, extremists and other groups or individuals. It also includes the analysis of the effectiveness of security measures and counter-intelligence operations.

[38] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.
[39] This includes dealing with persons who arrive at a base and make an unsolicited offer to provide intelligence (known as *walk-ins*) and people identified during screening tasks.

c. **Counter-Intelligence Advice**. Counter-intelligence staffs are responsible for advising commanders on the effectiveness of counter-measures and variation in the threat.

Counter-Intelligence Activities in Afghanistan

In Helmand Province in Afghanistan during October 2010, an RAF Police Counter-Intelligence Field Team (CIFT) was operating from Camp Bastion providing support to the force protection operation. While conducting screening of locally employed personnel, information was received about a firm of civilian contractors who were in possession of unauthorised automatic weapons. A counter-intelligence investigation was commenced. Liaison with base staff and the Afghan authorities established that the contractors were not entitled to posses firearms nor were they permitted to carry those firearms in Afghanistan. Intelligence was collected about the contractor and this identified the names of the individuals who had control of the weapons and where the weapons were being stored. Further liaison identified that the same contractor was also operating at Kandahar Airfield and the intelligence collected was shared with the Kandahar RAF Police CIFT. Intelligence collected at Kandahar identified that the contractor had a large compound on the base. The weapons were held contrary to Afghan Law and there was a risk that they could be stolen or used against Coalition forces. Briefed by the RAF Police team leaders, both base commanders agreed an intervention plan.

Weapons and ammunition seized by the RAF Police Counter-Intelligence Field Team Kandahar Airfield, October 2010

Simultaneous searches were co-ordinated at both bases and resulted in the seizure of a number of uncontrolled automatic weapons and ammunition for exploitation by TECHINT and FABINT. It also provided intelligence about the supply of black-market weapons.

233. **HUMINT and Counter-Intelligence**. HUMINT activities often occur alongside those involving counter-intelligence and many of the skills and capabilities are common. HUMINT and counter-intelligence should be regarded as being complementary intelligence functions and must not become competitive. It is essential that commanders encourage the respective intelligence staffs to co-operate.

SECTION VII – INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE

234. Within UK doctrine, the term Intelligence, Surveillance and Reconnaissance (ISR) is defined as *activities that synchronise and integrate the planning and operation of collection capabilities, including the processing and dissemination of the resulting product*.[40] The constituent elements are:

a. **Intelligence**. Within ISR, the term *intelligence* refers to the intelligence collection capabilities and to the analysis of information by the collecting organisations. For example the collection and analysis of HUMINT collected by human intelligence units or SIGINT collected by signals intelligence units. It is the intelligence staff who lead on target development in conjunction with the operations and plans staff. **Intelligence is a constant activity***.*

b. **Surveillance**. Surveillance is defined as *the systematic observation of aerospace, surface or subsurface areas, places, persons or things, by visual, aural, electronic, photographic or other means*.[41] Surveillance is conducted against adversaries and can be passive or active, covert or overt. It can be *coarse grained* to provide early warning of activity over a wide area, or *fine grained* to cover a particular location or facility. Surveillance over extended periods enables patterns and habits to be identified which leads to deeper understanding of other potentially threatening activities or behaviour. **Surveillance is an enduring activity for a specific period***.*

c. **Reconnaissance**. Reconnaissance is defined as *a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an opponent or potential opponent, or to secure data concerning the meteorological, hydrographical, or geographic characteristics of a particular area*.[42] It is a focused method of collecting information about specific locations, facilities or people. Reconnaissance is not confined by specific reconnaissance units but may be undertaken by other force elements in the course of their duties. **Reconnaissance is a mission specific task usually of relatively short duration***.*

235. **Non-Dedicated ISR**. Non-dedicated ISR assets are defined as *those assets not procured by MOD for specific ISR tasks but contribute to the intelligence picture as part of their routine operations*.[43] As communications

[40] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.
[41] AAP-6.
[42] *Ibid*.
[43] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.

improve across the joint force, the number of potential non-dedicated ISR assets will increase and should be exploited by commanders. Therefore, intelligence staff must continually look to exploit assets that have both a combat and an intelligence collection capability. Non-dedicated ISR assts can be as basic as personnel conducting routine activities to collect intelligence as a secondary role or technical innovations. Examples of non-dedicated ISR assets are infantry clearance patrols, service police patrols, joint logistic convoys and intra-theatre transport aircraft or combat aircraft fitted with sensor pods.

SECTION VIII – RECONNAISSANCE AND SURVEILLANCE SYSTEMS

236. **Space-based Systems**. Many space-based systems are defence orientated, but there are also other commercial systems whose output may be relevant to intelligence agencies. Defence space systems are used for wide-area surveillance and may be used to support other reconnaissance assets. Some assets provide their data on a strict rotational cycle to terrestrial fusion centres, from where processed information is further disseminated. However, some can downlink information in near-real time to dedicated ground stations.[44]

237. **Airborne Systems**. Airborne surveillance and reconnaissance assets may be manned or unmanned and equipped with a variety of radar, electronic, acoustic or electro-optic imaging sensors. While manned platforms are generally flexible and responsive assets, capable of collecting information as it occurs, they may not necessarily be able to download it immediately. The difficulty of providing communications bearers of sufficient bandwidth across significant distances is a key planning consideration.

With an array of high tech sensors and precision-guided weapons, the remotely piloted Reaper aircraft can carry out a range of missions in addition to its airborne surveillance role

[44] More details on the application of space are contained in *The UK Military Space Primer* published by DCDC.

238. **Ground-based Systems**. Ground-based intelligence systems can be deployed as organic capabilities to the lowest tactical level, and can be armoured, giving them a high degree of survivability and flexibility. They are usually capable of operating under all-weather conditions, although some specific sensors may be limited. Electronic sensors can be limited by terrain screening; coverage will thus be constrained by location. Unless located on high ground they may well suffer from limited range or the impact of areas of dead ground.

239. **Surface and Sub-surface Systems**. Maritime systems can vary greatly in size and capability. Invariably they have the advantage of sustainability and if employed on a suitable platform will have the ability to employ a number of different sensors, (e.g. radar, electronic and acoustic) to allow cross-correlation. Submarines are particularly suitable as platforms for clandestine reconnaissance operations within littoral waters.

240. **Special Forces**. Special Forces conduct covert, static or mobile surveillance and reconnaissance in support of their missions and joint operations. They can provide timely, accurate and critical information to respond to political and military decision-makers' information and intelligence requirements. They can often interpret what is seen, provide the important element of judgement, exercise initiative and react to changing circumstances.

241. **Covert Passive Surveillance**. Covert Passive Surveillance is defined as *the covert systematic observation of a person, place, object or activity from a covert static observation post or by use of foot, vehicle or aircraft, in order to gain or develop intelligence*.[45] It includes both directed surveillance and intrusive surveillance as defined within the Regulation of Investigatory Powers Act 2000. Trained operators conduct it, often over extended periods, to detect and identify an actor's activities and associations. Covert Passive Surveillance can support intelligence collection to evidential standard if required. It may be used as a stand-alone asset, in tandem with HUMINT operations or in support of HUMINT operations or as part of counter-intelligence operations. There are limitations in its use and it requires the correct equipment establishment, careful and detailed control, legal compliance and execution by appropriately trained personnel. However, when used correctly, it can provide essential decision-making intelligence as part of the wider all-source process.

[45] New UK definition established in JDP 2-00.

SECTION IX – LEGAL ISSUES

242. Adherence to the law is crucial in underpinning the legitimacy and campaign authority of any UK operation.[46] Intelligence activity conducted within the context of a military operation will have a legal dimension; there must be a basis for the activity and it must be conducted in a lawful manner. The applicable law will depend upon the overarching legal framework for a particular operation as well as the particular function conducted within each stage of the intelligence cycle. The *Legal Annex* of Chief of Joint Operation's Operational Directive provides further guidance for specific operations. Intelligence activity must be consistent with both the UK's obligations in international law, issued Rules of Engagement (ROE) and applicable domestic law as well as relevant aspects of host nation law and international human rights. To these may be added rights and obligations under UN Security Council resolutions or bilateral and multilateral agreements.

243. **Rules of Engagement**. ROE are a policy and operational guidance tool, which must sit within the legal framework of an operation. The responsibility for compliance with ROE is a command function and creating enabling ROE is a vital part of the d*irection* function of the intelligence process. ROE may restrict the use of some collection capabilities.[47] The formulation of ROE is a particular challenge in multinational missions, where the interpretation of international obligations, domestic laws and policies of the contributing nations add another layer of complexity.

244. **Domestic Law**. In accordance with Section 42 of the Armed Forces Act 2006, a person subject to Service Law or a civilian subject to Service discipline commits an offence if he performs an act that is punishable by the law of England and Wales. In this way, Service personnel and civilians working with the Armed Forces remain subject to the criminal jurisdiction of the law of England and Wales when conducting intelligence functions in the UK or elsewhere. UK statutory legislation that has particular relevance to intelligence activities includes:

a. **Regulation of Investigatory Powers Act 2000**. Covert human intelligence and surveillance operations are conducted by the armed forces and are planned, authorised, executed and recorded in a manner consistent with UK legislation, principally the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA provides a statutory basis for the use of investigative techniques and puts in place regulatory procedures which enable UK public authorities (including the MOD and

[46] JDP 0-01 *British Defence Doctrine* (BDD) (3rd Edition), paragraphs 160 -163.
[47] For example, an active collection radar system may be prohibited from use over a border.

Armed Forces) to interfere with an individual's recognised, but qualified, right to respect for their private life. Although that Act does not apply to overseas operations as a matter of law, policy should be developed to replicate it in suitably adapted form to provide appropriate control and supervision of the activities. RIPA requires, in particular, those authorising the use of covert techniques to consider whether their use is necessary and proportionate. It strictly limits the people who can lawfully use covert techniques and the purposes for, and conditions in which they can be used.

b. **Bribery Act 2010**. In accordance with Section 1 of the Bribery Act 2010 a person (including the UK Armed Forces) is guilty of an offence where he offers, promises or gives financial or other advantage to another person intending to induce that person to perform a function improperly or to reward them for improper performance.

c. **Data Protection Act 1998**. Many operations will rely on the exploitation of human, forensic, biometric, signal and other intelligence to counter threats and support other lines of operation. Some UK legislation directly applies to the activities of UK Armed Forces personnel on operations. Where legislation does not apply as a matter of law, policy should be developed to replicate the legislative arrangements, in suitably adapted form. This provides appropriate control and supervision of the activity to facilitate the transfer of collected data back to the UK and to share data with partners. The Data Protection Act 1998 and MOD's data protection policies are central to such considerations and of particular relevance to the dissemination of intelligence. Commanders must ensure the establishment of the legal framework for exploitation activities and information sharing before the commencement of an operation or as soon as feasible thereafter.

245. **Host Nation Law**. Host nation law may be a factor in identifying freedoms and constraints for particular intelligence activities. A Status of Forces Agreement (SOFA) or other agreement may be in place between the UK and the host nation that will highlight freedoms and constraints and define the extent of the applicability of host nation law to UK Armed Forces. Commanders and intelligence staff must be familiar with applicable host nation judicial and criminal processes.

246. **International Law**. In most operations of an international nature the legal mandate will be founded in international law and involve the application of elements of the Law of Armed Conflict (LOAC). All intelligence activity must be conducted within this overarching legal framework.

247. **International Human Rights Law**. The extra-territorial applications of the European Convention on Human Rights and the Human Rights Act have been the subject of extensive litigation in the UK domestic courts. As a result, it was accepted that the European Convention on Human Rights applied in a UK run detention facility in Iraq.[48] However, its application on operations elsewhere and at other times remains subject to legal and judicial scrutiny. Other international human rights law provisions may also be applicable to operations. Notwithstanding some lack of certainty about the relationship between international human rights law and LOAC, as well as the extra-territorial reach of the European Convention on Human Rights, UK personnel should treat Captured Persons (CPERS) humanely and conduct their exploitation and detention with all the protections afforded by international law.

248. **Rules of Evidence**. All intelligence collection is intended to satisfy intelligence requirements and no specific provision is made about the manner or method of collection to meet the requirements of the rules of evidence. Where it is envisaged that a line of information gathering may be intended for or result in criminal proceedings, intelligence staffs should advise the commander to seek early legal advice.

249. **Captured Persons**. One of the purposes of capturing persons is to obtain intelligence on an adversary's structures, capabilities and intentions. The intelligence exploitation of CPERS by tactical questioning and interrogation is a specialist skill that is only to be exercised by trained and competent staff.[49] In particular, humanitarian obligations relating to detention and the treatment of CPERS are paramount. Basic principles of humane treatment must be applied when dealing with all CPERS.[50] CPERS must be treated humanely at all times and provided with respect for their person, honour and religion. To the extent permitted by the military operation, they must be afforded protection from the conflict and treated consistently in accordance with the UK's obligations under customary international law, other applicable international law and treaty obligations, in particular Common Article 3 to the Geneva Conventions.[51] These basic principles are to be applied at all stages of the CPERS process from point of capture to release or transfer. During deployed operations, all personnel must be familiar with the processes for the handover of CPERS to the host nation and for criminal prosecution under host nation law.

[48] See House of Lords, Al Skeini (2007) UKHL 26, 13 June 2007.
[49] JDN 3/06 *Human Intelligence* provides details on tactical questioning and interrogation.
[50] See JDP 1-10 (2nd Edition) *Captured Persons*.
[51] *MOD Strategic Detention Policy* states that as a minimum, without prejudice to the legal status of a detained person, apply the standards articulated in Common Article 3 to the Geneva Conventions. Where other standards are applicable, they must be applied.

CHAPTER 3 – DEVELOPING INTELLIGENCE

'*Intelligence is an activity which has to perform 3 functions. Information has to be acquired; it has to be analysed and interpreted: it has to be put into the hands of those who use it.*'[1]

Professor F H Hinsley

Chapters 1 and 2 provide the strategic context for understanding and intelligence and the fundamentals of intelligence as an activity. The purpose of chapter 3 is to explain how we develop intelligence and to provide detail on the key intelligence activities.

SECTION I – THE INTELLIGENCE PROCESS AND THE CORE FUNCTIONS

301. The intelligence process is structured to collect and analyse information to turn it into intelligence. However, the word *process* has connotations of working by rote without imagination, which is unacceptable in the contemporary operating environment. The intelligence process must be sufficiently adaptable and dynamic to pass information as rapidly as possible to those who need it. This does not negate the requirement for the discipline of a systematic approach, but it does demand that we approach the development of intelligence differently. Imagination and a spirit of collaboration are critical to success during the intelligence process.

302. In the contemporary operating environment, intelligence development is based on 4 guidelines:

a. **A Common Purpose**. Producing intelligence is not an end in itself. All elements of the intelligence community and network must work to a common purpose. This common purpose can be achieved by having unity of command, a common taxonomy, common doctrine, common information protocols and common operating procedures.

b. **A Systematic and Flexible Process**. Intelligence is dynamic and perishable. There is a constant need for accurate and timely intelligence and this requires a continuous systematic, but flexible process based on sound principles. The principles of intelligence, which form the bedrock of the intelligence process, are described in Chapter 2.

[1] Hinsley F H, History of the Second World War, *British Intelligence in the Second World War* (abridged edition), HMSO, page 3, 1993.

c. **Fusion at the Point of Need**. Fusion improves the quality of intelligence. In intelligence, fusion is defined as *the blending of intelligence and/or information from multiple sources or agencies into a coherent picture. The origin of the initial individual items should then no longer be apparent*.[2]

d. **Synchronisation with Planning and Operation Cycles**. Intelligence staff must understand how the intelligence process fits in with other operational and planning processes. The intelligence process is not an end in itself.

303. **Process Theory**. A process is a series of actions or steps that achieves a particular outcome. In a generic process, the initial input triggers the requirement and the start of the process. This input is then transformed through a series of actions to develop an output. What we do with the output depends on the outcome that we wish to achieve.

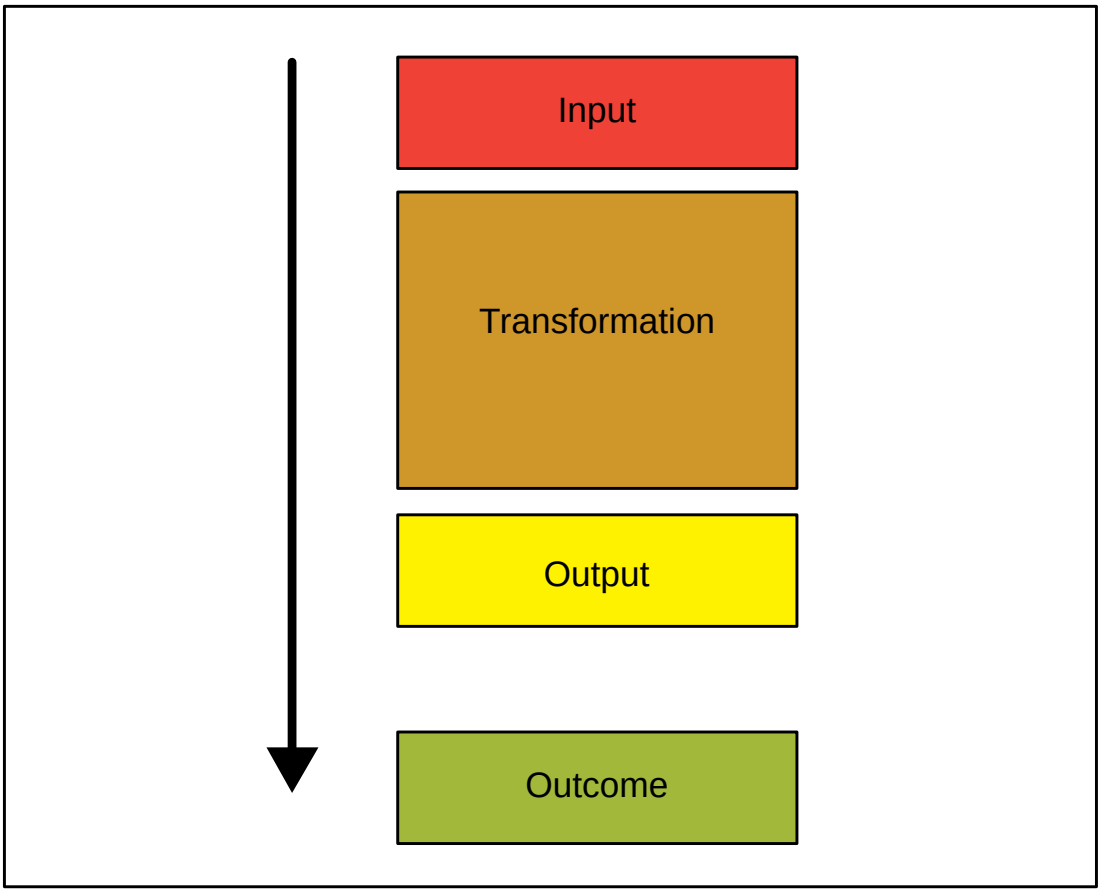


Figure 3.1 – Process Theory

[2] Allied Administrative Publication (AAP)-6, *NATO Glossary of Terms and Definitions*.

304. **The Intelligence Core Functions**. The intelligence process consists of 4 core functions, which closely follow process theory:

a. **Direction**. Direction is the key to the intelligence process. There are 2 distinct types of direction required to make the process work: external and internal. External direction comes from commanders at each level. It sets the parameters for the intelligence requirement and the intelligence objectives. Internal direction comes from the senior intelligence officer to each specialist element of the intelligence branch.

b. **Collection**. Collection is defined as *the exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence*.[3] Primarily Intelligence, Surveillance and Reconnaissance (ISR) assets conduct collection activities, but non-dedicated ISR assets also contribute. Collection activity requires close collaboration with intelligence direction staff to ensure efficient use of typically high-demand, low-volume assets.

c. **Processing**. Processing is defined as *the conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation*.[4] Processing is iterative and may generate further requirements for collection before dissemination of the intelligence.

d. **Dissemination**. Dissemination is defined as *the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it*.[5] It also requires security, conformity to the demander's requirement and a mechanism for feedback.

Figure 3.2 shows the link between the core functions and intelligence theory. Importantly, core functions produce the output and not the outcome, which is the result of decision-making.

[3] AAP-6.
[4] *Ibid*.
[5] *Ibid*.

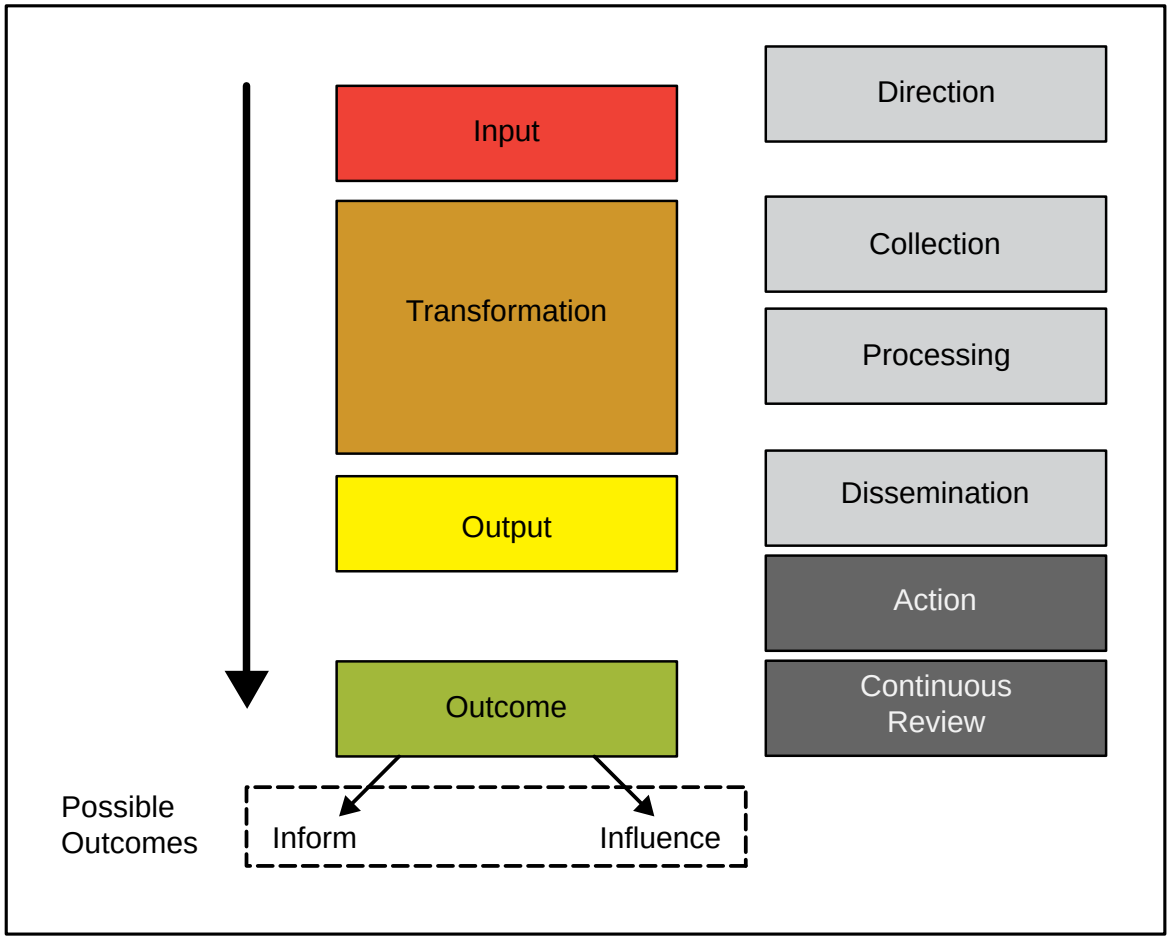


Figure 3.2 – Linking the Intelligence Core Functions to Process Theory

305. **The Intelligence Cycle**. The intelligence cycle is the common name for the intelligence process. Within the cycle, intelligence staffs conduct tasks and operations that provide relevant, accurate and timely intelligence to decision-makers. These activities are focused through the 4 intelligence core functions of direction, collection, processing and dissemination shown in Figure 3.3. It is a logical and methodical process intended to get the best available intelligence to the commander, but it should not be seen as prescriptive. It will always be imperfect, but decision-making has risks and the imperfect nature of the intelligence product must be factored in. While the intelligence cycle outwardly appears a simple process, in reality it is a complex set of activities. It is a continuous process comprising many cycles operating at different levels and speeds. Although the 4 individual tasks are discrete, as information flows and is processed and disseminated as intelligence, the tasks overlap and coincide so that they are often conducted concurrently, rather than sequentially.

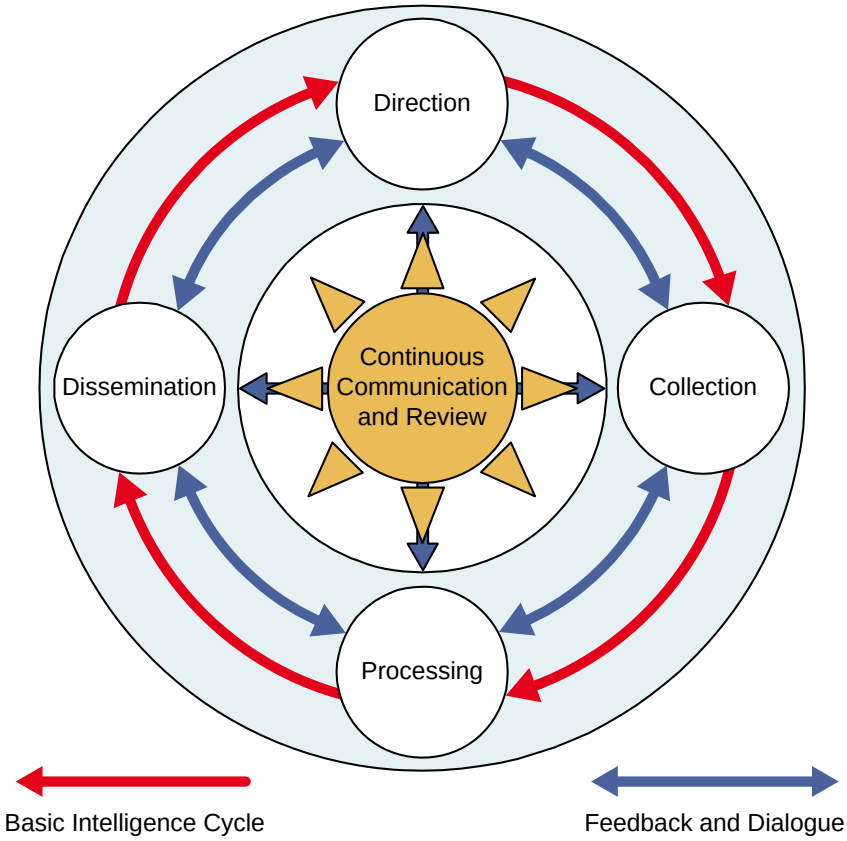


Figure 3.3 – The Intelligence Core Functions and the Intelligence Cycle[6]

306. **The Intelligence Process and the Intelligence Network**. All intelligence is ultimately about providing support to achieve national goals and objectives. Therefore, the intelligence network consists of multinational assets and multi-agencies. All of these agencies will be conducting the intelligence process at the strategic, operational and tactical levels continuously and concurrently while linked into other non-intelligence processes. The key to the optimal use of the intelligence process is continuous evaluation and feedback, unity of effort (based around the commander's information requirements) and the ability to adapt and change focus quickly. To achieve agility requires a change of ethos and philosophy and a willingness to operate in a spirit of collaboration. It also requires an in-depth understanding of the intelligence process to understand how to navigate through it.

307. **The Core Functions as Specialist Disciplines**. The core functions also drive intelligence specialist development. Under *direct*, intelligence staffs are trained to develop competences that include: knowledge of the national and operational intelligence architectures; leadership and management of personnel and information; and the provision of advice to operational commanders. *Collection* specialists develop competences relating to:

[6] Diagram based on an interpretation of the intelligence cycle by Dr Philip Davies from Brunel University.

understanding the sources of intelligence; selection of sources and agencies for specific tasks; understanding the tasking, processing and management of ISR and its manifold capabilities; and interoperability with multinational agencies. *Processing* expertise focuses on collation, evaluation, analysis, integration and interpretation. *Dissemination* crosses all disciplines, but is essentially concerned with the timely and appropriate promulgation of intelligence.

SECTION II – DIRECTION

308. Direction is defined as *the initial stage in the intelligence process and consists of the determination and prioritisation of intelligence requirements, planning the collection effort, the issue of tasks and requests to collection, exploitation and processing assets or external agencies, and maintenance of a continuous check on the progress of intelligence requirements throughout their lifecycle*.[7] There are 2 types of direction:

a. **External Direction**. The commander provides the external direction to the intelligence branch. He must direct the intelligence staff through clear intent, which underpins the intelligence that he needs and the time limits on its provision. This direction should be specific and, wherever feasible, should highlight those areas of information and activity that are critical to the planning process. As a minimum the commander must set the parameters for his intelligence requirement by telling his intelligence staff what he wants to know and when. The commander needs to articulate the requirement clearly. When faced with a problem the commander can address 5 generic requirements with his staff:

(1) What do we want to understand and how soon?

(2) What do we know?

(3) What are the potential gaps in our knowledge?

(4) How do we fill those gaps?

(5) How do we exploit our knowledge?

b. **Internal**. Based on the commander's intelligence requirements, the intelligence staff must direct the collection and processing of information and the dissemination of the resulting intelligence. This

[7] New UK definition established in Joint Doctrine Publication (JDP) 2-00 (3rd Edition) *Intelligence and Understanding* and awaiting formal approval by NATO.

requires internal direction by the chief of the intelligence branch and his subordinates. This direction involves:

(1) Deciding *how* to meet the commander's intelligence requirements and what information to collect.

(2) Planning and tasking the use of organic or subordinate assets, or issuing requests for information to external headquarters, sources or agencies, to collect or process the necessary information.

(3) Monitoring the lifecycle of intelligence requirements to ensure they answer the commander's requirements within his parameters.

Intelligence and Information Requirements

309. **Commander's Critical Information Requirements**. At the outset of planning, a commander and his staff will begin to formulate questions. More questions will be posed and existing questions will be amended as planning evolves and as the subsequent operation develops. These questions, many of which fall outside the remit of the intelligence staffs, are the C*ommander's Critical Information Requirements* (CCIRs).

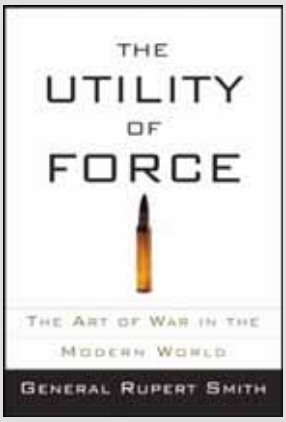
310. **Information Requirements**. Information Requirements are *those items of information regarding the enemy and his environment that need to be collected and processed to meet the intelligence requirements of a commander.*[8] They consist of:

a. **Specific Information Requirements**. Specific Information Requirements describe the information required, the location where the required information can be collected and the time during which they can be collected.

b. **Essential Elements of Information**. CCIRs can be broken down into more manageable Essential Elements of Information (EEIs), which clarify points for collection and analysis. These represent the intelligence consumers' specific requirements. Expressing complex intelligence requirements as a collection of essential elements of information provides the additional level of guidance needed by intelligence collectors and analysts to achieve the desired effect.

[8] AAP-6.

Commander's Critical Information Requirements
An Example: General Sir Rupert Smith's 8 Question Groups



In *The Utility of Force*, General Sir Rupert Smith postulates questions that demonstrate the difficulty in one particular environment and the depth of knowledge the commander needs to understand it. They are:

- Who are we opposed to? What is the outcome they desire? What future do they threaten? How does this differ from our desired outcome?
- Are we seeking order or justice? On a scale between them, where is our outcome? If we are seeking justice, who is it for?
- Who are we going to deal with, their present leaders or do we want others in power? If so, who are they? Are we changing the present leadership entirely? If not, who stays?
- Are we using their law or ours? If ours, do we want theirs to change?
- Who is administering the state, them or us?
- Do we know the outcome we want in sufficient detail that we can set objectives to be achieved?
- At what level can we in theory achieve objectives directly by force of arms? Should we do this? Can we do this? Will we do this? When do we do this?
- If not, what are we prepared to threaten and promise in order to achieve the objectives? What does the opponent most value that we can threaten? What does he want most?

311. **Requests for Information**. Where a unit does not have sufficient allocated ISR resources, it can issue an intelligence requirement to another organisation as a Request for Information (RFI). The term RFI is used to describe the format in which an intelligence requirement is passed to the intelligence requirements manager at higher or adjacent levels. The receiving

organisation will treat the incoming RFI as an intelligence requirement (and usually as a one-off requirement unless it is a standing task), the only difference being that the intelligence requirement is undertaken on behalf of another organisation. Intelligence requirements passed between coalition partners are passed as RFIs. A single intelligence requirement may generate a number of separate RFIs for different providers or other intelligence resources such as national assets or subordinate headquarters. The term RFI is also widely used outside of the intelligence specialisation.

312. **Intelligence Requirements**. A portion of the commander's critical information requirements will concern the adversary or the environment and since these are for the intelligence staff to answer, they constitute *intelligence requirements*. An intelligence requirement is *a requirement for assessed information about any aspect of a situation needed to develop a commander's understanding*.[9] In essence, it articulates gaps in knowledge that must be filled so that a commander can conduct planning. Intelligence requirements may be further categorised as:

a. **Priority Intelligence Requirements**. Some intelligence requirements will be critical to the planning and conduct of operations. Due to the importance of this intelligence to the commander's decision-making, these questions are designated *Priority Intelligence Requirements* (PIRs). They are defined as *those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decision-making*.[10] The commander should prioritise PIRs and keep them under continual review.

b. **Enduring Intelligence Requirements**. Enduring Intelligence Requirements (EIRs) are *intelligence requirements that require regular and repeated satisfaction over time*.[11]

313. **Expressing Intelligence Requirements**. Expressed in a clear and concise form, intelligence requirements should be:

a. **Specific**. Each intelligence requirement should clearly identify the information needed within the context of the commander's intent. Each requirement should outline a specific intelligence need, preferably in a single sentence. Multiple questions should be presented as separate intelligence requirements.

[9] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.
[10] AAP-6.
[11] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.

b. **Measurable**. It must be possible to determine when an intelligence requirement has been successfully fulfilled.

c. **Realistic**. A theoretically achievable intelligence requirement may be unrealistic due to capability or collection limitations, including response times.

d. **Timely**. Deadlines associated with each intelligence requirement should be clearly stated.

314. **Content of Intelligence Requirements**. Intelligence requirements are not framed as tasks for collection assets. However, they should include:

a. **Justification**. To assist in prioritisation, a justification for the request.

b. **Response criteria**. The required type and format of the response, including the highest acceptable security classification and the manner of dissemination.

c. **Consultation**. Details of any previous or current intelligence providers consulted to prevent duplication of effort.

Intelligence Requirements Management and Collection Management

315. To provide robust management during the intelligence process it is essential to have a coherent and focused ability for providing effective direction. Within the *direction* stage of the intelligence process, Intelligence Requirements Management and Collection Management (IRM&CM) are the main internal activities.[12] IRM&CM provides a central focus for the management of all intelligence requirements to harness the collection and processing capabilities across Defence by translating the intent implicit in an intelligence requirement into definitive collection and processing tasks. The roles of IRM&CM are to:

a. Synchronise intelligence collection and production efforts.

b. Ensure maximum advantage is made of intelligence collection and production capabilities.

c. Co-ordinate the tasking, production, storage and dissemination of intelligence using the underlying tenets of: *duty to share* and *collect once and use often*.

[12] Defence Intelligence holds responsibility for the Defence IRM&CM capability, which includes providing the single access point to national agencies and co-ordinating reach-back support for operational requirements.

d. Integrate intelligence into planning procedures across Defence.

e. Manage collaboration with partners at all levels.

Intelligence Requirements Management

316. It is the responsibility of IRM staff to determine, interpret, develop, prioritise, revise and manage the fulfilment of intelligence requirements. In carrying out their duties, IRM staff will:

a. Based on the commander's intent, his direction and the priority intelligence requirements, conduct an assessment to determine an intelligence requirement's relative priority.

b. Arrange for a search of existing databases and publications. This will negate any unnecessary collection or processing activity if an answer to the intelligence requirement is available within existing records.

c. Determine if the intelligence requirements can be met by tasking of assets under their operational control and if not produce a RFI. Should collection assets be required from higher formation, IRM staff should ensure that the commander is aware of the associated risks and potential delays associated with assets that may already have higher priority tasking.

d. Convert intelligence requirements that can be answered by assigned collection assets into collection requirements, which specifies the type of information and intelligence required. Subsequently, the collection management process will convert this requirement into specific tasks for a collection asset. To help co-ordinate the required collection, exploitation and processing IRM staff produce an intelligence collection plan.

e. Track the task until completion or rejection and keep the demander informed on its status. If there is doubt as to whether the timescale can be met, the intelligence requirement manager will consult the demander to ask if a later delivery is acceptable or if the task should be cancelled, releasing assets for other tasks.

f. Disseminate results to the demander. Once a task has been completed, the resulting information and intelligence is usually sent directly to the demander and the only involvement by an intelligence requirement manager is consultation with both the producer and demander to ensure that the remit has or will be met. Resulting

intelligence is placed in a database to be searched against in response to subsequent intelligence requirements and made available to as wide an audience as possible.

Collection Management

317. Collection management is defined as *the process of converting intelligence requirements into collection requirements, establishing, tasking or coordinating with appropriate collection sources and agencies, monitoring results and re-tasking, as required*.[13] It is illustrated at Figure 3.4. Collection management optimises the deployment and tasking of finite collection assets in accordance with the intelligence collection plan. Collection management matches each intelligence requirement to the most appropriate collector, accounting for the type of information required, timeliness, availability of assets and tasking authority.

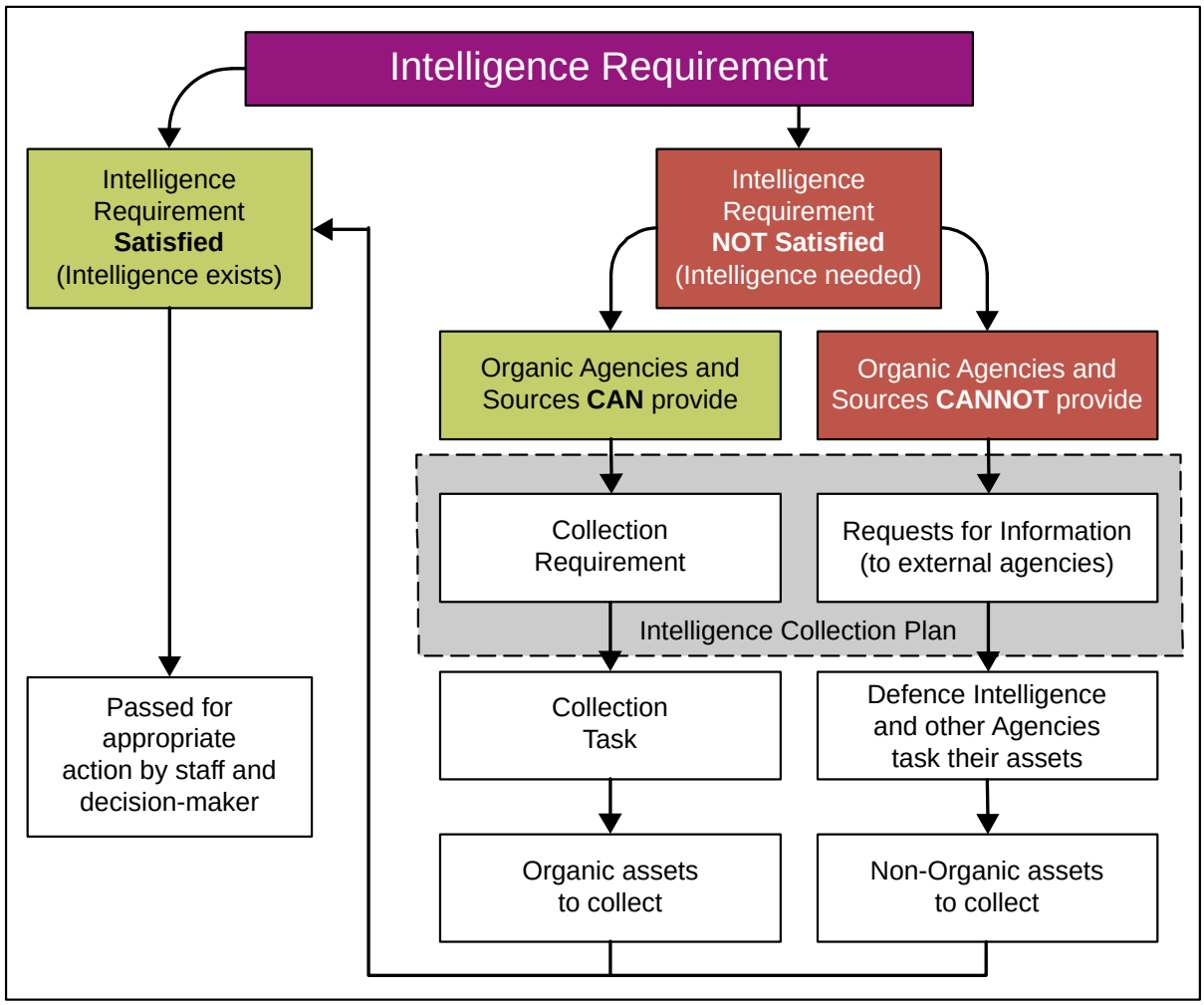


Figure 3.4 – Collection Management

[13] AAP-6

318. **Intelligence Collection Plan**. Operations place an enormous demand on assigned collection assets to deliver near-real-time information in a complex battle-space. Information is required to support situational awareness, including force protection, target acquisitions and combat assessment. There is a risk that the associated collection tasks are undertaken at the expense of sustaining the intelligence process and the longer view. An *intelligence collection plan* is a support tool to assist the IRM staff in producing, completing and monitoring unfinished intelligence requirements. It articulates the priorities and constraints for each intelligence requirement. In the intelligence collection plan, the IRM staff deconstructs intelligence requirements into their constituent priority or enduring intelligence requirements and essential elements of information. IRM staff should crosscheck collection plans with the other staff branches.

319. **Intelligence Indicators**. Before beginning the process of designing an intelligence collection plan, the intelligence staff must identify the indicators that are appropriate to the particular operation or threat. Indicators are *items of information that reflects the intention or capability of a potential adversary to adopt or reject a course of action*.[14] Indicators are normally categorised under 3 headings:

a. **Alert or Warning Indicators**. These relate to preparations by an adversary for offensive action. At the strategic level, this could include the collapse of negotiations or issue of ultimatums while at the operational level it could include the re-supply or re-deployment of adversary capabilities.

b. **Tactical or Combat Indicators**. These indicators reveal the type of operation the adversary is about to conduct. Indicators linked to these preparations can potentially be defined well in advance and must be reflected in the priority intelligence requirements. For example, tactical indicators could include the increasing number of naval ships in port or the purchase by insurgents of particular types of weaponry.

c. **Identification Indicators**. Identification indicators are those that enable the identity and role of a formation, unit, installation or irregular adversary grouping to be determined from its order-of-battle, equipment and tactics.

Selection of indicators appropriate to the operational situation is the responsibility of the intelligence staff. The nature of the indicators that they select will inform the intelligence collection plan.

[14] AAP-6.

320. **Review of the Intelligence Collection Plan**. IRM staffs should continuously review the intelligence collection plan, monitoring the productivity of sources and agencies in response to tasking. It should be distributed to higher, lower and lateral levels of command, including multinational partners, to inform them and facilitate co-ordination.

SECTION III – COLLECTION

'*Every sailor, soldier or airman is a sensor*.'[15]

321. Collection is defined as *the exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence*.[16] It comprises raw data, first-phase exploitation of the data and the dissemination of the product to processing users. In some cases, collection activities will not be required because data can be retrieved from archives or databases.

322. **Sources**. A source is defined as *a person, object, process or system from which information can be obtained*.[17] While analysis and some collection capabilities require specialist skills, anyone can be a collector if they have access to information. Sources are categorised as:

a. **Controlled**. Controlled sources are people, processes and systems that are under control of an intelligence agency or organisation, or specifically nominated intelligence staff.

b. **Uncontrolled**. Uncontrolled sources are those not under formal control of an intelligence agency or organisation, or specifically nominated intelligence staff. Therefore, they cannot be tasked directly. Examples include the media and other nation's intelligence apparatus. Information provided by uncontrolled sources is treated with caution as it may be intended to deceive or influence. Specialist personnel are trained to assess the reliability of uncontrolled sources.

c. **Casual sources**. Casual sources, such as defectors or refugees, provide unsolicited information. Such information is always treated with caution, as it may be intended to deceive or influence. Specialist personnel are trained to assess a casual source's reliability.[18]

[15] Adapted from *Every soldier is a Sensor,* a US Army training slogan. The slogan reflects the fact that every member of a deployed formation has a responsibility to collect intelligence as part of his or her duties. This includes reports from liaison officers, reports on official meetings and reports from routine duties (patrols, checkpoints etc).
[16] AAP-6.
[17] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.
[18] These personnel receive special training in the legal implications of their actions.

323. **Agencies**. An agency is defined as *an organisation or individual engaged in collecting and/or processing information.*[19] An agency is different from a source because a source produces raw data while an agency, having a collection capability, also possesses some degree of processing capability and can provide intelligence. Agencies can be national, (i.e. Secret Intelligence Service) or multinational (i.e. NATO).

324. **Agency and Source Selection**. Selection of a source or agency for a particular task is the responsibility of the IRM&CM staff who consider:

a. **Security**. Sources must be adequately protected unless, in exceptional circumstances, a decision is taken that the operational benefits of not doing so outweigh the likely consequences to the intelligence effort. Failure to protect sources will result either in the loss of the source or its compromise and possible use to deceive.

b. **Capability**. An agency tasked to collect an item of information or produce specific intelligence must be capable of doing so; it must possess the appropriate sensor, platform, collection opportunity and processing capability.

c. **Suitability**. There will be occasions when more than one type of source or agency may be capable of carrying out a collection task. IRM&CM staff must consider the attributes of each asset to ensure that the most appropriate is chosen.

d. **Risk**. There will often be an element of physical, political or military risk involved in the employment of a particular source or agency. The risk involved must be weighed against the value of the information sought.

e. **Battlespace**. Factors such as political constraint, weather, or terrain may limit the ability of a source or agency to collect information.

f. **Balance of Tasking**. Balance is achieved by an even distribution of the collection workload across the range of available sources and agencies. Although this is desirable, it is not always practical given limited collection assets and the need to prioritise.

g. **Timelines**. Sources and agencies selected to meet a request for information must be capable of achieving the task within the deadline.

[19] AAP-6.

325. **Single and Multiple-Source Intelligence**. Most intelligence is derived from a single source. However, there are significant advantages to be derived from the use of Multiple Source Intelligence (MULTI-INT). MULTI-INT is defined as *the deliberate application of 2 or more discrete but supporting intelligence disciplines (e.g. Geospatial Intelligence, Human Intelligence (HUMINT) and Signals Intelligence (SIGINT)) seeking to improve the quality of the intelligence product*.[20] Devoting time and effort to corroboration during intelligence collection activities increases certainty and reduces risk. Corroboration is achieved by comparing intelligence derived from one source with that derived from at least one other source so that common features or contradictions can be identified.

Multiple Intelligence (MULTI-INT)

Operation ATLANTA commenced in December 2008 and is the EU Naval Forces mission to counter piracy off the coast of Somalia. This operation was in response to an increase in piracy activity that affected commercial shipping movements. The area affected was some 1 million square nautical miles.

Due to the size of the sea area, unfocussed routine monitoring was unlikely to produce the results needed to pre-empt pirate activity. Therefore, the commander prioritised the identification of potential areas of operations for the pirates' mother ships, to enable a focussed application of intelligence assets. Analysis of open source information, the prevailing weather conditions and time/distance identified a number of probable piracy locations and timings. This analysis enabled the tasking of fixed-wing imagery intelligence platforms and naval assets into these locations and resulted in a number of successful piracy detections and boarding operations. The fusion of information recovered in these boarding operations with HUMINT, SIGINT and the results of document exploitation enhanced understanding of the piracy network and allowed focused targeting of pirates. Consequently, during a 2-week operation, 5 pirate vessels were neutralised and 20-suspected pirates arrested.

Multiple source intelligence will often have a higher degree of confidence than single-source intelligence, in part due to its resistance to deception. To gain additional benefit, intelligence staffs should fuse material, blending intelligence

[20] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.

and information from multiple feeds, including open sources, into a coherent picture. Cross-cueing of one type of collection asset from another may enable simultaneous, or at least nearly contemporary, observation with a resultant increase in the density of information on that target.[21] The adoption of such practices disguises the source of the material, which may also allow the product to have a lower protective marking, thus enabling wider dissemination. Intelligence staff must advise recipients when intelligence is uncorroborated.

326. **Selection of Collection Assets**. Resource tasking is defined as *the activity undertaken to complete the collection plan by selection of the most appropriate ISR resource types for which tasking authority has been allocated*.[22] Resource taskers select assets assigned to them according to their suitability and availability rather than ownership. For tasks involving complex targets, or the possibility for camouflage, concealment and deception techniques, multi-collection capabilities may be necessary to answer a single intelligence requirement. Resource taskers will collaborate closely with resource liaison officers to identify the most appropriate assets to meet the intelligence requirement.[23] In some instances, it may be preferable to modify the constraints of the intelligence requirement to match an available asset than to pass an unachievable intelligence requirement to another organisation as a Request for Information (RFI). In addition to knowledge of dedicated ISR assets, and non-dedicated ISR assets organic to their organisation, resource taskers should be familiar with assets of higher or national organisations and the process to task them.

327. **The ISR Tasking Plan**. The ISR tasking plan is a collaborative effort between the operational staff and the intelligence staffs that aims to match requirements with specific collection assets based on a number of factors. It directly supports the Intelligence Collection Plan. Having determined which assets best suit the task, resource taskers allocate the appropriate resources.

328. **Allocation of Collection Assets**. Co-ordination is required to prioritise competing demands on the same collection capability. This includes re-allocating assets between components and the direction of one component's assets to support another as the situation requires. Coordination also ensures coherence between the collection and alternative functions of dual-role or multirole assets.

[21] Cross-cueing is the deliberate direction of a separate collector onto a target that has already been identified.
[22] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.
[23] Resource liaison officers provide intelligence and operations staffs with detailed advice relating to the capabilities and limitations of specific ISR assets.

329. **Multinational Assets**. The pooling of multinational ISR assets and their control by a central collection management organisation, using NATO or locally established procedures, ensure effective operation. Nations' individual interests and release issues may constrain interoperability, but a coalition-wide community of interest promotes collaboration and access to wider collection capabilities.

SECTION IV – PROCESSING

'*True genius resides in the capacity for the evaluation of uncertain, hazardous, and conflicting information*.'

Sir Winston Churchill

330. Processing comprises the extraction and exploitation of collected information and its conversion into intelligence. It is at the heart of the intelligence process and there is no intelligence without detailed analysis.

331. **The Aim of Processing**. Processing is the conversion of information into intelligence. Key processing tasks are:

a. Collating information for comparison.

b. Evaluating the reliability of sources.

c. Evaluating the accuracy of information.

d. Analysis and integration of information and intelligence.

e. Interpreting information and intelligence.

f. Producing intelligence.

g. Re-processing in the light of new information or intelligence.

Figure 3.5 illustrates the components of intelligence processing.[24]

[24] Extracted from the *Principles of Defence Intelligence Analysis* (PODIA) (2nd Edition), October 2006.

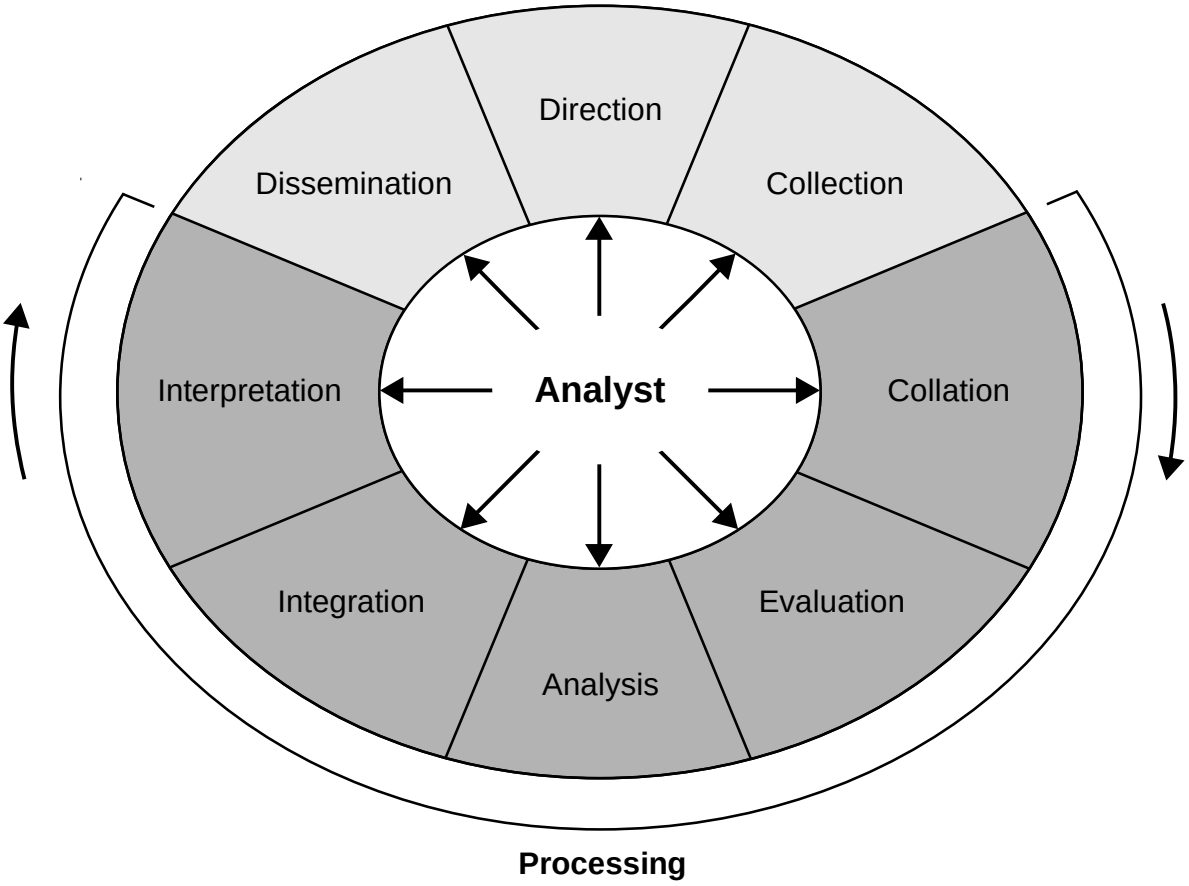


Figure 3.5 – The Components of Intelligence Processing within the Intelligence Cycle

Collation

332. Collation is *a step in the processing phase of the intelligence cycle in which the grouping together of related items of information provides a record of events and facilitates further processing*.[25] In practice, it is made up of the procedures of receiving, grouping and recording all reports arriving with the intelligence staffs at any level. Specifically it involves:

a. Registering the receipt of incoming information and intelligence.

b. Placing each piece of information or intelligence into an appropriate category or group. This can be done by logging the information, marking on a map or chart, filing or indexing, or through the entry into an electronic database.

c. Maintenance of the collation process to ensure it is carried out rapidly and efficiently.

[25] AAP-6.

333. **Collation Databases**. At its simplest, collation may involve no more than the maintenance of a log and a marked map or chart. However, in the future as the sophistication of intelligence collection increases, collation system should be automated and use electronic databases linked to graphic interfaces and high-speed automatic data transmission. As a basic principle, the use of graphical displays of information will aid intelligence staff in acquiring the maximum amount of information in the shortest possible time. Within the collation system: the type of operation conducted; the intelligence requirements of the commander; and the volume of information expected will affect the categorisation of information and intelligence groups.

Evaluation

334. Information may not be reliable or accurate, for example because of deception, subjectivity or bias or due to lack of sufficient detail. Therefore, evaluation is defined as *a step in the processing phase of the intelligence cycle constituting the appraisal of an item of information in respect of the* ***reliability*** *of the source and the* ***credibility*** *of the information*.[26] This is fundamental to analysis, as the judgement of relative value will determine how different or conflicting reports are considered.

335. **Grading of Intelligence**. During evaluation, the reliability and credibility of information are considered independently to ensure each does not influence the other. The allocation of an alphanumeric rating reflects the level of confidence in the material. This allocation is based on experience of other information from the same source or, in the case of information produced by a sensor, on the accuracy or limitations of the particular system. However, even the most reliable sources can produce wrong information. Equally, provision of confirmed information does not indicate a reliable source. A source's expertise, motivation and access will affect both reliability and credibility. Figure 3.6 shows the grading system for source reliability and credibility. Combining values produces ratings for individual pieces of material, which indicates the degree of confidence placed upon it (for example, something judged *probably true*, from a *usually reliable* source is rated *B2*). Given their knowledge of the source or the sensor, collection assets providing material will pre-grade their information before processing by the intelligence staff. Where the collection asset or agency fails to do this, the analyst will need to make a judgement regarding credibility of the information compared to what they already know. Sometimes an analyst's wider understanding of the subject may mean that they disagree with the evaluation provided by the collector, who may not be able to contextualise in the same way or may lack the deep subject matter understanding. It is important for the analyst to share this information

[26] AAP-6.

with the collector as feedback will improve collection capability in future. Similar grading systems are used throughout the international intelligence and law enforcement communities.

Reliability of the Source		Credibility of the Information	
A	Completely reliable	**1**	Confirmed by other sources
B	Usually reliable	**2**	Probably true
C	Fairly reliable	**3**	Possibly true
D	Not usually reliable	**4**	Doubtful
E	Unreliable	**5**	Improbable
F	Reliability cannot be judged	**6**	Truth cannot be judged

Figure 3.6 – Intelligence Grading Criteria[27]

Analysis and Integration

336. **Analysis**. Analysis is defined as *a step in the processing phase of the intelligence cycle in which information is subjected to review to identify significant facts for subsequent interpretation*.[28] During analysis, collated and evaluated information is reviewed for significant facts that will enhance understanding. These are then related to other known facts, and deductions drawn from the comparison. This aspect of processing, as with evaluation, is in practice almost totally based on human judgement, informed by subject matter expertise and is a critical point in the intelligence process. Analysts closely examine raw data, facts, statements, opinions and ideas, and then combine them to determine their meaning, relevance and significance.[29] This analysis is converted into an intelligence picture or assessment for dissemination. Analysis normally requires personnel, often with responsibilities for separate but related themes and topics, to analyse and integrate data, information and intelligence from a series of sources and agencies.

337. **Predictive Analysis**. Intelligence should forewarn wherever possible, but prediction is the most demanding part of analysis. In addition, prediction is peculiarly susceptible to uncertainty. It is the analyst's responsibility to ensure this uncertainty is conveyed to the commander and the commander's responsibility to ensure he understands the uncertainty. Both should abstain from *hindsight analysis*, as it is always easier to deliver accurate intelligence if you know the actual answer.

[27] Known as the Admiralty Grading System in *ABCA Coalition Intelligence Handbook* dated March 2009.
[28] AAP-6
[29] For example flow of material, linkages between entities or event timelines.

338. **All Source Analysis**. Single-source analysis provides most intelligence and this can lead to unbalanced or incomplete assessments. Therefore, it is preferable to utilise as many intelligence sources as are available and appropriate when conducting analysis. All source analysis may involve material from a variety of sources, including open sources, covert sources and classified reporting. Importantly, the use of multiple sources of intelligence when conducting analysis will reduce the risk of deception and provide the most complete, accurate and objective view possible. Analysts are responsible for ensuring the fusion of collected information in order to produce all source intelligence assessments and, importantly, for reviewing assessments on receipt of new information.

339. **Avoiding Deception**. Intelligence staffs are a prime target for adversary deception. Consequently, the analyst must be suspicious by nature and not jump to conclusions during interpretation. The analyst must seek confirmation of even the most credible information from the most reliable of sources. The intelligence picture must include deductions and conclusions made during the interpretation phase. In almost every case, the resultant intelligence will lack certainty and there will be a need to acquire further information, either to confirm or to refute. Given that accountability is a growing factor on all operations, analysts should be clear about what parts of their interpretation are fact, deduction and assumption. This will not only contribute to confidence in the validity and accuracy of assessments that will drive subsequent operational activity, but it will also make it easier to identify lessons and shortcomings in analytical challenge or any subsequent examination of the analytical output. Analytical methods and techniques may expose deception or at least maintain the robustness of the assessment.

340. **Integration**. In the course of producing intelligence, integration is defined as *a step in the processing phase of the intelligence cycle whereby analysed information and/or intelligence is selected and combined into a pattern in the course of the production of further intelligence*.[30] Integration should give new significance to activities, offer new predictions of events or generate a new intelligence picture. Geospatial intelligence is a key enabler for integration that allows subsequent analysis to extract additional intelligence such as networks, patterns and trends that would not have been possible without having first integrated the initial intelligence.

[30] AAP-6.

Interpretation and Probability

341. **Interpretation**. Interpretation is defined as *the final step in the processing phase of the intelligence cycle in which the significance of information and/or intelligence is judged in relation to the current body of knowledge*.[31] It is a process of comparison and deduction based on expertise and experience. It requires the comparison or addition of new information or intelligence with existing material to produce a fresh or updated intelligence assessment.

342. **Probability**. A rigorous understanding and interpretation of uncertainty is central to robust intelligence analysis. Many factors influence an analyst's assessment of the probability that a hypothesis is true, or that an outcome will occur. These include the frequencies of those kinds of events, the strength and reliability of indicators related to the specific topic or event, the confidence that the analyst has in the source material relating to those indicators and the extent of intelligence coverage.

343. **Uncertainty Yardstick**. It has been repeatedly shown that individual interpretations of probabilistic language (such as *likely* and *probably*) vary widely. To avoid misinterpretation and misrepresentation, analysts should make clear exactly what they mean when they use such terms. Defence Intelligence mandates the use of the *uncertainty yardstick* (see Figure 3.7), which indicates to customers a probability range against a standardised qualitative term for each intelligence product.

Qualitative Term	Associated Probability Range
Remote *or* highly unlikely	Less than 10%
Improbable *or* unlikely	15-20%
Realistic probability	25-50%
Probable *or* likely	55-70%
Highly probable or highly likely	75-85%
Almost certain	More than 90%

Figure 3.7 – Defence Intelligence Uncertainty Yardstick

344. **Legal Compliance**. Intelligence reports produced by analysts are often used by commanders when making decisions about the selection of targets for lethal prosecution. In making these decisions, the commander is required to

[31] AAP-6.

satisfy the standards given within the Law of Armed Conflict. When analysts produce material for the commander or his staff to use in targeting activities, both the sources of the information, the intelligence grading criteria and the level of probability should be included in a clear and unambiguous format.

Validation

345. **Process Validation**. It is difficult to evaluate the success of an assessment before the event, but using structured analytical approaches can avoid analytical biases and provide a clear intellectual audit trail for judgements made in all-source intelligence assessments. A number of methods can validate analytical process, but these will vary between organisations depending on their role, together with the nature and importance of the assessment. For example, intelligence staffs may choose to have a separate team that seeks to directly challenge or test important all-source intelligence assessments, or help analysts to do so, before they are finalised and issued to customers. Where appropriate this can involve external experts, such as academics, who may have a different perspective. Useful techniques and approaches include:

a. **Key Assumptions Check**. This involves breaking down an analytic line into the individual assumptions underpinning it and then testing these using a series of questions. If too many unsupported or questionable assumptions are identified an assessment may require revision before release.

b. **Devil's Advocacy**. This involves drawing on the same information underpinning an assessment and using it to disprove rather than prove the hypothesis. This process should help test the assumptions underpinning an assessment, expose any potential weaknesses in it, and allow revision before the assessment's release.

c. **Red Teaming**. The term *red teaming* has different nuances in the context of intelligence analysis and different organisations are likely to approach it in different ways depending on the precise issue at hand. Fundamentally, it involves setting up a team or teams of players to get into the mind of an opponent to think through in a structured manner their likely policy or strategy. The military approach to red teaming specifically involves playing the adversary as effectively as possible to test plans, capabilities and concepts. Red teaming can help analysts avoid a number of biases; in particular mirror imaging, which is the tendency to assume that others will act much in the same way we would under similar circumstances. The involvement of red team members who share the ethnic background of the protagonist or who at

least have experience of the culture can enhance the output of red teaming activities.[32]

d. **Peer Review**. A peer review is a common validation approach often used prior to the issue of assessments. It includes a review by seniors and peers. Such reviews focus on how well an assessment's judgements are supported or argued and whether alternative outcomes have been considered.

SECTION V – DISSEMINATION

'*Intelligence without communication is irrelevant.*'

General A M Grey, US Marine Corps

346. Getting intelligence to the user at the right time and in the appropriate format is the key to successful intelligence operations. Therefore, information requirement management is as vital in the dissemination phase as it is in direction and collection. Wherever possible, initial tasking should include the requirement for direct dissemination and the means by which this should be achieved. It is vital to have a system whereby the status of each intelligence requirement can be tracked to confirm whether it has been satisfied or requires further tasking. This mechanism will also ensure that the demander confirms receipt of the report.

347. It is important for intelligence staff to manage continuously the dissemination process. Without effective management, communications paths can become saturated by information. For example, single-source reporting may be re-transmitted by many intermediate collection agencies, resulting in *circular reporting*. Advances in technology are also affecting dissemination. Computers and modern communication systems have reduced the information-to-production timeline for delivering ISR products. Likewise, some collection systems are capable of disseminating collected information to requesters on a real-time or near real-time basis, vastly increasing their responsiveness.

Factors Affecting Dissemination

348. **Formatting**. After determining who needs to receive each report, intelligence staffs must determine how much of the report each user requires and in what format. Considerations include the commander's requirement, speed of transmission, the available bandwidth, legal restrictions and protective marking.

[32] Greater detail is provided within the DCDC Guidance Note *A Guide to Red Teaming*.

349. **Push and Pull Principles**. Intelligence can be disseminated by 3 methods: verbal briefing, printed material and web-based.[33] Dissemination consists of both *push* and *pull* control principles. The *push* concept allows higher formations to push information down to lower levels of command to satisfy intelligence requirements and for lower levels of command to push intelligence upward. The *pull* concept involves direct electronic access to databases, intelligence files or other repositories by intelligence organisations at all levels of command. Intelligence products should be organised and presented using web-based technologies and standards. This includes operational support pages, which link related intelligence products and operational information on a single web page.

350. **Principles of Dissemination**. Dissemination is governed by the following principles:

a. **Timeliness**. There are 2 aspects to timeliness. The first is when dissemination is too late for an intended purpose and is thus redundant. The second refers to intelligence that is time sensitive, where accuracy decays or the information loses its value with the passage of time. Both aspects drive the requirement to deliver intelligence to its intended user as quickly as possible. Intelligence product must detail when the truncation of processing was required to meet deadlines so that the user may treat it with an appropriate discretion.

b. **Appropriateness**. Disseminated intelligence should enhance understanding and be in an accessible format. Effective information IRM&CM will ensure the appropriateness of intelligence to meet the user's needs, that it is intelligible and disseminated across a suitable system. If it fails to do so, it will be worthless.

c. **Urgency**. Whenever possible, information should be converted into intelligence before dissemination because the interpretation of the facts is often more valuable than the facts themselves. However, when time is at a premium, processing of information may not be possible and dissemination should be as quickly as possible, with the caveat that it is unprocessed and may not be reliable. This applies particularly to urgent operational information and intelligence at the tactical level.

[33] Printed material includes intelligence reports, intelligence summaries, maps and imagery intelligence reports. An Intranet-hosted website can store multiple forms of information and may allow demanders to conduct their own intelligence requirement management. The effectiveness of a web-based database is dependent on its management and the quality of the inputs.

d. **Distribution**. Intelligence staffs are responsible for ensuring the dissemination of all information and intelligence to those who need it, including flanking or neighbouring formations. The commander and his intelligence staff may require the distribution of additional summaries of intelligence to other agencies and formations outside the normal chain of command such as governmental departments. Commanders should ensure that suitable capabilities and processes are in place to enable effective distribution to occur.

e. **Security**. Intelligence should not be over-classified. Over-classification causes delays in handling and transmission. Care must be taken not to reveal the source of information needlessly, though there will be occasions where the risk of compromising the source will have to be weighed against the value of the information. On such occasions, the intelligence staff will have to make recommendations on the impact of possible compromise to assist the commander in making a decision. Special arrangements will be required to ensure effective intelligence exchange between allies and occasional partners. The classification of the product must reflect its content and the final arbiter of this will be the agency supplying the information.

Dissemination Procedures

351. **Virtual Knowledge Databases**. Completed intelligence reports recorded in a database allows the searching and retrieval by other headquarters staff. Intelligence staff should establish an audit trail recording who has received what information to ensure that users receive each report only once to avoid multiple event reporting. Where possible, intelligence staff should create a *virtual knowledge database* consisting of interconnected intelligence databases to simplify access to intelligence in multiple databases, guarantee data integrity and speed dissemination.

352. **Dissemination Issues**. Dissemination is reliant on the availability of suitable accredited systems to process the information and have sufficient bandwidth to transport data between disparate locations. In addition, security procedures must ensure personnel viewing the intelligence produced have the necessary security clearances. The IRM&CM staff must consider the means of dissemination on receipt of the original intelligence requirement. They must also check with the demander the format in which they want to receive an answer, as well as checking they have the means to receive it.

353. **Evaluating Reports**. Evaluating reports will determine how well the intelligence process is satisfying the commander's and others' intelligence requirements. Reports should be synchronised with the tempo of the

operation. IRM&CM staff should review the relevance, completeness and timeliness of each report.

354. **Quality Control**. Intelligence must be in a form that the recipient readily understands and can directly use. Before dissemination of a product, intelligence staff should consider:

a. **Clarity**. Visual aids (maps, drawings and diagrams) should be used to enhance the clarity of the information being discussed. A clear differentiation must always be made between facts and their interpretation.

b. **Relevance**. The information should be relevant, current and not previously disseminated.

c. **Brevity**. Brevity and succinctness help the successful dissemination of information and intelligence. Good intelligence imparts the most information in the fewest words.

d. **Security**. The briefing must be conducted within the bounds of current security policy.

e. **Ease of Assimilation**. Fused products assimilated from multiple sources are more easily and readily comprehendible than several individual products.

Reporting Formats

355. **NATO Reporting Formats**. The UK uses NATO standards for report formats and message sets to guarantee multinational interoperability. Wherever possible, written and web-based intelligence reports should follow the appropriate NATO formats, which include:

a. **Intelligence Report**. An Intelligence Report (INTREP) is sent whenever information or intelligence is urgent, and contains any deductions that can be made in the time available.

b. **Intelligence Summary**. An Intelligence Summary (INTSUM) is a concise, periodic summary of intelligence about the current situation within the Joint Operations Area (JOA). It is designed to update the current intelligence picture and to highlight important developments during the reporting period and includes any information or intelligence relevant to extant intelligence requirements.

c. **Supplementary Intelligence Report**. A Supplementary Intelligence Report (SUPINTREP) is a stand-alone summary of intelligence for a given subject or situation within the JOA. It updates the current intelligence picture, addressing a specific issue or highlighting important developments inside the normal reporting cycle.

d. **Single-Source Reports**. A number of other intelligence reports and summaries are generated periodically, for example interrogation reports and technical intelligence reports, to address specific subjects.

e. **Counter-Intelligence Reports**. Counter-intelligence (CI) reports are similar to INTREPs, consisting of CI-INTREPs, CI-INTSUMs and CI-SUPINTREPs. Counter-intelligence staffs may also produce threat assessments and threat warnings, by which commanders are informed of specific security threats.

f. **Thematic Reports**. Thematic reports address particular aspects of the operating environment, such as a region or town, a political or religious movement or a particular adversary organisation, sometimes covering longer time-scales.

356. **Other Reporting Formats**. The UK is a member of a large number of political and military alliances on both a bilateral and multilateral basis. Comprehensive intelligence exchange arrangements already exist between most of our allies and partners. In addition to NATO, intelligence specialists must be aware of other intelligence reporting formats that they may need to use. JDP 3-00 (3rd Edition) *Campaign Execution*, Annex 1B describes some of the organisations and groups that we regularly operate alongside. Intelligence specialists should familiarise themselves with the reporting formats for:

a. US-UK bilateral partnership.

b. UK and the EU.

c. UK and the UN.

d. American, British, Canadian, Australian and New Zealand Armies Programme (ABCA).[34]

[34] ABCA intelligence collection and other reporting formats are in the *ABCA Coalition Intelligence Handbook*, ABCA Publication 325.

e. Australia, Canada, New Zealand, UK and the US (AUSCANNZUKUS).

f. The Five Powers Defence Arrangements signatories: UK, Australia, New Zealand, Singapore and Malaysia.

The basic principle is for each nation to deploy with its own intelligence infrastructure and then adapt to the requirements of the organisation or coalition. This is much easier to achieve if reporting formats have been decided from the outset.

CHAPTER 4 – INTELLIGENCE SUPPORT TO JOINT OPERATIONS

'*To lack intelligence is to be in the ring blindfolded*.'

General David M. Shoup[1]

Chapter 4 describes intelligence support to joint operations at home and overseas. It specifically considers national military tasks and the range of military activities that intelligence has to support: the joint operational environment; intelligence support to homeland security and defence; and intelligence support to operations overseas.

SECTION I – JOINT OPERATIONS AND INTELLIGENCE

401. A national security policy or theatre-specific policy should provide strategic direction for future joint operations. Joint operations are operations in which the elements of more than one Service participate and may involve maritime (including amphibious), land, air, space, cyber and special forces. The joint operational plan synchronises and co-ordinates these forces in the operational theatre or for a specific operation.

402. **The Focus of Operational Intelligence**. The focus of operational intelligence is to assist the operational commander's decision-making by enhancing his understanding.[2] This applies equally to national and coalition operations. Operational intelligence provides commanders with the information and analysis to make decisions and contributes to the planning and execution of operations.

SECTION II – THE RANGE OF JOINT MILITARY TASKS

403. The Strategic Defence and Security Review (SDSR) promulgated the primary military tasks (Figure 1.1 refers) in 3 categories: prevention; crisis; and war. Within each of these are a number of possible military tasks and activities. The emphasis on intelligence and the lead agency changes for each task or activity.[3] This necessitates the development of a proactive and responsive intelligence organisation.

[1] Former Commandant of the United States Marine Corps.
[2] Chapter 2 defines operational intelligence.
[3] For example, in a counter-insurgency operation, the requirement for intelligence staff down to the lowest level will increase. The size of the understanding and intelligence network, and the range of experts required in such disciplines as tribal dynamics and languages, will also increase.

Homeland Security and Defence

404. **The Military Network and Homeland Defence**. There is already co-operation between the various national agencies both centrally and at regional level for the defence of the UK. Details of the UK's Homeland Security and Defence infrastructure, legal basis and operating framework are in JDP 02 *Operations in the UK: the Defence Contribution to Resilience* and are summarised in this section. The legal framework for all military support including intelligence support reflects the Civil Contingencies Act 2004, the Emergency Powers Act 1964 and the Armed Forces Act 2006.

405. **Intelligence Support to Joint Operations in the UK**. Intelligence support for joint operations in the UK comprises:

a. **Homeland Security and Homeland Defence**. There is a legal distinction between homeland security and defence. Homeland security is primarily a Home Office function concerned with maintaining law and order. MOD is responsible for the defence of the Homeland from physical attack. Defence Intelligence ensures the sharing of intelligence obtained for homeland security and defence with the appropriate UK agencies.

b. **Support to the Civil Ministries**. Military Aid to the Civil Authorities is the collective name for UK military assistance to civil ministries. Specific intelligence support may be necessary, particularly when the military operate in direct support of the civil power. There are 3 specific types of assistance:

(1) Military Aid to other Government Departments: examples include providing fire coverage during a fire fighters' strike or support to local government during a *foot and mouth* epidemic.

(2) Military Aid to the Civil Power: direct support to the police such as in Northern Ireland.

(3) Military Aid to the Civil Community: such as in the event of flooding and other natural occurrences or disasters.

Joint Operations Overseas

406. **Intelligence Support to Joint Operations Overseas**. In an interconnected world, events overseas may have an effect on security in mainland UK and *vice versa.* During national, alliance or coalition operations, the deployed intelligence staff must have links into the UK intelligence community (including those involved in counter-intelligence). This includes

other government departments (for example the Foreign and Commonwealth Office, Department for International Development, Department for Trade and Industry), academia, allies (including coalition partners), international governmental organisations (for example the UN) and non-governmental organisations.

407. **Intelligence Architecture**. Subordinate commanders employ their assigned intelligence capabilities to support their mission. At the same time, those capabilities must be available to assist the joint effort. The intelligence staff should establish flexible and task-orientated intelligence architecture to focus on the commander's needs. This intelligence architecture should complement and reinforce the assigned capabilities at each echelon and provide direct support to subordinate commanders whose assigned capabilities may be inadequate.

408. **Use of Intelligence Assets**. Intelligence is a multi-source activity and requires the use of many resources. The UK Joint Force Commander within a coalition will need to share UK assets and intelligence as much as he expects to receive support from the lead nation. Intelligence assets provided by the UK to support the operation will probably form part of a much larger national and coalition network. The commander must know the intelligence assets assigned to his force and how he can access non-assigned assets.

SECTION III – INTELLIGENCE SUPPORT TO UNDERSTANDING

409. Areas where intelligence staffs support the development of understanding include:

a. **Horizon Scanning**. Horizon scanning is *the systematic search across the global environment for potential threats, hazards and opportunities*.[4] Horizon scanning may also provide an innate audit function to identify weaknesses in current assessments or policies, but it is not amenable to specific tasking requirements. In the UK, horizon scanning is a Cabinet Office lead in conjunction with the Foreign and Commonwealth Office. Within MOD, Defence Intelligence is the focal point for horizon scanning.

b. **Intelligence Monitoring**. Intelligence monitoring provides an intelligence baseline on countries, regions and actors before a crisis arises. Open source material, as well as defence relations and diplomatic activity contribute to monitoring. Normally based on the results of horizon scanning, the Chief of the Defence Staff determines the Defence priorities for monitoring based on the advice of Chief of

[4] JDP 04 *Understanding*.

Defence Intelligence and drawing on requirements identified by the Joint Intelligence Committee.

c. **Situational Awareness**. Situational awareness is defined as *the ability to identify trends and linkages over time, and to relate these to what is happening and not happening*.[5] It can be improved using intelligence, including indicators and warnings, to identify trends and scan for emerging threats, hazards or opportunities. Situational awareness is the first step in developing understanding. It enables us to relate what has happened, what is happening and what might happen in the future. In particular, a commander requires situational awareness to identify the atmospherics and boundaries of a problem including the threats, opportunities and consequences of an action.

d. **Analysis**. Defence Intelligence conduct strategic analysis of threats to the UK. This analysis can provide the operational context for past, present and anticipated events.

SECTION IV – INTELLIGENCE SUPPORT TO COMMANDERS

410. **Commanders' Responsibilities**. The ultimate responsibility for intelligence rests with the commander. The commander should be familiar with the intelligence process and have sufficient situational awareness to articulate his critical information requirements. With the increasing complexities of modern military operations, commanders and their respective staff should embrace the views of subject matter experts within their headquarters, even if their views are diametrically opposed to those of the rest of the team.[6] Sensitive handling of the resulting creative tension can enhance both understanding and decision-making.

411. **Support to Strategy Formulation**. Intelligence plays a significant role in the development of military strategy. This should include assisting in the clear articulation of an end-state, goals, objectives and an appraisal of the national resources needed.

412. **Informing the Commander**. To maintain the initiative, the commander will seek to make good decisions quickly. This requires an ability to assess the adversary's decision-making cycle, identify opportunities for exploitation and to disseminate critical information. Intelligence directly supports the commander by producing assessments and reports that aid decision-making.

[5] JDP 04.
[6] Examples of subject matter experts include geographers, ethnologists, sociologists, anthropologists, economists and historians.

413. **Support to Contingency Planning**. In the military context, contingency planning means developing plans for potential military operations.[7] The starting point for all contingency plans is to develop an understanding of the strategic environment and the nature of the potential problem. Intelligence can provide this understanding if there is a coherent framework in which the capture intelligence requirements is recorded and retained in a disciplined manner that allows it to be recovered easily in the event of a crisis. This can provide the foundation data that is required when activating or revising contingency plans.

SECTION V – INTELLIGENCE SUPPORT TO JOINT ACTION

414. *Joint action* is *the deliberate use and orchestration of military capabilities and activities to realise effects on an actor's will, understanding and capability, and the cohesion between them to achieve influence*.[8] It is implemented through coordination and synchronisation of: fires (physical or virtual means to realise primarily physical effects); information activities (manipulation of information or perceptions of information to affect understanding); manoeuvre (gaining advantage in time and space); and outreach (including stabilisation, support to governance, capacity building, and regional and key leader engagement).[9]

Anti-piracy Operations off the Coast of Somalia

[7] A contingency plan is defined as *a plan which is developed for possible operations where the planning factors have been identified or can be assumed. This plan is produced in as much detail as possible, including the resources needed and deployment options, as a basis for subsequent planning*. (JDP 0-01.1 *United Kingdom Glossary of Joint and Multinational Terms and Definitions*).
[8] JDP 3-00 (3rd Edition) *Campaign Execution*.
[9] Joint Action is explained in detail within JDP 3-00 (3rd Edition).

415. Intelligence is pivotal to joint action. It allows the commander to conduct his decision-making on the basis a comprehensive understanding. It helps to both frame the problem and illuminate its specific elements. Traditionally, intelligence has focused on 2 overlapping and complementary subjects, the actors (their characteristics, culture, capabilities, locations, intentions, relationships and objectives) and the physical environment (geospatial) within which they operate.[10] In the contemporary operating environment, there is also the *information environment* (how the actors receive information and transmit their narratives).

416. Intelligence staff should provide the commander with:

a. Intelligence that locates the components of a target and indicates its vulnerability and relative importance.[11] At the operational and tactical levels, intelligence will support the deliberate targeting process for the full spectrum of lethal and non-lethal options to meet the commander's objectives, including information operations.[12]

b. Tactical intelligence, which can support ongoing tactical offensive operations. This intelligence should have an emphasis on the timely passage of critical intelligence for target development. This includes advice on the selection of targets based on the commander's priorities.

c. Intelligence that informs those activities seeking to affect the character or behaviour of an individual, group or organisation.

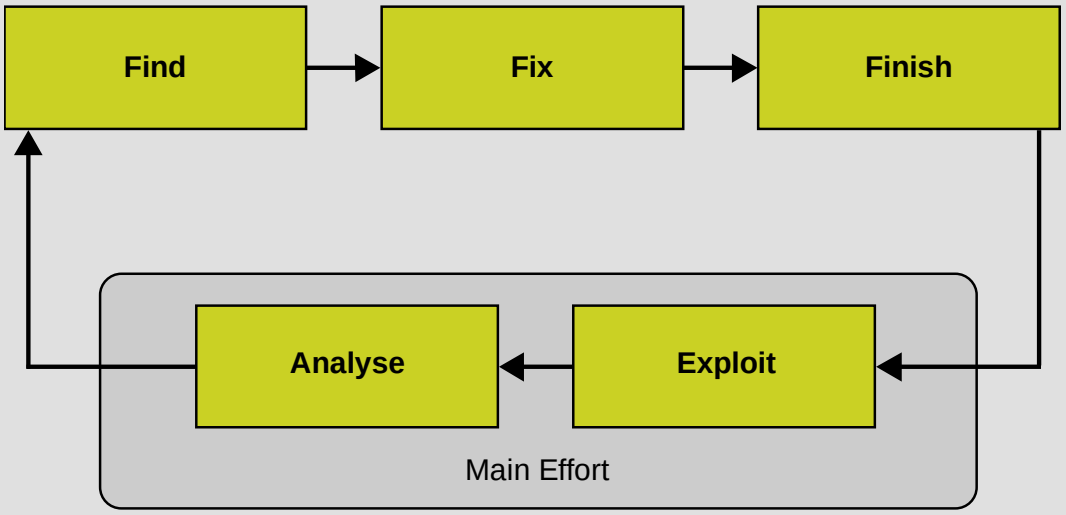
d. Analysis of acts of deception conducted by an adversary.

[10] Actors refer to friends, neutrals and adversaries.
[11] A target is *the object of a particular action, for example a geographic area, a complex, an installation, a force, equipment, an individual, a group or a system, planned for capture, exploitation, neutralisation or destruction by military forces*. (Allied Administrative Publication (AAP)-6, *NATO Glossary of Terms and Definitions* (2010).)
[12] Targeting is *the process of selecting and prioritising targets and matching the appropriate response to them taking into account operational requirements and capabilities*. (AAP-6)

Intelligence Support to Joint Action – The F3EA Framework

A model devised by Special Forces treats each actor in the operating environment (particularly adversaries) as distinct systems. These systems are interrelated to provide a holistic view and a better understanding of the overall environment. The model identifies areas and points in the systems that are suitable for the application of power or influence.

The model consists of the generic operational *Core Functions* (*Find*, *Fix, Finish, Exploit* and Analyse or F3EA). Although developed principally to deal with specific adversaries, the method works equally well with a much wider range of target sets.



Find. The locating and assessment of adversaries is critical. This includes physical locations, motivations, movements, capabilities and networks. A systematic approach and long-term investment is required to build the understanding of a particular system.

Fix. Once found, the target can be fixed either by physical force or less intrusively by the use of intelligence collection assets. This expands understanding of the target and provides the commander with more options for the *finish* phase.

Finish. The commander may want to assault the target (kill or capture) to remove it from the system. Alternatively, an indirect approach may be more useful, for example to recruit an element of the adversary's network.

Exploit. Exploitation of intelligence opportunities includes interrogation or document examination to feed the analysis process.

Analyse. Analysis is a continuous and dynamic process comprising the fusion of materiel and personnel exploitation with existing intelligence. This analysis provides new intelligence that enhances understanding. Based on this understanding the command provides the start points for further *find* activity.

SECTION VI – INTELLIGENCE SUPPORT TO MONITORING AND EVALUATION

417. **Monitoring**. Monitoring is the process of tracking changes in the environment. It is the continually gathering and interpreting of information to maintain situational awareness, to develop insight why something is happening, and knowing what activities have been conducted, are underway or are planned or indicated. Monitoring helps identify the extent of a plan's implementation and the achievement of objectives. It can also track the status of critical assumptions identified within the planning process.

418. **Evaluation**. In the operational context, evaluation is the observation and interpretation of progress towards desired conditions against selected criteria. It draws on monitoring. Evaluation allows commanders and staffs to develop insight on successes or failures. This allows the development of the foresight required to make decisions to continue on the same trajectory or to change course.

419. **Intelligence Support to Evaluation**. Intelligence can provide an evaluation of progress, based on subjective and objective measurement to inform decision-making.[13] Intelligence provides direct support to evaluation through:

a. **Measurement of Effect**. Measurement of effect is *the assessment of the realisation of specified effects*.[14] It examines whether or not the operation or campaign is achieving its purpose and if the logic of the operation is plausible, complete and accurate. It monitors and assesses progress, including setbacks, to support planning decisions.

b. **Measurement of Performance**. Measurement of performance evaluates task performance at all levels of war. It effectively measures task accomplishment (for example, how the maritime force performed against its given mission tasks within the joint operational plan). In partnership with other staff branches, intelligence staffs at strategic and operational levels may be required to produce assessments that provide the commanders with agreed measurements of performance. The focus for the intelligence staff will be the impact of joint operations on an adversary. It normally consists of an informed narrative assessment by intelligence staff (for example, the success of the air campaign in achieving control of the air could be assessed by the

[13] JDP 01 (2nd Edition) *Campaigning*.
[14] JDP 3-00 (3rd Edition) *Campaign Execution*.

number of effective attacks conducted by an adversary against friendly forces since the commencement of the air campaign).

c. **Measurement of Activity**. Measurement of activity focuses on answering whether we successfully accomplished the things we planned and if an activity should be repeated or altered. In general, there is a quantitative and qualitative nature to measurement of activity. Commanders may draw on measurement of activity to inform decisions, but it is essentially tactical business. Measurement of activity is reviewed within the daily campaign rhythm, under the activity review cycle. Battle damage assessment is the most common form of measurement of activity.

d. **Battle Damage Assessment**. Battle damage assessment consists of physical damage assessment, functional damage assessment and target systems assessment. It is defined as *the timely and accurate estimate of damage resulting from the application of military force either lethal or non-lethal, against a pre-determined target*.[15] Such assessment is primarily an intelligence staff responsibility, but links into the targeting process. The production of battle damage assessments will give rise to a series of post-attack intelligence requirements. Intelligence staff should establish effective procedures to support the battle damage assessment.

420. **Intelligence Assessments**. Intelligence assessments are critically important for enabling the commander to measure progress towards mission accomplishment. The intelligence staffs should assist the commander to establish joint and interagency assessments. This will include assessments against progress in the political, diplomatic, economic, rule of law and security spheres of activity, with specific measurements for campaign objectives and decisive conditions. The method and criteria behind the assessments must be coherent across the joint task force. To ensure coherence, the commander and his staff design and agree measurements and assessments during the operational planning process. Assessments provide the information on campaign progress that MOD requires before making further strategic decisions and direction. Therefore, the joint task force commander must ensure that higher-level commanders understand the assessment system. Example measurement and assessment criteria may include:

a. Adversary capabilities, vulnerabilities and intentions.

b. The impact of the results of elections.

[15] JDP 0-01.1.

c. Impact of the death of a respected leader.

d. Access by the general population to common law (i.e. the right to own property and land).

e. Economic progress (i.e. the creation of new businesses).

f. The provision of basic services such as medical care, sanitation, water and power.

g. Diplomatic representation overseas. This includes the establishment of embassies and the development of cordial relations with neighbouring countries.

SECTION VII – UNDERSTANDING THE JOINT OPERATIONAL ENVIRONMENT

'*. . . information which is persistently collected and compiled in peacetime, should enable an intelligence officer to enter a campaign with a practical knowledge of the strength and condition of the enemy's available forces, of the nature and capabilities of the country in which fighting [the operation] is likely to take place, and of the disposition and temper of its inhabitants.*'

Brevet Lieutenant Colonel David Henderson DSO, 1904[16]

421. An environment is *the surroundings in which an organisation operates, including air, water, land, natural resources, flora, fauna, humans and their interrelation*.[17] The Joint Operational Environment (JOE) is defined as *the overall space, conditions and surroundings within which military forces operate*.[18]

422. **Joint Operations Area**. The Joint Operations Area (JOA) is defined as *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.*[19] This definition delineates an area of responsibility given to a specific command structure.

[16] Brevet Lieutenant Colonel David Henderson DSO, Argyll and Sutherland Highlanders: *Field Intelligence, Its Principles and Practice*, HMSO 1904.
[17] AAP-6.
[18] New UK definition established in JDP 2-00 *Intelligence and Understanding* (3rd Edition) and awaiting formal approval by NATO.
[19] JDP 0-01.1.

423. **Joint Intelligence Areas**. To enable the commander and his intelligence staff to focus their intelligence effort, the JOA is divided into 2 areas:

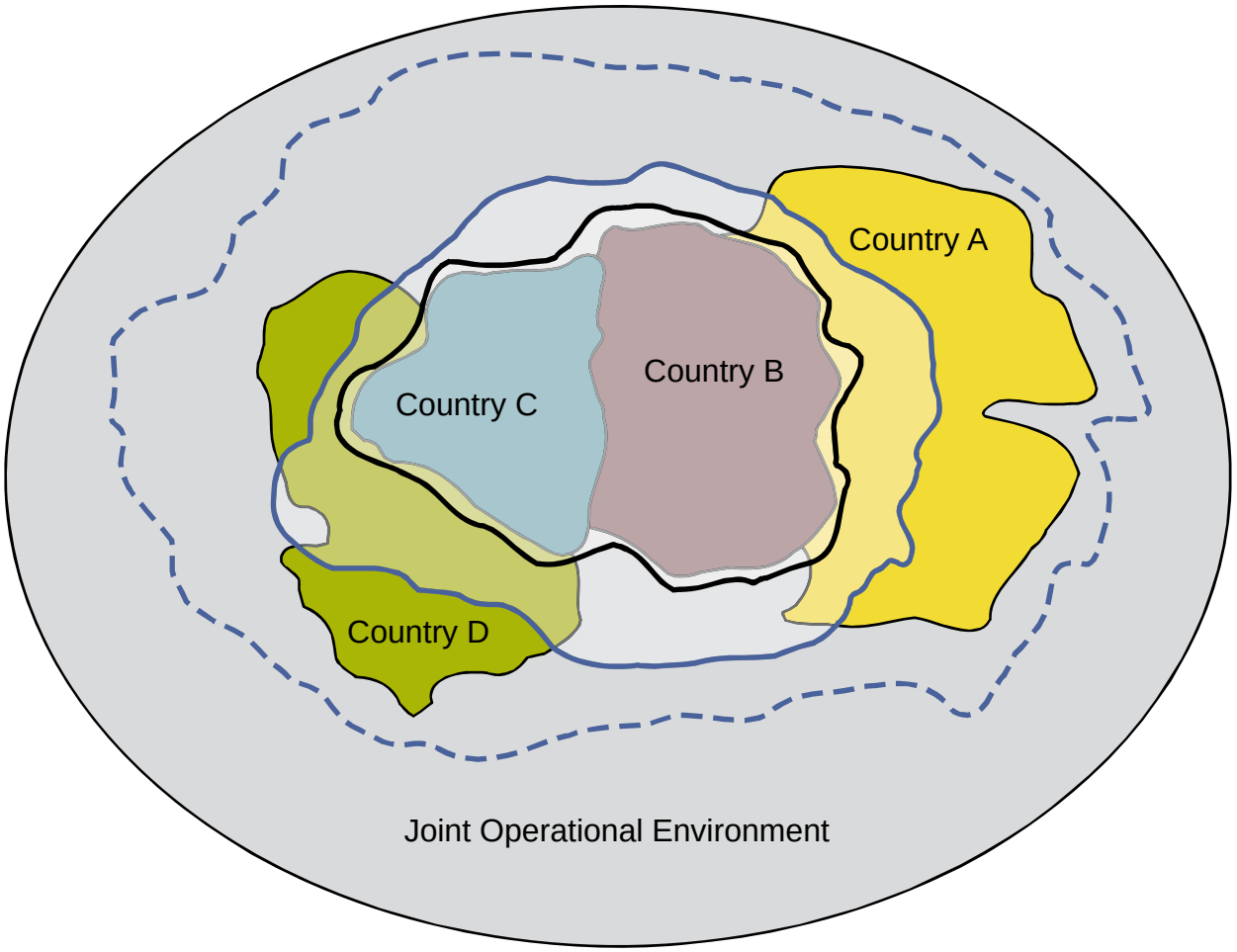
a. **Area of Intelligence Responsibility**. The area of intelligence responsibility is *an area allocated to a commander, in which he is responsible for the provision of intelligence, within the means at his disposal*.[20] It encompasses the area in which adversary actions can directly affect the commander's forces and to which he can respond using his assets. In practice, the nature of the commander's assigned collection capabilities will determine the allocation of the area.

b. **Area of Intelligence Interest**. The area of intelligence interest is *the area in which a commander requires intelligence on those factors and developments likely to affect the outcome of his current and future operations*.[21] The commander is not responsible for intelligence collection capability in the area. However, higher or neighbouring formations should provide answers to his intelligence staff's questions pertaining to the area. The area of intelligence interest is likely to include locations where an adversary's actions will influence the commander's decisions, but he is not required to respond with his assets. The area need not be geographically contiguous and there may be areas outside the main area of intelligence interest that could exert influence on the JOA.

424. **Cyberspace**. As an operating environment, cyberspace transcends our traditional concepts of geographic and political boundaries. It forces commanders to consider operational functions or responsibilities rather than a geographical area. Commanders' should consider cyberspace to be an area of intelligence responsibility in its own right.

425. **The Operational Environment and Operations Area**. The JOA is the designated area of command in which a commander exercises control of the forces designated to him. The JOE captures the wider bounds of the JOA where commanders can exert influence. Therefore, the JOE constitutes the physical, human and virtual environments with which a joint task force commander exercises his authority and the physical or conceptually adjacent areas within which activity can influence success or failure for an operation. Figure 4.1 graphically demonstrates these relationships.

[20] AAP-6.
[21] JDP 0-01.1.



Legend
Joint Operations Area
Area of Intelligence Interest
Area of Intelligence Responsibility

Figure 4.1 – The Relationship between the JOE, JOA, Area of Intelligence Responsibility and Area of Intelligence Interest

426. **The Human Domain**. The human domain is *the totality of the human sphere of activity or knowledge.*[22] It represents the interaction between human actors, their activity and their broader environment. The human domain therefore consists of the operating environment (whether that is at the global, regional, national or local level) created by the interplay between 4 sub-environments, and the actors and activities that affect or are affected by it (global, state, non-state and local). The 4 sub-environments are:

a. **The Cultural Environment**. Culture covers the most general and pervasive ideas of a society such as language, historically rooted

[22] JDP 04.

concepts of collective identity and fundamental existential and moral beliefs such as those provided by religion.

b. **The Institutional Environment**. The institutional environment forms the landscape of social life and the organised activity required to develop and implement technology and infrastructure.

c. **The Technological Environment**. The technological environment covers information, communications and technology that have evolved from the actors' interaction with and because of their environment.

d. **The Physical Environment**. The physical environment provides both the raw materials for survival and many of the most significant challenges to that survival.

427. **Actors**. While the focal point for understanding is the roles that people enact on the global stage, as states, non-state actors, populations, organisations, groups and individuals, it is not the only point of focus. Actors must be set within their cultural, institutional, technological and physical environments to provide the context for developing a better understanding of their motivations fears and perceptions.

428. **The Interdependency of Human Domain Environments**. The cultural, institutional, technological and the physical environments can overlap in many areas. Certain religions have prescribed specific institutional arrangements such as religious courts. Technologies are intimately interwoven with the institutions, which provide them (such as manufacturing firms) or regulate them. The physical environment fundamentally shapes many communication and transportation technologies. Economic affairs seem to lie at the very centre, overlapping the technological in terms of real assets (from farms to factories) and the institutional in terms of currency exchange and regulatory frameworks for that exchange (contract law). More fundamentally, *everything* in the human domain is conducted in terms of underlying cultural media such as language and almost everything in the cultural sphere is, at some level, about how humans go about surviving in the physical world and their place in that world. Figure 4.2 shows the interaction between human actors, their activity and their broader environment.

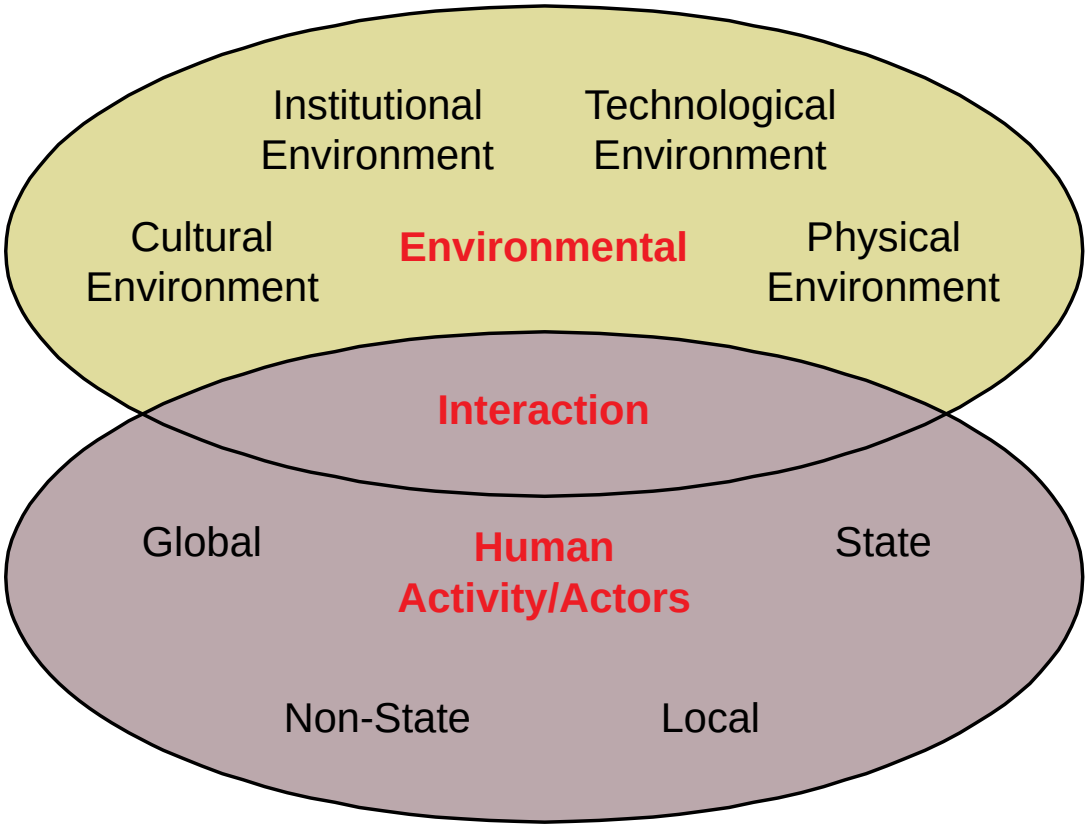


Figure 4.2 – The Human Domain

429. **Analysing the Joint Operational Environment**. Analysis must consider all aspects of the operating environments and the people who live, work and fight within them. The human domain framework focuses on the factors that help us to understand the relationship between actors, their environment and their activities both within a global and situation-specific context. The terms maritime, land, air and space refer to the physical environments in which we conduct intelligence activity, but what we are seeking to understand is the human domain. Although the traditional focus for military activity is the physical environments, the people among whom we conduct operations live in these environments and it shapes their attitudes and behaviours. In the contemporary operating environment, rarely is a military operation limited to one of these environments and even consideration of the physical environments must include understanding of their interrelationship. Nevertheless, the physical environments do have a distinct impact on the way that our maritime, land and air forces conduct operations and organise themselves. Section VIII considers the distinct differences between each physical environment.

SECTION VIII – THE EFFECT OF THE PHYSICAL ENVIRONMENTS ON UNDERSTANDING AND INTELLIGENCE CAPABILITY

430. **The Maritime Environment**. In the maritime environment, operational areas can be vast and often opaque to normal observations. For example, a surface unit moving at 20 knots covers 480 nautical miles (well over 500 statute miles) per day. Precise sensor details are unimportant, but if a ship were monitoring activity out to 250 miles from its track, it would be traversing almost 250 000 square miles per day, an area about the size of France. These factors strongly influence maritime intelligence gathering. Historically, the maritime environment shapes the character of land-based populations. Thus, it will often form part of the context for understanding and intelligence. The key factors affecting military operations are:

a. **Legal**. The complex legal regime of maritime zones (for example the territorial sea, contiguous zone and exclusive economic zone) and freedom of navigation on the high seas must be understood as the defining context for gathering commercial information or military data, as well as visiting and searching vessels.

b. **Natural Resources**. The enduring importance of the maritime environment for exploiting natural resources and providing energy supply routes will increase the potential for friction and dispute.

c. **Maritime Capability**. The characteristics of a nation's maritime capability, civil as well as military, may offer insight into national aspirations, as can its ability to exploit maritime resources. Underwater sensors can contribute significantly to situational awareness at sea, while surveillance from the air or from space can address some of the problems posed by scale and area. The maritime domain also offers a haven for discrete observation of coastal areas and adjacent airspace with a minimal footprint on land.

d. **Maritime Intelligence**. Due to the nature of maritime operations, particularly in the littoral, maritime intelligence must embrace both the air and land environments. The principal focus for maritime intelligence is shared situational awareness through the near real-time fusion of multiple intelligence sources, such as communications intelligence, electronic intelligence, imagery intelligence and acoustic intelligence. In the maritime environment, there is a heavy reliance on technical intelligence gathering capabilities and a reliance on other national agencies or allies.

431. **The Land Environment**. The defining characteristics of statehood, territory and a permanent population are only meaningful on land.[23] It provides the basis for territorial claims, sources of livelihood and historical narratives. Consequently, almost all intelligence and understanding tools are associated with the geography. Intelligence factors for consideration are:

a. **Technology**. Technology enables populations to exploit their surroundings, whether by facilitating access, enabling agriculture, supporting industry or providing transport. The tangible aspects of national technical capability, such as likely performance of systems and sustainability of industrial sectors are natural subjects for intelligence.

b. **Geography**. Military practitioners have understood the importance of geography since ancient times. This includes the use of terrain for cover or for observation, the constraints on movement enforced by obstacles that give rise to preferred routes and passes, or the influence of climate and other environmental factors.

432. **The Air Environment**. The fact that the air environment covers both the maritime and land environments has enduring implications for intelligence activity. The key factors affecting intelligence are:

a. **Operating Restrictions**. No general right of over-flight exists over land. This can give nations the ability to regulate the aerial reconnaissance activity of other nations if they are not at war. Conversely, deliberate unauthorised over-flight over another country can also lead to conflict.

b. **Technology**. The platforms operating in the air environment can have speed, reach and height, which are all virtues for reconnaissance. However, there are corresponding weaknesses of impermanence, limited payload, fragility, cost, basing constraints and vulnerability to weather.

433. **Space**. Reconnaissance and surveillance were the earliest drivers for the development of satellites and are still important. The biggest change in the use of space is not the nature of the operations carried out, but rather how access to space has proliferated. Originally exploited only by the superpowers, the numbers of nations (and indeed in some cases non-state actors) with direct or indirect access to space has increased rapidly. The capability of the commercial space sector has also increased dramatically, and

[23] The Montevideo Convention on the Rights and Duties of States (1933) lists the 4 defining characteristics of statehood as a permanent population, a defined territory, a government and the ability to enter into relations with other states.

actors without an indigenous capability, or access to that of an ally, may now be able to purchase access commercially. This trend is likely to increase. The key factors for intelligence are:

a. **Military Reliance on Space**. Given its use for surveillance and reconnaissance, the factors outlined for air are also relevant to space.

b. **Space Law and Over-flight**. Unlike air, there are no legal restrictions on over-flight by satellites of sovereign territory. Indeed, this was one of the reasons for the development of space-based reconnaissance and surveillance.

c. **Technology**. The high level of technical proficiency required to exploit space has constrained some actors, but the benefits, both tangible and intangible, of success continue to encourage and reward effort. Understanding activity in space is technically challenging, but the need for effective warnings and indicators of such activity is undiminished.

SECTION IX – ANALYSIS OF THE VIRTUAL ENVIRONMENT

434. **Cyberspace**. Cyberspace is a channel of communication between people. The growth and popularity of the Internet has allowed dispersed groups of people with shared interests to interact on-line in ways not possible using only telephones and postal systems. Cyberspace has become a normal part of everyday culture and society. It largely reflects regular human experiences.

435. **Cyberspace Threats**. A human creation, cyberspace is not a fixed entity and almost everything within it is changeable. Manipulation of technologies, by either hacking or installing hardware, can have either a virtual or a physical effect that can pose a real danger to a variety of institutions, including the critical national infrastructure, communications and intelligence gathering. Furthermore, despite technical challenges, cyberspace provides states with advanced propaganda capabilities, which are restricted only by the level of control a state has over its media environment. However, this is not limited to states and organisations or non-state actors, acting individually or in virtual groups, are able to conduct harmful activities.

436. **Cyberspace and Intelligence**. Networking and digitisation mean that cyberspace provides easy access to vast amounts of potentially useful intelligence. The monitoring of cyberspace and analysis of activity conducted within it can provide useful intelligence. The information available is not only personal information about actors, but often includes information about

physical activities (such as locations of nuclear facilities, power or water supply pipes). However, that the emergence of language-specific websites is expected to break up the Internet into language-specific zones, making it more difficult to navigate without language skills.

SECTION X – ANALYSIS OF THE HUMAN TERRAIN

437. **Cultural Practices and Social Structures**. It is important to examine all aspects of the human terrain, and to avoid only focusing on the obvious and different aspects of the group. Cultural practices are the things that are immediately observable in a society, such as people's style of dress, greetings and rituals, flags and other symbols. On an individual level, cultural practices manifest themselves in a person's *behaviour*. However, to understand the human terrain, we need to look beyond the immediately observable cultural practices to examine what drives or underlies these practices. These social structures are the normally invisible concepts and institutions that organise society.

438. **The Human Terrain Model**. Understanding the human terrain requires us to understand the local population's environment from their perspective. To do so we tend to create categories to structure our understanding, but we should be aware that these categories would always be to some extent artificial and separate things that in reality are interconnected. In our daily lives, we do not think about our families as being a form of social organisation, or the market where we buy vegetables as part of our society's economic organisation, and nor do any of the populations that we operate amongst. The aspects of human terrain described here (social; political; economic; beliefs; values; and interaction) simply provide one model that encourages to help analysts ensure that they have consider all significant aspects of the human domain.

439. **Social Organisation**. Social organisation refers to the basic building blocks of society. It includes the groups into which people are born, and which influence their attitudes and behaviour throughout their life. Kinship is a fundamental organising principle in all societies and the family is the group to which most people in most societies owe their first and most strongly held allegiance. Tribes and clans are essentially extended families in that they see themselves as descended from a common ancestor. On a larger scale, a person shares a language, history and usually religion with his ethnic group. Gender is also part of social organisation, as men and women usually have different roles and responsibilities in a society. Understanding the forms of social organisation in the joint operational environment is an important step in understanding those groups with influence over how people behave and the groups to which they feel allegiance.

440. **Political Organisation**. Power and politics work in different ways in different societies. The western centralised state model of political organisation, in which a bureaucracy supports a central leader who provides services to the group, is only one of a number of ways of organising control within society. Not all groups need or want the state to organise them. The segmentary political system (of which tribes are an example), in which groups come together when it suits them to do so, but may otherwise be in conflict, is another form of political organisation which operates without a centralised leader. Individuals often have power for different reasons. For some, such as the British military, power derives from a person's appointed position. In other groups, power is inherited or derived from spiritual qualities or learning. Successful engagement with people in power relies on understanding why the people around them follow their directions. Understanding the nature of political organisation in the society is essential in determining who actually holds the power and their influences.

441. **Economic Organisation**. Access to resources underpins behaviours and attitudes of all people. How resources are distributed and exchanged differs according to the group. Large-scale economic ideologies such as capitalism or socialism influence how people earn a living and obtain the things they need. However, every society also has alternative economic structures, such as the *black economy* or bartering, which people use in parallel to formal systems. Networks of patronage may be essential for supporting and linking together members of a community for mutual support. Knowing where and how people work, exchange and own things will help to ensure that any economic or development engagements are successful, as well as helping to identify pressure points on an adversary.

442. **Beliefs and Values**. Groups have shared beliefs and values that ensure the loyalty of members to the group. These may include formal ideologies or religions, which often include set roles for key individuals, and a textual guide on how to live one's life. However, informal or non-codified beliefs about the nature of the world and of society are as important for guiding how people act. Notions of what makes a good person or honourable behaviour, when loyalty is expected and how much deviance from a group's norms is acceptable are all essential aspects of a group's beliefs and values. Concepts of time and the significance of history also influence how a group acts. Understanding these values helps commanders anticipate the likely behaviour of the group.

443. **Interaction**. All groups have normal ways for their members to interact with each other, ranging from the language that they share, through their concepts of personal space, hand gestures and clothing. Differences in interaction styles are often the most obvious aspect of the human terrain.

Underpinning these practices will be concepts of what are appropriate displays of emotion, principles of hospitality and ideas of friendship, which are just as important for a commander to understand when planning operations, particularly those that rely on the cooperation of local people. Interacting with people in ways that make sense to them is far more likely to achieve the intended goals than acting in ways that they do not understand or that will cause offence. Therefore, understanding local norms and practices in interacting with others is essential for mission success.

444. **Human Terrain in Military Physical Domains**. The aspects of the human terrain described above apply to people wherever they live. For military forces, these aspects are essential for understanding the people among whom we operate, but will not be equally accessible in different environments. In the maritime environment for example, aspects of economic organisation may be visible in the form of fishermen and industries sited along the coast. However, this is only one aspect of economic activity for these people and maritime commanders require as much of an understanding of the economic social structures underpinning the visible patterns of fishing activity as their land-based counterparts. It is therefore essential that intelligence staff examine the people in the joint operational environment from the perspective of the people, rather than from the perspective of the military environment in which they are placed.

CHAPTER 5 – UNDERPINNING JOINT INTELLIGENCE: STRUCTURES, PROCESS AND PEOPLE

Chapter 5 describes how intelligence at the national level and in the joint operating environment is underpinned by structures, process and people. It explains: the single intelligence environment; the role and specific responsibilities of the joint commander and the intelligence staff; the joint operational intelligence architecture; the education and training of intelligence personnel; and information flow.

SECTION I – THE SINGLE INTELLIGENCE ENVIRONMENT

501. The single intelligence environment is as much an attitude of mind as it is about physical capabilities. It is defined as *the overall space, conditions and surroundings within which the military intelligence structure interfaces and operates with other national and international information and intelligence agencies to support decision-makers at all levels*.[1] Maintaining a dynamic single intelligence environment is critical to the conduct of intelligence operations in the contemporary operating environment. The keys to its success are: the education, training and attitude of our people; making the optimum use of our legacy Intelligence, Surveillance and Reconnaissance (ISR) and information systems; and maintaining our cross-governmental and multinational links.

502. **Method of Operating**. The single intelligence environment is a collaborative endeavour involving all the members of the UK intelligence community. It aims to harmonise all elements of the intelligence process to achieve the optimal use of intelligence specialists, agencies, sources and activities to produce the best possible products. This is achieved by combining skilled professionals with technology. The key tenets are:

a. **Fusion and Integration**. User requirements drive fusion and integration at all levels.

b. **Collaboration**. Work is completed in collaboration with national intelligence agencies and allies, to optimise the range of input.

c. **Environment**. The single intelligence environment is unrestricted by environments or geography and it embraces the maritime, land, air, space and cyber operating domains. It is unbounded by the historical

[1] New UK definition established in JDP 2-00 and awaiting formal approval by NATO.

distinctions between the strategic, operational and tactical levels of intelligence activity.

d. **Interconnectivity**. The single intelligence environment links networks to enable the effective operation of the diverse competencies within the intelligence community.

503. **The Concept of Fusion**. Fusion is defined as *the blending of intelligence and information from multiple sources or agencies into a coherent picture. The origin of the initial individual items should no longer be apparent*.[2] Fusion can occur at the point of need and be a very informal process. For example, commanders involved in a specific operation may need to fuse information together quickly to make a time-dependent decision without reference to agencies or formal organisations. This does not negate the importance of dedicated fusion centres, but does demand a more flexible and agile approach. A collaborative approach between actors provides the best possibility of achieving coherence.

504. **Intelligence Fusion Centres**. UK intelligence fusion centres include:

a. **Defence Intelligence Assessment Staff**. The Defence Intelligence Assessment Staff is the primary all-source assessment body within Defence and supports the other government departments through the Joint Intelligence Committee process.

b. **The Defence Geospatial Intelligence Fusion Centre**. The Defence Geospatial Intelligence Fusion Centre manages and produces geospatial intelligence and fused multi-intelligence in support of strategic and operational decision-makers.

c. **The Operational Intelligence Support Groups**. Operational Intelligence Support Groups are the focal point for the tasking of national agencies and fusion of national intelligence in support of the operational commander.

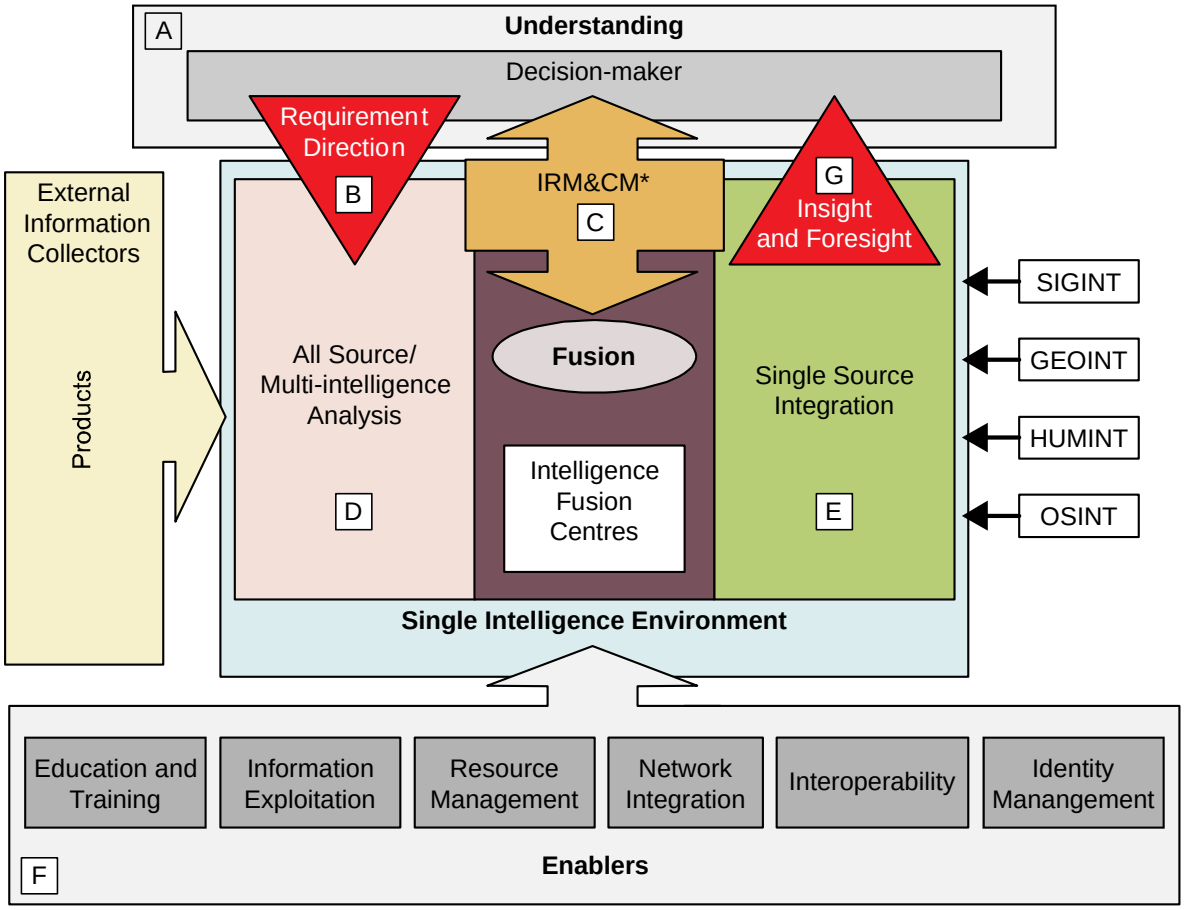
d. **The Maritime Intelligence Fusion Centre**. The Maritime Intelligence Fusion Centre is the focal point for fusing operational maritime intelligence across Defence.

e. **The Land Intelligence Fusion Centre**. The Land Intelligence Fusion Centre is responsible for the intelligence preparation of personnel and formed units for deployment.

[2] AAP-6.

f. **Air Intelligence Centre**. The Air Intelligence Centre is the intelligence hub for air and aviation intelligence and integrated mission support. It also acts as J2(Air) on behalf of PJHQ.

505. **The Single Intelligence Environment Model**. Figure 5.1 represents the single intelligence environment. Decision-makers (Box A) will clearly identify their requirements and provide direction to the intelligence specialists (Box B) who have access to the appropriate information and intelligence sources. Where possible, intelligence is fused within other national or operational intelligence at the point of need. Where further support is required, the fusion centres will search for the relevant information (Box C). They integrate multi-intelligence analysis (Box D), as well as single sources (Box E). A range of personnel and activities (Box F) will enable this process. The fusion centres will collate, analyse and disseminate the intelligence product back to the decision-maker and his staff. Based on the quality of the product, the decision-maker will gain an insight to why the problem has occurred, and he will then use his judgement to develop the foresight to take the appropriate action (Box G). The decision-maker will also take whatever risk he feels is necessary based on the intelligence product.



* Intelligence Requirements Management and Collection Management

Figure 5.1 – The Single Intelligence Environment Model

506. **The Single Intelligence Environment Functional Areas**. The functional areas of the single intelligence environment are:

a. **Analysis and Assessment**. Analysis is at the centre of the single intelligence environment because it provides the insight and foresight required by the decision-maker.

b. **Intelligence Management**. Management of intelligence within the single intelligence environment must ensure that the intelligence functions are responsive to the direction of decision-makers at all levels. A dynamic process, it helps to develop and prioritise information requirements and their subsequent tasking based upon a common system of governance. This common system of governance must be coherent with that of coalition partners and key UK institutions (National Security Council and UK intelligence agencies).

c. **Collaboration**. To realise the benefits of burden and information sharing within a coalition, it is important to develop a spirit of collaboration based on personal relationships, trust and mutual respect. The single intelligence environment embraces all stakeholders, irrespective of their location, organisational boundaries and security working levels.

d. **Integration of Collection Capabilities**. Rigorous standards enable the seamless sharing of raw data and analysed product to underpin further analysis, assessment and dissemination. The single intelligence environment must integrate with the full range of current and future collection capabilities provided by the UK, 5-Eyes community,[3] NATO, European Union (EU) and *ad hoc* partners to ensure persistent and the widest possible coverage.

e. **Interoperability**. The single intelligence environment should be interoperable, or at least compatible, with 5-Eyes, NATO, EU nations and other architectures and technologies. This is achieved by intelligence systems constantly developing and maintaining interfaces that allow seamlessly operations with allies and coalition partners.

f. **Information Integration and Sharing**. It is important to balance information sharing with security and information assurance measures. This requires confidence and respect for each other's products and information handling processes, including the management of *need-to-know* groups and agreed access permissions.

[3] The 5-Eyes Community consists of US, UK, Australia, Canada and New Zealand.

g. **Knowledge Management**. The information that drives the single intelligence environment is diverse in origin, format, protective marking and releasability. It supports both government and military requirements. Defence Intelligence should constantly aim to link the resources and information capabilities inside and outside government and other partners to enable the effective search, retrieval and visualisation of networked information and intelligence. Such a networked approach requires people with the systems, tools, skills, individual and collective behaviours, who can manage, make sense of, process and exploit rising volumes of information and intelligence. Intelligence staff must fully exploit experts and knowledge repositories.

h. **Agility**. The single intelligence environment requires the capacity to adapt and develop appropriate combinations of people, structures, processes and technologies to react to changes in intelligence requirements. Commanders can achieve this by appropriate training of their staff in current systems and processes.

507. **Populating the Single Intelligence Environment**. Figure 5.2 shows the single intelligence environment as envisaged at full operating capability.

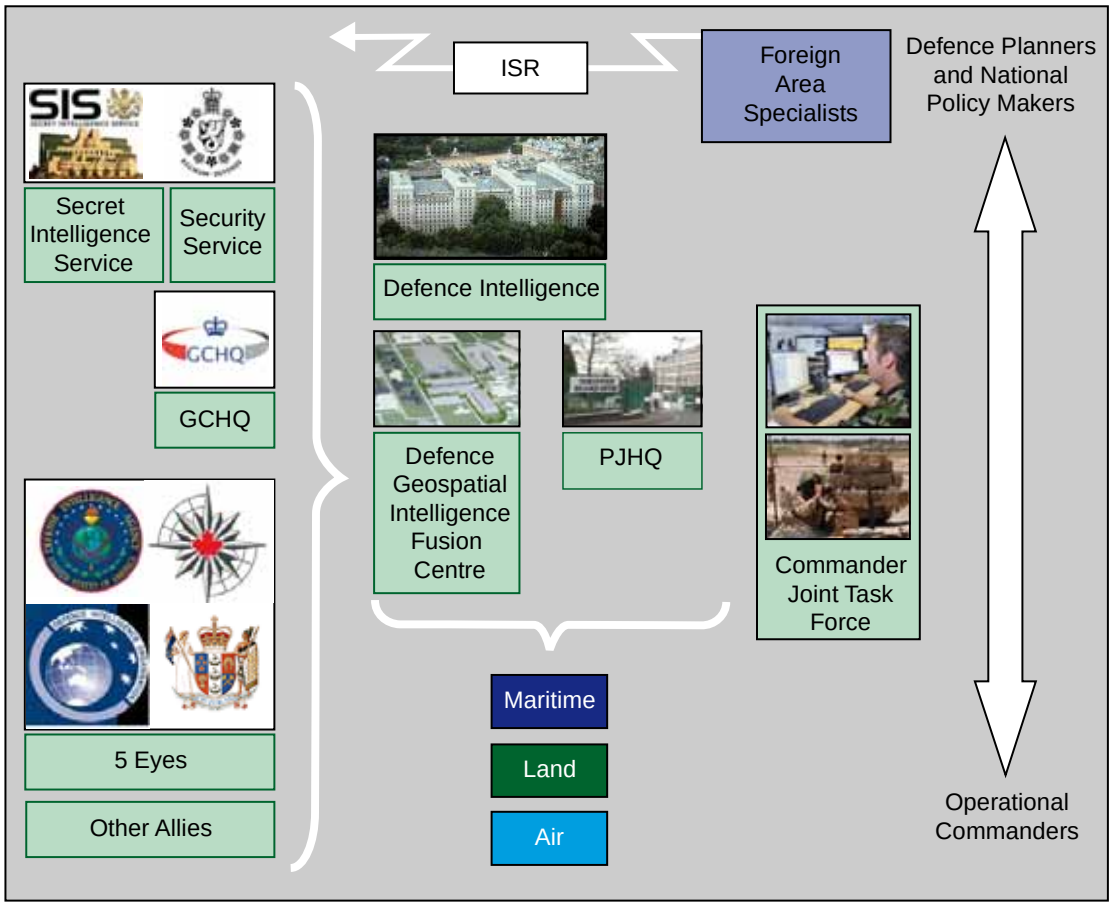


Figure 5.2 – The UK Single Intelligence Environment

SECTION II – THE COMMANDER, INTELLIGENCE AND DECISION-MAKING

'*Creating effective intelligence is an inherent and essential responsibility of command*.' [4]

Major General M T Flynn

508. The relationship between the commander and his staff at all levels is critically important for effective decision-making. The commander provides the leadership, judgement and energy to focus the staff and the forces under his command towards the goal of achieving the mission.

509. **Commander's Intelligence Responsibilities**. Commanders are more than just demanders and consumers of intelligence. They are the key players in the planning and conduct of intelligence operations. Commanders organise and assign their own staff, configuring them to meet the information, intelligence and operational requirements they set. It is the commander's responsibility to provide direction and guidance, to define priorities, to resource intelligence collection and analysis effectively, to demand the highest standard of products and to review the effects of his chosen actions. Critical factors in the conduct of joint operations are: the direction given to the joint force commander; the relationship that the commander has with his staff and with his superior headquarters; the degree of political support for the operation that a commander can influence; and the nature of the environment.

Commanders' Intelligence Responsibilities	
Develop a thorough knowledge of understanding and intelligence doctrine, intelligence capabilities and their limitations	
Provide clear direction and planning guidance	
Clearly define the areas of interest	
Identify and clearly articulate critical intelligence requirements	
Integrate intelligence into all aspects of plans and operations	
Create the right command climate:	
Proactively engage intelligence staff Create an atmosphere that allows open-mindedness, critical analysis and creative thinking	Develop trust with, and amongst, the staff Demand high quality, predictive intelligence

[4] Taken from *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, January 2010.

510. **The Commander and Decision-Making**. Effective decision-making is an art that is part nature and part nurture. A good commander knows that:

a. There is both a correlation and a relationship between quality and timeliness, and that some risk are inevitable.

b. Commanders must not delegate decisions unless there are exceptional circumstances.

c. Good decisions come with training.

d. The outcome of decision-making is more important than the process of decision-making.

e. The staffs assist the commander to make decisions and there must be mutual trust and confidence in one another.

511. **Commanders' Vision and Intent**. Vision is the ability to create a mental image of the future using imagination and wisdom. It is the articulation of foresight, the primary outcome of understanding. It provides the context for the development of understanding at all levels, and for determining the level of intelligence support required. At strategic and operational level, vision determines campaign design, how we prosecute the campaign, how we allocate resources and the operational priorities. At the tactical level, vision helps explain the context and purpose of an operation.

512. **Promoting Access to Intelligence**. A challenge for the commander is to focus the intelligence effort and to achieve timely dissemination. This includes ensuring the exchange of intelligence among all echelons and components. Unity of effort is essential to ensure comprehensive, accurate and current intelligence while reducing unnecessary redundancy and duplication. It implies all individuals, groups and agencies working together collaboratively to achieve a common objective. Therefore, access to intelligence capabilities to support mission requirements should not be restricted by organisations or command configurations, but prioritised by need. If higher priority or competing tasks affect optimisation of intelligence activities, the commander should make alternative provision from within his assigned resources, request assistance from national agencies through his chain of command or assess the effects of gaps in intelligence to the operation.

513. **Prioritising Capabilities**. Intelligence capability requirements are situation-dependent and should be flexible enough to support non-lethal and lethal activities. Seldom will it be possible to have exactly what is required and there will always be an element of risk management.

514. **The Command Climate**. Commanders should create an atmosphere that allows open-mindedness, critical analysis and creative thinking. Trust is a 2-way process and the command climate should enable key staff to tell the commander what he needs to know, even if it contradicts to his own view.

515. **Command-Intelligence Failures**. The relationship and trust developed between a commander and his staff is a critical component of operational success. There are numerous examples throughout history where the breakdown of this relationship has led to operational failure. Failure in this context is generally attributed to either a failure of intelligence or a failure of command. The reality is that it is often a combination of both. Examples of factors that lead to command-intelligence failures are:

a. **Failure to Warn**. The failure to provide early warning is a predominant theme at both the operational and strategic levels. Examples include Korea in 1950 and the Falkland Islands in 1982. This does not necessarily mean that the intelligence staff had not identified the threat.

b. **Poor Analytical Capability**. Insufficient or weak analytical capability can lead to failure. In the Korean War, the US failed to assess firstly, Chinese intent, despite several public pronouncements, and secondly, the capability of the Chinese Army compared with that of North Korea. The US made the error of comparing the North Korean Army with the Chinese Army. In fact, it was a very different adversary with different characteristics, strengths and weaknesses. Analytical weakness may reflect a lack of intellectual competencies or particular group dynamics. Analysis also fails when it does not notice the trends by focussing instead on the day-to-day increments in isolation.

c. **Intelligence Gaps**. Intelligence will rarely provide all the answers the commander would wish. He must use his judgement and be prepared to take risk.

Guarding against the potential for failure places an emphasis on the commander to ensure that: the intelligence organisation is right for the theatre or operation; there is both long and short-term understanding of the adversary; he understands intelligence gaps; the people have the right training and skill sets; and the right supervision and management practices are in place. Annex 5A is a case study that provides examples of both failure of command and failure of intelligence.

516. **Operational Risk**. When reviewing intelligence as part of an overall risk assessment process, commanders must consider the totality of the risk

and resist the temptation to focus solely on one aspect. For military operations, risk can be in 2 forms: operational and operating. Operational risk refers to how the adversary can affect your operations while operating risk is that risk you expose yourself to by choosing to conduct your operations in a certain way. For example, an adversary with a functioning Integrated Air Defence System might drive the decision to operate aircraft only at night or at low-level in order to minimise the risk of detection, thereby reducing operational risk. However, this tactic may carry increased operating risk, particularly if aircrews are not trained in this discipline. Thus, a judgement between operational and operating risk considerations will be required. All commanders in the risk management chain require a common understanding of the intelligence picture before making informed judgements on risk. Therefore, commanders will need to understand the risk management process and maintain continuous dialogue from the strategic to the tactical level.[5]

SECTION III – THE JOINT HEADQUARTERS AND THE INTELLIGENCE STAFF

517. **The Generic Functions of a Joint Headquarters**. The primary functions of a headquarters are to exercise control over assigned forces and to enable the commander to make effective decisions on their operational employment. The intelligence staffs are an essential part of the headquarters and are involved in all of its key functions. It is vitally important that all of the staff branches share information and work together to avoid stove piping. The generic functions of any operational headquarters are:

[5] More details on risk analysis and risk management are contained in JDP 5-00 (2nd Edition) *Campaign Planning*.

Generic Functions of a Headquarters	
Support to decision-making	The primary role of a headquarters is to support the commander's decision-making.
Organisation	Responsibility for the organisational structure and functional operation of the headquarters and assigned forces. Provide the commander with the information and facilities required to exercise command.
Planning and Control	Control is the process through which the commander, assisted by his staff, integrates subordinate forces with the factors and conditions for the area of operations: • Command resides with the commander. Control is inherent within command and, except for those critical aspects that commanders perform themselves, normally resides with the staff and occurs through command support. • Control is the duty of the staff and includes collecting, processing and disseminating information for creating the common operating picture and using information during planning, reviewing, executing, and evaluating operations. • To achieve control, the staff must ensure commonality of approach to training, planning procedures and understanding at all levels. • The staff must translate the commander's plans and decisions into orders and actions.
Management and Communication	The management of information assurance, information management and information exploitation. Specifically: • Disseminate information and provide assistance in order that subordinate formations and units can carry out their mission tasks. • Keep subordinate and flanking units, formations and allies informed of activities and intentions.
Management of Resources	Manage resources ensuring that there is always sufficient to fulfil the mission and highlighting risk.

518. **The Headquarters Staff**. The purpose of the headquarters staff is:

a. To support the commander to make timely decisions.

b. To translate the commander's plan into action through careful control and co-ordination.

c. To facilitate the conditions for him to command effectively, for example by making sure he can communicate with whom he needs to, when he needs to.

d. To identify the art of the possible and any associated risks.

The Intelligence Officer

'The successful Intelligence Officer must be cool, courageous and adroit, patient and imperturbable, discreet and trustworthy. He must understand the handling of troops, and have knowledge of the art of war. He must be able to win the confidence of his General, and to inspire confidence in his subordinates and of the officers holding responsible commands in the force.'

Extracted from: Lieutenant Colonel David Henderson DSO, Argyll and Sutherland Highlanders: *Field Intelligence, Its Principles and Practice*, HMSO 1904. Later, Lieutenant General Sir David Henderson KCB, KCVO, DSO, LLD (Late Royal Flying Corps)

519. **The Intelligence Staff**. One of the critical paths to achieving operational success is the organisation of the headquarters to make the optimum use of information and intelligence. This requires intelligence staffs that are responsive enough to react to new problems and have the professional skills required for their role. Often the intelligence staffs consist of a combination of specialist, trained as collectors, analysts and other intelligence skills, and generalists seconded from other branches to intelligence. There is a tendency to confine the intelligence staff within stove-piped structures either of their own making or through the ignorance of the other staff branches. The contemporary operating environment requires permeable boundaries between functional areas to obtain greater co-ordination. The following measures are examples of how this may be achieved:

a. The integration of other members of the headquarters staff into some intelligence functions to broaden their expertise.

b. Using intelligence staff in the broader staff environment and employ them in more areas. Figure 5.3 provides an example of this during operations.

c. Involving commanders in intelligence training to increase knowledge and to manage expectation.

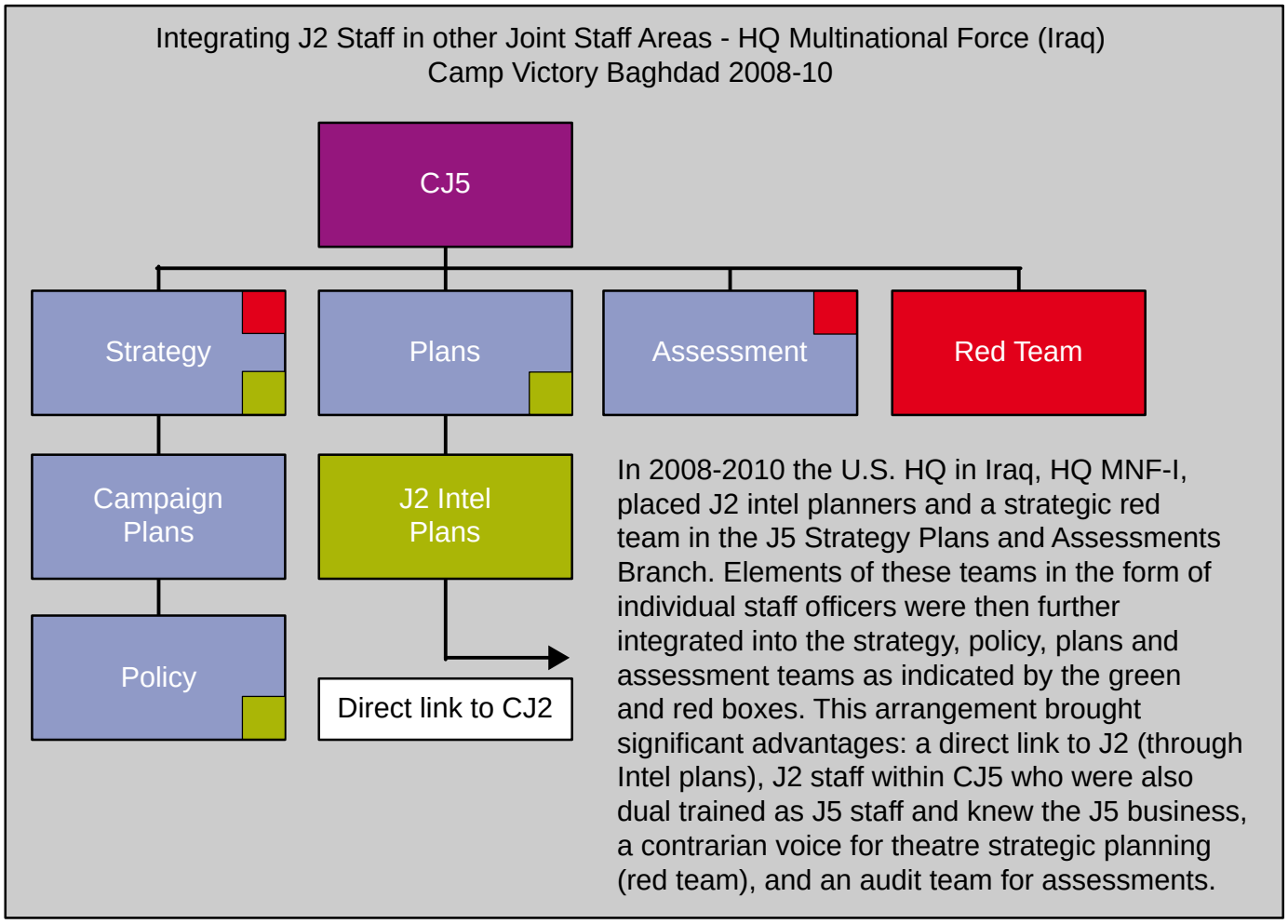


Figure 5.3 – Integrating Intelligence Staff into other Staff Areas

520. **Intelligence Staff Support to the Commander**. The intelligence staff must continually refine the intelligence operation to reflect changes in the commander's mission, the situation and objectives. Intelligence operations must be synchronised with other operational activity to ensure integrated and responsive support throughout all phases of the operation. The responsibilities of the intelligence staff are:

Intelligence Staff Responsibilities
• Maintain a thorough knowledge of understanding and intelligence doctrine, intelligence capabilities and their limitations. • Develop detailed intelligence plans and advice based on a sound intelligence estimate, intelligence collection plan and support to campaign and other operational planning. • Participate in all joint-interagency and military planning conducted by the combined joint task force headquarters. • Ensure that all intelligence is set within the wider framework of understanding and that it meets the commander's requirements. • Integrate national, theatre, operational and Allied/coalition intelligence support. • Build and maintain a dynamic, agile and adaptable operational intelligence architecture based on the principles of collaboration and fusion. • Synchronise intelligence planning with operational planning for all operations. • Develop and maintain an intelligence concept of operations that supports commanders at all levels. • Ensure intelligence unity of effort and continuity to the lowest levels. • Organise for continuous operations. • Ensure accessibility of intelligence. • Continuously review all intelligence.

SECTION IV – JOINT OPERATIONAL INTELLIGENCE ARCHITECTURE

521. The intelligence architecture enables the flow of information and incorporates command and control, information management and communications information systems. It links intelligence processing and dissemination, the military intelligence systems and national intelligence capabilities. The intelligence architecture for deployed operations is based, as far as possible, on peacetime operational structures and arrangements. It is a mix of both human parts of the network and the technical means of enabling the human network to interface and operate effectively. The architecture must not only focus on the intelligence process, but must also engender trust, particularly in a multinational environment. It should provide clear lines of

direction and promote an effective prioritisation system that is linked to the command chain.

522. For each operation PJHQ will produce the *Intelligence and Security Management Plan* that defines for a joint task force commander:

a. The intelligence support to be provided.

b. The ISR assets assigned in support.

c. The planned intelligence architecture.

d. The management of the security aspects of the operation.

This plan may be adjusted to meet the specific needs of the campaign or operations. For example, specific niche support may be required from national intelligence agencies.[6]

523. To achieve operational success, the quality of the joint force commander's decision-making and execution of operations must be consistently better and faster than that of his adversaries. Therefore, intelligence must not only be faster, but also better than the other actors can access through their own networks. To ensure that this occurs there are some basic precepts:

Precepts for Successful Joint Operational Intelligence Architecture
The commander must drive the intelligence effort
The intelligence staff must be organised and structured for agility
The requirements of the joint task force must be supported
The allocation of collection assets must be based on validated information requirements
Robust communications information systems infrastructure must enable the optimum exchange of intelligence within a multinational construct

[6] For example other governmental departments may create a liaison cell within the intelligence branch to ensure unity of purpose.

524. **Functional Relationships**. The effectiveness of the architecture is based upon the relationships between:

a. Commanders and the staff who conduct the ISR process.

b. Formations and units that own the collection assets, processing and dissemination, and particularly analytical capabilities.

c. The availability of non-assigned collection assets.

d. Communications and information systems that enable the process.

525. **Command, Control, Communications**. Achieving better and quicker information and intelligence than the other actors requires effective command and control over the collection, processing and dissemination of information. Command and control relationships need to be clear, especially about collection management responsibilities. Intelligence staff should be able to communicate with collection assets and intelligence users. Commanders should be aware that given the automation of intelligence systems and the need for reach-back to the UK effective communication information systems within the intelligence branch are critical to success.

526. **Agility**. Intelligence architectures must be physically and intellectually capable of responding to, and ideally pre-empting, an evolving situation. Before deployment, Commanders should test the agility of their headquarters and the intelligence staff.

527. **Multinational and Agency Integration**. The intelligence architecture should be integrated, within security constraints, with multinational headquarters, other nations and national agencies. Multinational operations may not have a conventional hierarchical structure, but may operate as a series of linked commands and responsibilities. Intelligence nodes may be established, for example, linking nations through formal intelligence sharing agreements, or groups of partners with common interests.

528. **Intelligence Resources and Architecture**. MOD intelligence resources are only one part of a bigger equation. National intelligence is a multi-source activity and all resources should be used, where applicable, to meet the national intelligence requirement. Articulating the requirement and obtaining the resources are necessary parts of developing capability. When working in a coalition, the UK should share assets and intelligence.

529. **Continuity**. A key to the success of any intelligence endeavour is not only continuity at the national level but, more specifically, in theatre. Once a

force deploys overseas, it is vitally important to establish a long-term view and provision a properly constituted national contingent headquarters in the operational theatre that has an intelligence support element designed to achieve intelligence continuity.[7] The staff for this headquarters must be carefully selected and expect to deploy in a pattern that ensures continuity.

SECTION V – THE DEPLOYED INTELLIGENCE (J2) ARCHITECTURE

530. **Chief J2**. Chief J2 is the commander's principal intelligence adviser. The relationship between a commander and his Chief J2 is critical to the operation of a headquarters. This requires the development of considerable trust between the individuals concerned. Chief J2's responsibilities include:

a. Acting as a focal point for all information and intelligence passed to or from the commander.[8] The information manager normally undertakes this role.

b. Ensuring the working relationships between intelligence staffs and other staff branches remain effective. Poor relationships may hamper communication and information flows and depreciate the value of the intelligence staffs.

c. Maintenance of effective and productive relationships with national intelligence agencies. It must be a relationship built on interpersonal skills rather than process. To achieve this, Chief J2 will:

(1) Engage with the agencies before deployment and recognise and acknowledge the agencies' own responsibilities to develop a direct relationship with the commander.

(2) Aim to draw the agencies into the military briefing process to enhance mutual understanding.

531. **J2 Plans, Operations and Targets Staffs**. J2 plans staffs are primary operational planning interface with the other parts of the headquarters. J2 operations use all-source intelligence to inform *joint action*, bringing together campaign understanding and network analysis.[9] Within the contemporary operating environment, sensitive intelligence collected by national intelligence and security agencies provide the commander with unique opportunities to

[7] One example may be the theatre level Operational Intelligence Support Group that have deployed to Iraq and Afghanistan.
[8] This is likely to include at a minimum the Commander's Critical Information Requirements, the Joint Intelligence Estimate and the Intelligence Collection Plan.
[9] JDP 5-00 (2nd Edition) *Campaign Planning* refers.

employ a wide range of effects against opponents and to influence key actors within the joint operations area. These effects range from targeting of opponent networks to the co-ordination of hard and soft power to achieve influence over and between actors. Targeting requires collaboration between intelligence specialists, operations staff and planners. This is normally undertaken through a targeting co-ordination group which is described in more detail in paragraph 539.

532. **J2 Cells**. The intelligence staffs are normally divided into a number of specialist cells who are responsible for: responding to intelligence requirements and requests for information; the processing and dissemination of intelligence; and producing intelligence reports. These may include:

a. **All-Source Analysis Cell**. An all-source analysis cell comprises a task-orientated production section for processing information and providing all-source intelligence products. The all-source analysis cell co-ordinates closely with J2 Plans to ensure that intelligence products meet the commander's needs and that intelligence requirements and requests for information raised during processing are addressed accordingly.

b. **Materiel and Personnel Exploitation Cell**. Increasing intelligence complexity and cross-government engagement during operations, predicates the need for coherent exploitation arrangements. A materiel and personnel exploitation cell may be established to provide intelligence through the exploitation of people, documents, electronic media, biometrics and technical equipment.

c. **Geospatial Intelligence Support Element**. A geospatial intelligence support element can provide intelligence derived from the analysis and exploitation of geospatial information and imagery to describe, assess and visually depict physical features and geographically referenced activity. Its output will usually be referenced by geospatial position and arranged in a coherent structure. A geospatial intelligence support element can draw on imagery from specialist geospatial centres.[10]

d. **Counter-Intelligence Cell**. Joint task force commanders increasingly require counter-intelligence activities to address multi-dimensional and asymmetric threats. The creation of a counter-intelligence cell aids the co-ordination of these activities. It will also

[10] UK specialist geospatial centres include the Joint Air Reconnaissance Intelligence Centre, Hydrographic Office, Meteorological Office, Defence Geographic Centre and Joint Aeronautical and Geospatial Organisation.

oversee the activities, briefings and debriefings conducted by counter-intelligence staff. The counter-intelligence staff will work closely with the J2X staff to de-conflict operations and sources.

e. **Open Source Intelligence Cell**. Some multinational headquarters may contain an open source intelligence cell. However, in UK national headquarters, this analytical capability is integrated into the all-source analysis cell, as the same analytical competences and management processes are required to assess both open source and classified intelligence. The management and fusing of open and classified material feeds back into the effective management of collection systems, ensuring that the collection of classified and open material complement each other rather than compete.

f. **J2X Cell**. The direction, co-ordination and supervision of deployed military Human Intelligence (HUMINT) elements are the responsibility of the J2X Cell as part of collection management. J2X staff will maintain the register of sources and de-conflict both HUMINT and counter-intelligence activity. In addition, they will provide advice to commanders on HUMINT and the Regulation of Investigatory powers Act 2000.

533. **Subject Matter Experts**. Intelligence staff should establish relationships with any subject matter experts attached to a headquarters, (for example regional experts and academics). Commanders may be provided with support from the academic community to assist the J2 branch in the development of understanding. This community may be organised into an academic support cell within the headquarters or form a virtual network.

SECTION VI – THE INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE CELL

534. The Intelligence Requirements Management and Collection Management (IRM&CM) staff will produce an intelligence collection plan (Chapter 3 refers). However, they do not have the authority to issue and execute orders in the operating environment. That responsibility falls to the ISR cell staff. They will produce the collection and exploitation plan (known as the CXP) and allocate ISR tasks to assigned or subordinate ISR assets. The collection and exploitation plan is the result of a collaborative effort between the IRM&CM staff and the ISR cell staff. It comprises the intelligence collection plan, ISR synchronisation matrix, and ISR overlay, and is used to direct the employment of assigned ISR assets. Importantly, it articulates in time and space the appropriate resource groups to collection requirements and from this ISR tasks will be generated.

535. The ISR Cell's roles are:

a. Co-ordinates and synchronises the intelligence staffs' collection requirements with those of the operations and plans staff.

b. Translate collection requirements, drawn from the intelligence collection plan into specific collection tasks.

c. Task collection assets and monitor execution.

d. Advise commanders on collection capabilities.

SECTION VII – OPERATIONAL INTELLIGENCE SUPPORT GROUPS

536. An operational intelligence support group provides a mission-tailored national intelligence capability able to support joint, combined and single-service operations. Specifically, it provides the commander with access to national intelligence capabilities to enable tactical exploitation of their products. It is the single route for collection by UK strategic intelligence organisations and has an all-source analytical capability. It should be integrated into the intelligence staff structure to ensure sharing of products. An operational intelligence support group goes beyond simply being part of the intelligence structure; it is a think-tank for the commander, exploring ideas and concepts. Although working alongside the intelligence staffs, the operational intelligence support group is compartmentalised and operates at the highest level of protective marking.

537. **Operational Intelligence Support Group Capability**. An operational intelligence support group provides additional depth and capability to support multi-source intelligence and appropriately sanitised products.[11] It is able to:

a. Operate with the all-source analysis cell.

b. Conduct target development and intelligence exploitation.

c. Process information and produce fused intelligence product.

d. Provide releasable intelligence to allies.

e. Support the intelligence requirement management process.

f. Conducts liaison with intelligence agencies from other nations.

[11] Sensitive content and details that could cause compromise are removed, such as the origin or source of the intelligence.

g. Provide UK-eyes only or compartmented area for intelligence activity.

538. **Operational Intelligence Support Group Structure**. Each operational intelligence support group is structured to meet specific theatre and operational needs, but most are likely to contain:

a. **Specialist Intelligence Elements**. National intelligence organisations are represented by specialist intelligence elements, which facilitate direct reach-back to parent organisations and complement the assigned J2 architecture. These elements normally include experts on HUMINT, Signals Intelligence (SIGINT) and Geospatial Intelligence (GEOINT), although not all will be present in each operational intelligence support group.

b. **Analytical Elements**. The analytical element will carry out analysis of national level intelligence in a theatre context. It links the specialist intelligence elements to the J2 staff and maintains a bespoke intelligence database. A Defence Intelligence analyst is often included in the analytical element.

539. **Targeting Co-ordination Group**. The joint task force commander must establish a mechanism to examine targeting opportunities, which brings together intelligence specialists (military, national and international) with operations and planning staffs. This mechanism should include liaison staff from national intelligence agencies embedded within a headquarters, as they are integral to the intelligence development of those targets. Given the sensitive nature of covert intelligence sources and associated products, the best mechanism could be a commander-led targeting co-ordination group. It should operate as a discrete aspect of the operational intelligence support group, with whom there must be very close co-ordination. This co-ordination needs to support the development of actionable intelligence, manage risk to sources and ensure de-confliction between source operations.

The Targeting Co-ordination Group in Northern Ireland

The intelligence structure established in Northern Ireland in 1969 had changed little since 1916. Indeed the mistakes of 1916 were replicated in 1969 with a failure to: link military and civilian intelligence agencies; and to understand and agree the roles of the agencies, the Royal Ulster Constabulary and the Army. Initially, the Royal Ulster Constabulary and the Army operated a number of intelligence-gathering units with similar, but discrete, functions, as did the national intelligence and security agencies. There was little co-ordination between the units, resulting in missed opportunities, duplication of effort and even an *own goal*. Consequently, in 1979 Sir Maurice Oldfield reviewed intelligence and design a single co-ordination point for all covert units and the wider security forces that were able to react in a timely way and ensure the most appropriate intelligence capability was applied to resulting exploitation. The targeting co-ordination group was the result.

SECTION VIII – EDUCATION AND TRAINING

540. The educating and training of intelligence staff is an essential enabler of effective joint intelligence. It includes not only training for individuals, units and headquarters staff, but also training for both generalists and specialists. It must be dynamic and adaptable enough to be able to react to changes in Defence and operational thinking, particularly in respect of new threats, opportunities and priorities.

541. **Intelligence Education and Training Progression**. There are 3 basic levels of intelligence education and training:

a. **Intelligence Awareness**. Intelligence awareness is based on individuals being able to recognise the importance of intelligence and knowing how they should report the information that they collect during their routine duties. All personnel should be made progressively intelligence aware through their careers, but particularly during pre-deployment training before entering an operational theatre. During pre-deployment training individuals should understand the intelligence structures, standing intelligence requirements and the need to obtain regular intelligence updates.

b. **Intelligence Practitioner**. Intelligence practitioners gain experience through progressive education and training, supported by specific pre-employment training and often followed by practical experience within an intelligence appointment. This can lead to a high degree of proficiency, which can be developed to achieve expert status. Non-specialist personnel assigned to intelligence positions or

conducting intelligence duties as part of their secondary duties need to develop into intelligence practitioners.

c. **Intelligence Experts**. Intelligence expert are personnel who undertake advanced specialist intelligence training followed by an extended period employed on intelligence duties. Expertise is only achieved by individuals that complete specialist training: very often these will come from an intelligence career field. It also implies that these specialists will spend a considerable amount of time in their specialist areas thus providing continuity.

542. **Cultural Training**. Cultural awareness is defined as *an awareness of the current and historic values, norms and beliefs reflected in different social structures and systems and in particular, how they contribute to an actor's motives, intents and behaviours*.[12] Cultural training is designed to provide different standards of cultural awareness in support of everyday Defence activity and operations. It requires the development of cultural expertise in areas where we are likely to operate, together with a more general awareness of other cultures. Cultural training provides 3 levels of cultural ability:

a. **Cultural Awareness**. Cultural awareness provides a basic knowledge of cultural issues, an understanding of their importance and impact, and the ability to apply this knowledge to predictable scenarios to create desired effect.

b. **Cultural Competence**. Cultural competence provide the intermediate knowledge of cultural issues, the comprehension of their importance and impact, the ability to apply this knowledge, skill and attitude to unpredictable scenarios and contribute to analysis of the effect. It is achieved by a daily requirement to interact with another culture either directly (where basic language skills have been achieved) or, more likely, through an interpreter, requires confidence, interest and a willingness to succeed. This approach can deliver a high degree of cultural competence, which can develop into expertise.

c. **Cultural Expertise**. Cultural expertise is an advanced knowledge of cultural issues. This includes: comprehension of the importance and impact; the ability to apply this knowledge; the skill to deal with unpredictable scenarios; and the ability to analyse and evaluate the effect to synthesise this evaluation to create new improved effect. It requires immersion into a culture and generally develops in concert with the ability to think with the same mindset. Developing expertise is a

[12] Joint Doctrine Note (JDN) 1/09 *The Significance of Culture to the Military*.

long-term process, requiring investment to provide opportunities for immersion and proximity to the culture. Selection of individuals for such opportunities should focus on their aptitude to develop such expertise; the necessary attributes may not necessarily be those required in other aspects of military life. However, commanders must recognise the value of cultural expertise and that true cultural experts can be campaign-winners.

543. **Specialist Advice**. Commanders may receive cultural advice from foreign area specialists, both military and civilian. These include: Defence cultural specialist; academics; experts from other departments (for example the Foreign and Commonwealth Office and Department for International Development); military intelligence liaison officers; and Defence attachés.

544. **Contextual Training**.[13] Contextual or applied training is provided to prepare a unit or a headquarters' staff for a particular deployment. Such training provides an understanding of a particular operation, the local structures and current processes. It should explain how intelligence is provided to customers during that operation. It may also incorporate mission rehearsal exercises or study days. Effective contextual training requires the trainers to understand the evolving operational environments and keep pace with the operational context.

545. **Collective Training**. Collective training includes the process of integrating intelligence staffs with other intelligence agencies and command staffs to ensure that individual skills can be applied within a headquarters or wider force enterprise. Collective training should test the skills of the intelligence staffs and not just be used as an enabler for testing command or other staffs.[14]

546. **Immersive Training**. Immersive training aids the development of understanding by allowing commanders and their staffs to immerse in current theatre intelligence prior to deployment. The intelligence product to support immersion will be tailored to the appropriate level. Immersion products could include *get-you-in-packs* for intelligence staffs or a rolling series of briefings, education and bespoke assessments for operational staffs.

547. **Language Training**. It is likely that the intelligence function will need to draw on capability outside its own resources to meet linguist demands. This capability can be obtained from contractors and locally employed civilians.

[13] Also known as pre-deployment training.
[14] Historically, intelligence has only been used to *drive* exercises, as injects etc. It must be noted that intelligence staffs should be tested, as should the mechanisms for integrating with wider headquarters element.

However, due to security considerations some intelligence function will require military linguists. They require a high level of competence that must be developed and maintained. This requires deliberate capability planning within the intelligence community. The cost of training may be high and careful judgement is required about the volume and variety of standing capability.

Jomini on Intelligence

Antoine-Henri Jomini

1. A general should neglect no means of information

2. By multiplying the means of obtaining information; for no matter how imperfect and contradictory they may be, the truth may often be sifted from them.

3. Perfect reliance should be placed on none of these means.

4. As it is impossible to obtain exact information by the methods mentioned, a general should never move without arranging several courses of action for himself, based upon probable hypotheses ... and never losing sight of the principles of the art.

SECTION IX – INFORMATION FLOW ON JOINT OPERATIONS

548. Conceptually the flow of information has 3 component parts. First, the commander directs what information he needs collected. Second, the commander and his staff use the information to gain a degree of understanding and situational awareness of the Joint Operations Area (JOA). 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. The 3 component parts have not changed since Napoleonic times when a dispatch rider galloped between units and commanders carrying hand written notes that were read by the commander and then returned back with the commander's orders.

549. **The Character of Information Flow**. Advances in technology have not changed the nature of the components of information flow, but it has changed their character. Information can now be transferred almost instantaneously, over greater range, in greater volume and in variety of formats. In the contemporary operating environment, the horse is transformed into broadband satellite, microwave links and digital radios, while the handwritten note is replaced by satellite communications and teleconferencing. However, the

fundamental requirement to provide information to a commander to enable a decision and then disseminate that decision has not changed.

550. **Information Management**. Information management is the supervision, administration, regulation and timely dissemination of information. All personnel within the management process must understand the context of the information that they are handling in order to manage it effectively. Simply processing it is insufficient. While software applications allow the staff to receive, store, manipulate and disseminate information, it is human interaction that provides the ability to identify opportunities to exploit it. Information management must not be regarded as a separate process in its own right, but part of an overall approach that includes exploitation and assurance, providing the highest possible quality of information efficiently and on time.

551. **Effect of Technology**. Modern technology has revolutionised the information flow in the JOA. This provides the commander with significant new capabilities that can deliver operational advantage. The challenge is that although technology enhances the range, speed and volume of the bearers, provides new formats for information and the ability to manipulate information, it does not necessarily enhance either understanding or the ability to exploit the information. 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.

552. **Combined Joint Task Force Information Flow**. The information flow within a combined joint task force is illustrated in Figure 5.4. The intelligence architecture and the communications required to support it must be capable of linking into all parts of the joint force, as well as the wider external network.

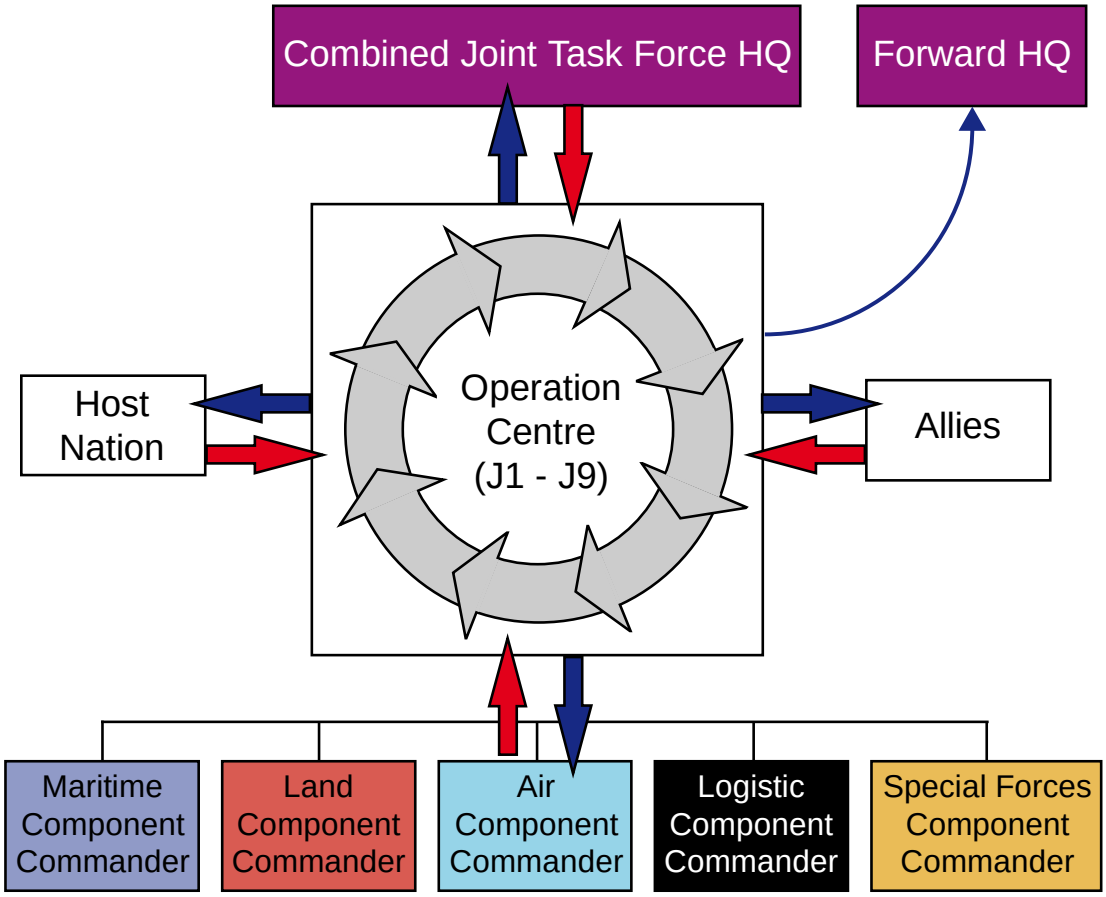


Figure 5.4 – Combined Joint Task Force Communication and Information Systems Architecture: Information Flow

SECTION X – JOINT INTELLIGENCE OPERATING GUIDELINES

553. A number of factors affect intelligence in the contemporary operating environment:

a. Commanders and staff must avoid becoming overly-focused on adversaries and the physical terrain. A more comprehensive view of the dynamics of situations is required. Commanders need to conduct their joint intelligence estimates through physical, cognitive and virtual environments and they should consider all actors within the wider operational environment.

b. The levels of warfare should not be used to constrain the operation of intelligence. The boundaries between strategic, operational and tactical intelligence are increasingly blurred.

c. Adversaries are as likely to be low-contrast or low-resolution as they are to be clearly defined and categorised. Intelligence gathering

requires precision and accuracy to generate the required contrast and resolution.

d. The balance between security and a *duty to share* is moving in favour of the latter becoming the default, with each denial of information requiring justification.

e. The links between the commander and his intelligence staff must be strong and immediate. A commander cannot afford merely to set requirements and then leave the intelligence staff to feed them independently. He personally must drive the meeting of those requirements.

f. Information should be passed horizontally as well as vertically within a staff. Too often, a vertical command structure means that not all staff has the necessary situational awareness. Staff should be encourage to *pull* the intelligence they require for network systems rather than expecting the intelligence staff to routinely *push* the intelligence to them.

g. Target development (achieving greater understanding in order to yield opportunities) is as important as targeting (identifying and prosecuting targets).

(INTENTIONALLY BLANK)

ANNEX 5A – CASE STUDY: COMMAND AND INTELLIGENCE FAILURES

FAILURE OF COMMAND – 1942, CONVOY PQ17

A4. In June 1942, Admiral Sir Dudley Pound (First Sea Lord of the Admiralty), fearing an attack by the German battleship Tirpitz, ordered the Royal Navy cruisers and destroyers escorting the Murmansk bound Convoy PQ17 to abandon the convoy while it was off the North Cape of Norway. The convoy was ordered to scatter and each ship was to make its way to Murmansk alone. Admiral Pound ordered the convoy to disperse despite Commander Denning's (the Admiralty's Operational Intelligence Centre German surface ship section chief) assessment that the Tirpitz had not sailed from her Norwegian port. Denning's assessment, which proved to be correct, was based on communications intelligence intercepts. Nevertheless, the convoy dispersed on Pound's orders and became vulnerable to German air and submarine attacks. Twenty-three of the 34 merchant ships in the convoy were sunk in one of the worse disasters to befall any Allied convoy during World War II.

Admiral Sir Dudley Pound

5A1. Patrick Beesly, who served in the Operational Intelligence Centre during World War II, offered the following analysis of the fatal decision to scatter the convoy. 'Quite apart from age and health (Pound was 65 and would die from a brain tumour the next year), and despite his great experience as a staff officer, Pound did not, in my opinion, understand the intelligence scene. Although the Operational Intelligence Centre was only a few minutes walk from his own office, he very rarely visited it. He appreciated neither the strengths nor weaknesses of intelligence: he required 'Yes' or 'No' answers to his question ('Can you assure me that Tirpitz is still in Altenfjord?') something that the very best intelligence officers can seldom provide. In all intelligence problems, there must always be some element of uncertainty, always a last piece of the jigsaw puzzle that can only be filled in by guesswork. It may be inspired intuition, but it should always be based on thorough background knowledge of the enemy and his way of thinking. After 3-years of war, it ought to have been obvious that Denning, one of the most brilliant intelligence officers of either world war, had this gift, but Pound could not bring himself to rely on so junior an officer's opinion. Events proved Denning right and Pound wrong. Senior

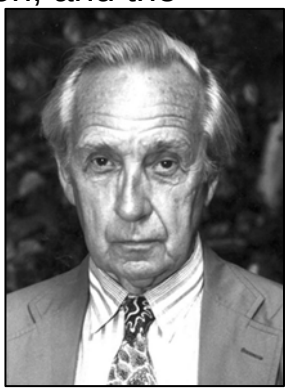
officers, who have to take final responsibility, must not only fully understand the sources, methods, and extent of their intelligence organisation, but also personally know their intelligence officers sufficiently well to assess their capabilities and to rely on their assessments or, if they are not satisfied, replace them.'[1]

FAILURE OF COMMAND – SITUATING THE APPRECIATION: OPERATION MARKET GARDEN 1944

5A2. In September 1944, Major Brian Urquhart was the intelligence officer for the 1st Airborne Corps during the planning for Operation MARKET GARDEN, an ambitious airborne operation designed to seize the Dutch bridges over the rivers blocking the Allied advance into northern Germany. During the operational planning, Urquhart became convinced that the plan was critically flawed based on his analysis of information obtained from aerial reconnaissance (imagery intelligence) and the Dutch resistance (human intelligence). He even tasked reconnaissance aircraft over the drop zone to confirm his analysis. Confident in his assessment he briefed General 'Boy' Browning the commander of 1st Airborne Corps that a German SS panzer division was refitting in Arnhem, which was the main target for 2 airborne brigades.

5A3. General Browning rejected the assessment. He dismissed Urquhart and had the senior medical officer send him on sick leave due to *nervous strain and exhaustion*.[2] The subsequent failure of the operation, and the heavy casualties that resulted, vindicated Urquhart's assessment. Urquhart was a very high-grade officer and would later rise to become an Under-Secretary General at the UN in which capacity he organised the first UN Peacekeeping mission after the Suez Crisis in 1957. Browning could not see this quality. He was fixated by his own plan and was determined not to let anything or anyone stand in his way. It was a fateful decision.

Lt Gen Sir Frederick 'Boy' Browning GCVO, KBE, CB, DSO Commander 1st Airborne Corps



Brian Urquhart when Under-Secretary General of the UN

[1] Beesly, P, Convoy PQ17, A Study of Intelligence and Decision Making, published in Intelligence and Military Operations, Michael I. Handel, London, 1990, pages 292-322.
[2] Middlebrook, M, *Arnhem 1944: The Airborne Battle*, Penguin, 1995, page 66.

FAILURE OF INTELLIGENCE – 9/11 TERRORIST ATTACKS

5A4. In February 1995 the US Congress' Special Task Force on Terrorism and Unconventional Warfare published a warning that al-Qaeda was planning a terrorist attack on lower Manhattan using hijacked civilian airlines as flying bombs. All intelligence agencies were issued with a report regarding this threat. However, despite this warning, on 11 September 2001 al-Qaeda terrorists hijacked 4 commercial passenger jet airliners and intentionally crashed 2 of the airliners into the Twin Towers of the World Trade Center in New York City, killing everyone on board and many who were working in the buildings. Both buildings collapsed within 2 hours, killing a number of rescue workers and destroying or damaging nearby buildings. The third airliner was flown into the Pentagon, home of the US Department of Defense. The fourth plane crashed into a field in Pennsylvania after some of its passengers and flight crew attempted to retake control of the plane, which the hijackers had redirected toward Washington. There were no survivors from any of the flights and 3,000 people died in the attacks.

5A5. On 27 November 2002 the 9/11 Commission was established to investigate the terrorist attacks. The final report issued on 22 July 2004 stated that the attacks were a shock, but they should not have come as a surprise. Islamic extremists had given plenty of warnings that they meant to kill Americans indiscriminately and in large numbers. The Report continued that '*during the spring and summer of 2001, U.S. intelligence agencies received a stream of warnings about an attack al-Qaeda planned, as one report puts it 'something very, very, very big.'* George Tenet, the Director of Central Intelligence, stated that '*the [warning] system was blinking red*.'

5A6. Rovner and Long state that the 9/11 Commission found that the intelligence community suffered from a lack of institutional imagination before the September 11 attacks.[3] This made it impossible for most analysts and policymakers to gauge the terrorist threat. Had they better understood the danger of al-Qaeda they could have taken steps to improve warning

[3] Rovner J and Long A, *Breakthroughs*, Volume 14 number 1 (Spring 2005), pages 10-21.4.

intelligence. More imagination also might have helped analysts reveal the crucial network of terrorists that planned and executed the attacks. In other words, the intelligence community could not *connect the dots* because it was not sufficiently imaginative.

CHAPTER 6 – INTELLIGENCE SUPPORT TO JOINT OPERATIONAL PLANNING

'Although the process is disliked, a joint-interagency approach to planning is critical; it is the glue that brings players together cementing the relationships. It also provides a shared vision and means of achieving it.'[1]

Rear Admiral Dave Buss, US Navy

Chapter 6 examines intelligence support to joint operational planning. This includes: pre-deployment preparation; undertaking joint intelligence preparation of the operational environment and intelligence support to planning. The Chapter ends with a case study on the use of intelligence during operational planning. The nature of these activities requires an inherently joint, inter-agency approach. JDP 04 *Understanding* and JDP 5-00 *(*2nd Edition) *Campaign Planning* both explain how the operational estimate relates to the 5-step rational planning process, which is a good start point for developing a common joint, inter-agency approach.

SECTION I – PREPARATION

601. It is important to maintain core intelligence capabilities and skills in anticipation of future operational requirements. This applies particularly to those intelligence disciplines that are not easily surged due to the long lead times required to establish resources (for example due to the need for specialist language training, technical development or source recruitment).

602. Joint task force headquarters staffs provide the intelligence production and dissemination focus for operational and deployed force activity beyond the UK.[2] These staffs, in close co-operation with Defence Intelligence, are responsible for estimating an adversary's courses of action, centres of gravity and vulnerabilities. At the outset of campaign, intensive planning ensures that appropriate intelligence is available to the joint task force commander and his assigned forces.

603. **Intelligence Support to Operational Staff Work**. Intelligence supports development of all headquarters output at the strategic, operational and tactical levels; Figure 6.1 depicts this support. All members of the intelligence

[1] Rear Admiral Buss US Navy, Commander CJ5, Headquarters Multinational Forces–Iraq, June 2008-May 2009, extracted from his interview to the Headquarters Multinational Force-Iraq Historian in March 2009.
[2] This includes not only the staff of the intelligence branch, but also the operations and plans staffs.

staff should understand their specific responsibilities for the production of each of these documents.

Strategic	• CDS Directive • Joint Commander's Directive • CDS Planning Directive
Operational	• JTFC Planning Guidance • Campaign Directive • Force Instruction Document • Operation Plans (OPLANs)
Operational and Tactical	• Contingency Plans (CONPLANs) • Operation Orders (OPORDs) • Fragmentary Orders (FRAGOs)

Figure 6.1 – The Hierarchy of Joint Operational Staff Work

604. **The Intelligence Directive**. The intelligence staff should draft an intelligence directive for their formation's element of an operation, informed by PJHQ's *Intelligence and Security Management Plan* (see paragraph 522). This short, succinct and clearly understandable directive aims to:

a. Articulate the role of intelligence in the operation.

b. Define the area of intelligence responsibility and area of intelligence interest for the operation.

c. Clarify the intelligence architecture, command arrangements and information exchange requirements.

d. Define the roles and responsibilities of elements of the operational intelligence team.

e. Detail what collection assets are available within the operation and their tasking arrangements.

f. Outline intelligence agencies and their liaison arrangements.

g. Confirm the battle-rhythm and intelligence reporting requirements for the operation.

Once complete, the intelligence directive requires approval by the commander and inclusion as an annex in the overall operation order.

605. **Example Intelligence Directive Format**. Figure 6.2 is an example of an intelligence directive format:

Context

Aim

Scope

UK National Aim

Operating Space

- Joint Operational Environment
- Joint Operations Area
- Area of Intelligence Responsibility
- Area of Intelligence Interest

J2 Mission

Concept of Operations

- Intent
- Scheme of Manoeuvre
- Main Effort

Specific Tasks

Troops To Task/Manning

- Assigned and Non-assigned Military Assets
- National and Defence Intelligence Assets
- Multinational/Coalition Assets

Force Preparation

Oversight and Governance

- Collaboration Protocols
- Arrangements for Fusion

Command and Control

- Chain of Command
- Joint Operational Architecture
- Communications and Information Systems

Figure 6.2 – An Example of an Intelligence Directive Format

SECTION II – JOINT INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT

606. Joint intelligence preparation of the operational environment is a continuous process that seeks to provide an understanding of the operating environment and forms the basis for the development of the joint intelligence estimate. It produces a dynamic product that focuses intelligence effort and informs prioritisation of intelligence requirements. In addition to contributing to the early stages of the operational estimate, it assists in the implementation of the operations plan by identifying opportunities to promote decisive action. It underpins the operational planning process, execution and assessment of operations. It encompasses the *process* for intelligence development and up-dates, and the *product* itself, using a variety of formats that offer:

a. Ease and speed of updating, presenting and prioritising large quantities of intelligence, usually in graphical form.

b. Ease of assimilating information, incorporating changes to the intelligence picture and identifying threats and opportunities.

607. The joint intelligence preparation of the operational environment promotes situational awareness and highlights future requirements for intelligence. It relies on the constant interaction between headquarters' staff from the intelligence, operations and plans branches to ensure accurate representation of current and future activities of friendly, neutral and hostile actors. It is widely exploited across the headquarters for a variety of purposes.

608. The joint intelligence preparation of the operational environment should:

a. Define the operating environment.

b. Describe the environment's effects on the conduct of operations.

c. Analyse the actors or intended targets.

d. Identify possible risks to operations.

e. Identify areas where intelligence collection assets must monitor or detect threats or assess progress.

f. Identify opportunities where friendly forces can influence events or opinions through lethal or non-lethal means.

g. Identify decision points when the commander must act to influence the outcome of the operation.

h. Analyse the commander's and adversary's centres of gravity.

609. The joint intelligence preparation of the operational environment is a systematic and cyclical process that is closely connected to the individual stages of the commander's decision-making process. A series of overlays normally represent in graphical form the results of the process; these overlays include basic data on terrain, obstacles, weather, the adversary's tactical doctrine or preferred scheme of manoeuvre and any other actors impacting on the operation, all of which can be prepared well in advance. Just before and during operations, inclusion of updates serves to reflect changes in key factors that may affect force activity across the spectrum of conflict. Figure 6.7 depicts the 4 broad stages within the joint intelligence preparation of the operational environment process.

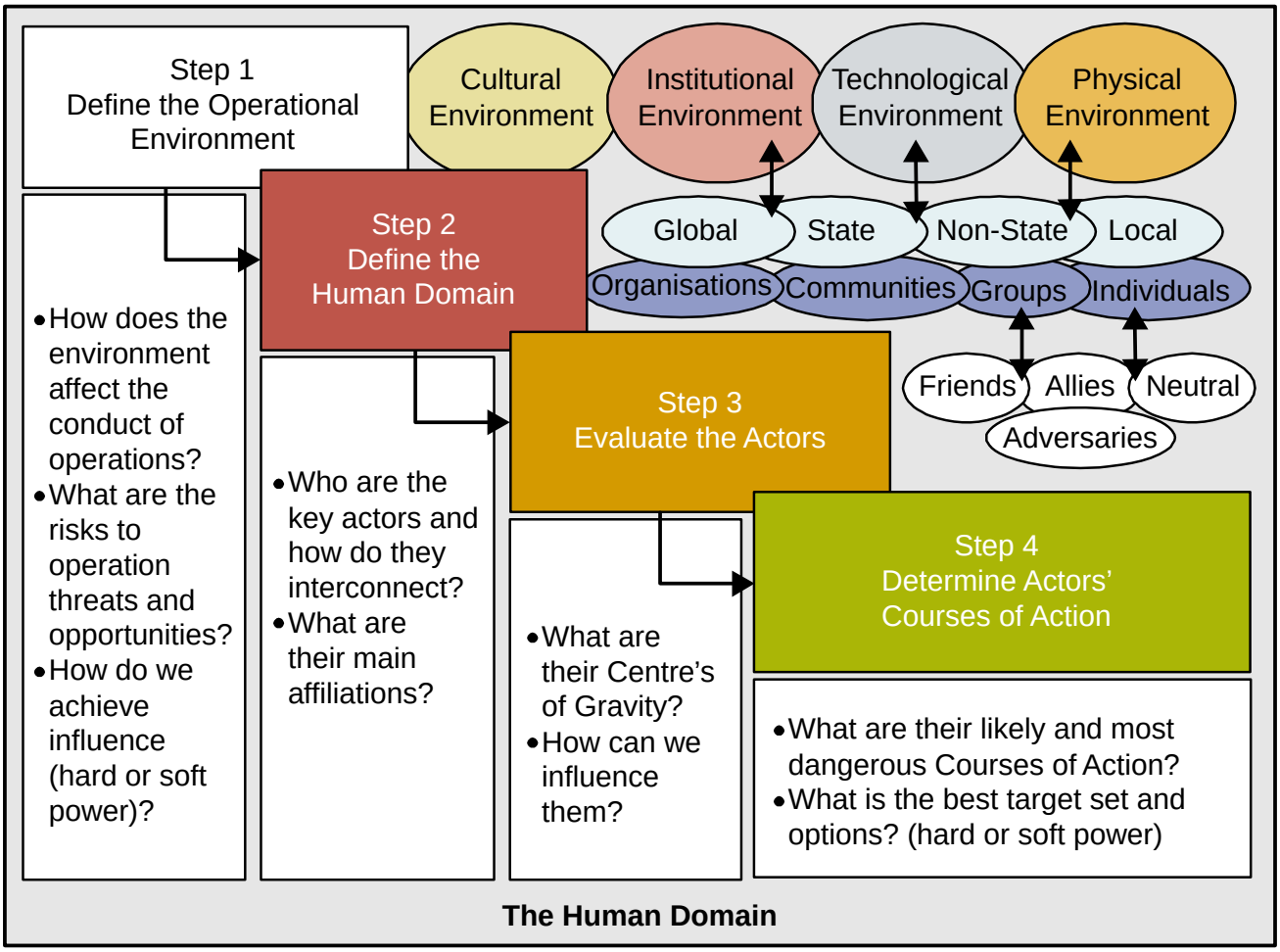


Figure 6.7 – The 4 Steps of the Joint Intelligence Preparation of the Environment

SECTION III – INTELLIGENCE SUPPORT TO PLANNING

610. The intelligence process does not work in isolation from other planning processes within a headquarters. To achieve the optimum effect all of the planning processes should be synchronised. At the joint operational level, the intelligence process is one of the key activities that support the campaign

planning process. The intelligence process is a continuum and the constant flow and updating of information within the cycle may provide intelligence that fundamentally changes the campaign plan at any stage during the planning process. Figure 6.3 provides a graphic illustration of how the intelligence cycle relates to other staff branches and planning functions within a joint headquarters.

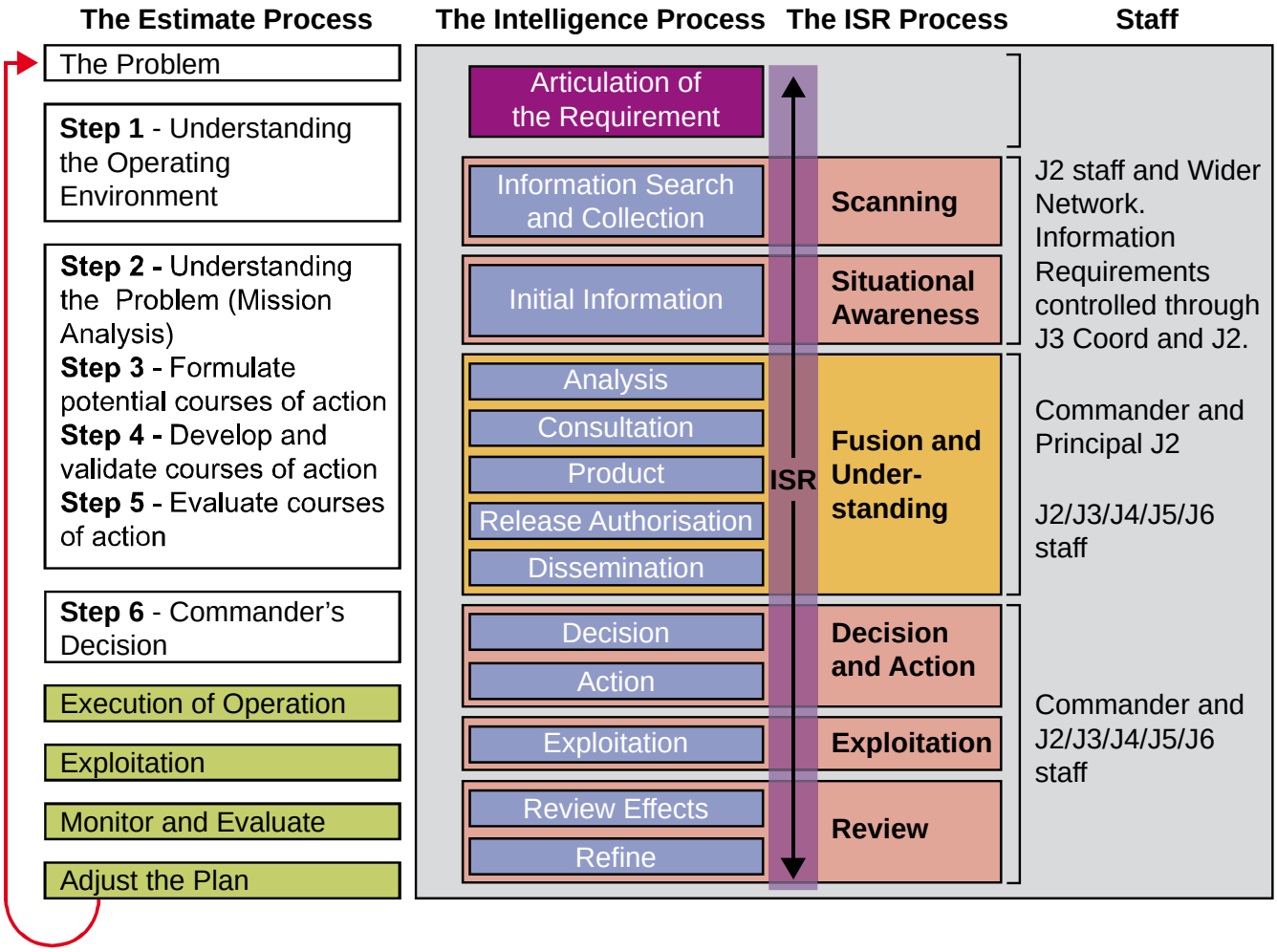


Figure 6.3 – The Interrelationship between the Intelligence, Staff Functions and Planning

611. **Intelligence Support to the Joint Operational Estimate**. The operational estimate is fundamental to campaign planning and to supporting operations. It aims to reduce a complex mass of information into a number of courses of action from which the commander will select his preference. It is by this means that the commander formulates a campaign plan. Intelligence supports the joint operational estimate by developing understanding to enhance decision-making. Intelligence staffs must remain cognisant of the commander's requirements as they evolve, so the commander must include the intelligence staff in all aspects of his planning.

612. **The Joint Intelligence Estimate**. The joint intelligence estimate is a product of the estimate process. It informs the operational estimate process, contributing to the commander's understanding and informing campaign planning. The joint intelligence estimate aims to:

a. Describe the operational environment and the adversaries.

b. Provide input to the evaluation of actors and analyse centres of gravity.

c. Assist the development of understanding.

d. Furnish the commander with basic intelligence that provides reference material for the operational estimate.

e. Provide the starting point for intelligence planning by identifying intelligence requirements.

f. Highlight intelligence-sharing requirements between nations.

Intelligence gathering will add progressively more detail to the joint intelligence estimate, which in combination with the deductions from the joint intelligence preparation of the operational environment, provides significant input to the operational estimate.

613. **The 6-Step Operational Estimate Process**. The operational estimate process is command led, but is intelligence driven. JDP 5-00 describes the 6-step operational estimate process that forms the joint operational estimate. Figure 6.4 summarises the process.

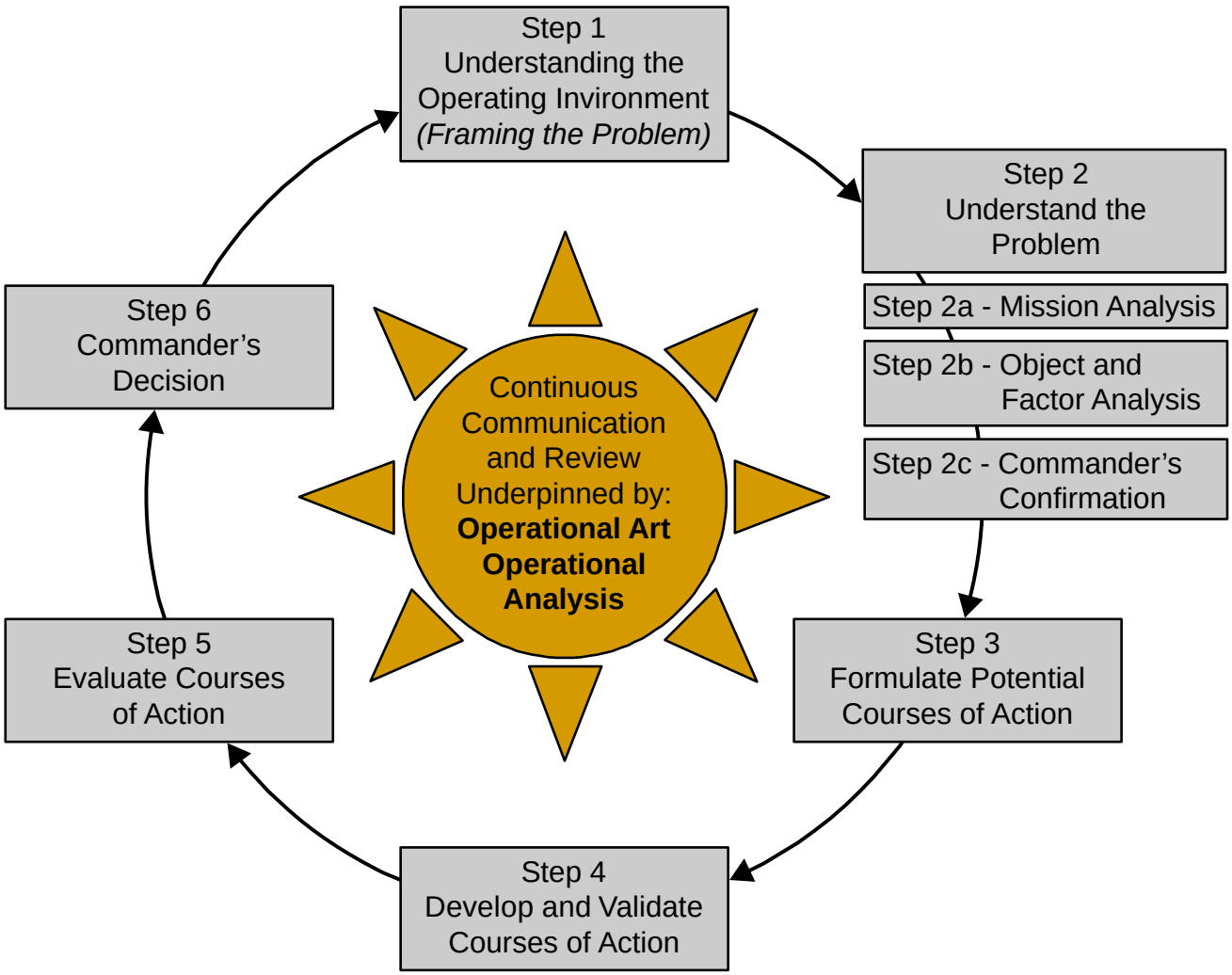


Figure 6.4 – The 6-Step Joint Operational Estimate

a. **Step 1** – **Understand the Operating Environment**. The joint intelligence estimate forms the basis of understanding the operating environment.[3] The primary focus of the Step 1 is to achieve collective and common situational awareness.

b. **Step 2** – **Understand the Problem**. The commander's principal intelligence adviser and his staff play a critical role in identifying and analysing the problem through the conduct of the joint intelligence estimate. The principal intelligence adviser also helps the commander to identify his critical information requirements. By understanding the mission and the commander's intent, he can direct his intelligence staff to begin detailed intelligence planning. This will include: analysing the impact of the operational environment on UK national agencies; identifying gaps in the deployed intelligence architecture; identifying the specific and implied intelligence tasks; reviewing the availability and capabilities of intelligence assets; determining the commander's initial

[3] Chapter 4 describes the joint operating environment in more detail.

critical information requirements; determining the limitations of intelligence support; proposing acceptable risk guidelines; and conducting a thorough timeline estimate. Specifically:

(1) **Step 2a**. **Mission Analysis**. The commander's command group conducts step 2a. This should include the principal intelligence adviser, but this is dependent upon the commander. Intelligence support to mission analysis outputs includes: support to developing the initial campaign end-state and objectives; the development of potential centres of gravity; and staffing of commander's critical information requirements.

(2) **Step 2b**. **Object and Factor Analysis**. The intelligence input during Step 2b is critical. It is here that intelligence staff begin to develop understanding for the commander. The joint intelligence preparation of the operational environment and other intelligence products form the basis of object and factor analysis.

(3) **Step 2c**. **Commander's Confirmation**. Intelligence staff can help to provide final confirmation of issues raised through the commander's critical information requirements process.

c. **Step 3 – Formulation of Potential Courses of Action**. Step 3 is a command-led activity. The commander identifies what he considers the optimum course of action for his staff to develop in detail. The principal intelligence advisor has an important role in helping the commander decide which to choose.

d. **Step 4 – Development of Course of Action and Step 5 - Evaluation of Course of Action**. Intelligence input to courses of action development and evaluation includes:

(1) Conducting a review of the situation and environmental characteristics, concentrating on those aspects that have changed since development of the initial courses of action.

(2) A detailed description, in priority order, of the threats for each course of action from most likely to least likely and from most dangerous to least dangerous.

(3) Support to war-gaming (described in paragraph 615).

(4) Updating understanding through responses to the commander's critical information requirements and other information requirements.

e. **Step 6 – Commander's Decision**. During Step 6, the intelligence staffs support any war-gaming (if required at this stage) that the commander requires before making his final decision. Subsequently, a final intelligence assessment is required for the joint force commander's directive.

614. **Intelligence Support to Warning Orders**. Plan development is a collaborative process within the headquarters and between subordinate and neighbouring formations. In general, development of a campaign or operational plan will require the issue of at least 3 iterative warning orders, as Figure 6.5 depicts. The first warning order provides a basic intelligence summary at the start of the planning process outlining the operational environment and the actors within it. Warning order 2 refines the intelligence assessment based on analysis of the joint intelligence estimate and the more holistic joint intelligence preparation of the operational environment. Warning order 3 refines this information further and provides sufficient understanding to allow the commander to make effective decisions.

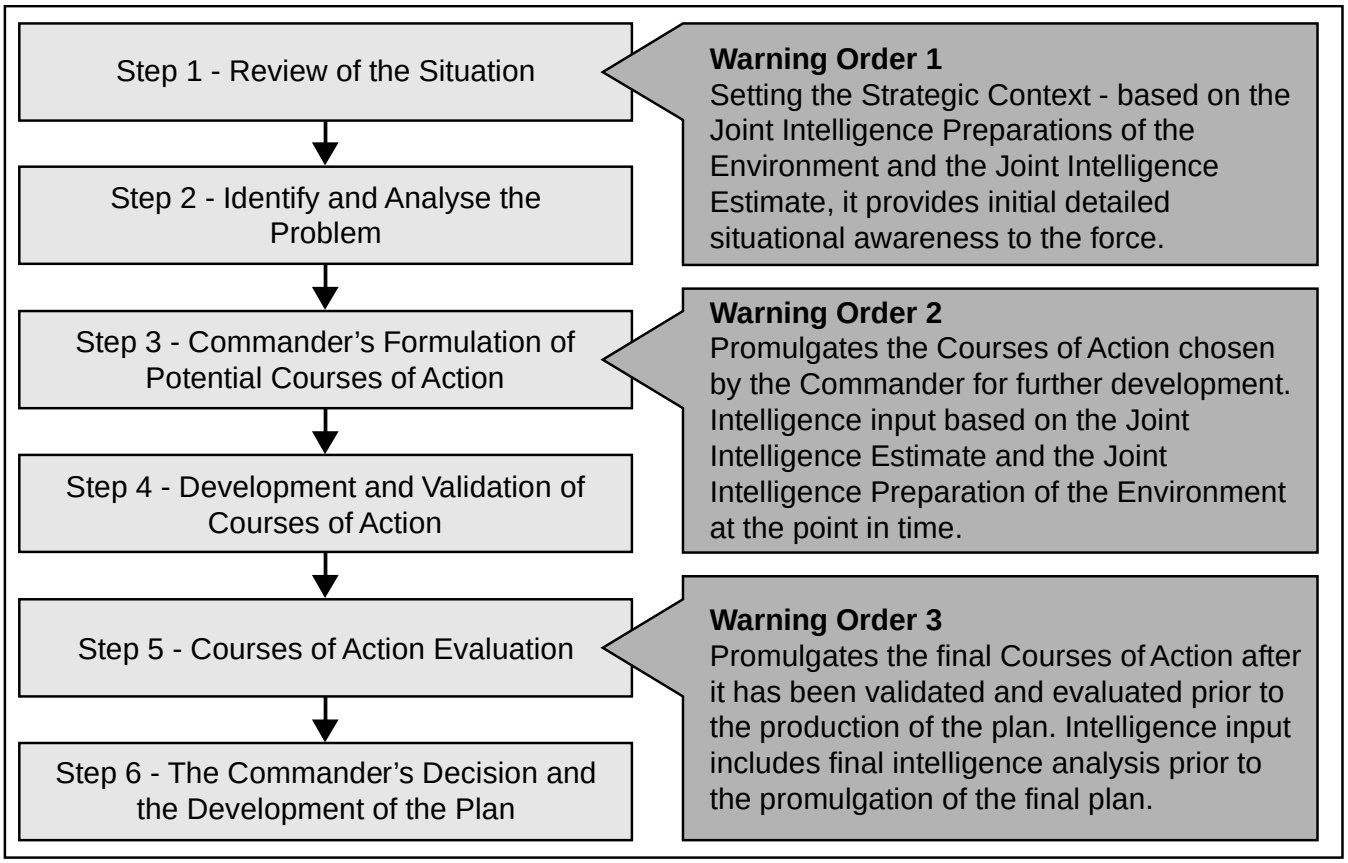


Figure 6.5 – Intelligence Support to Warning Orders

615. **The Intelligence Staff and War-gaming**. War-gaming normally occurs from Step 4 onwards, as represented in Figure 6.6. The intelligence staffs play an important role in this process, providing the overall context for the operation and representing the various actors, especially adversaries. In addition, intelligence personnel (usually from organisations external to the participating headquarters) often provide the red team.[4]

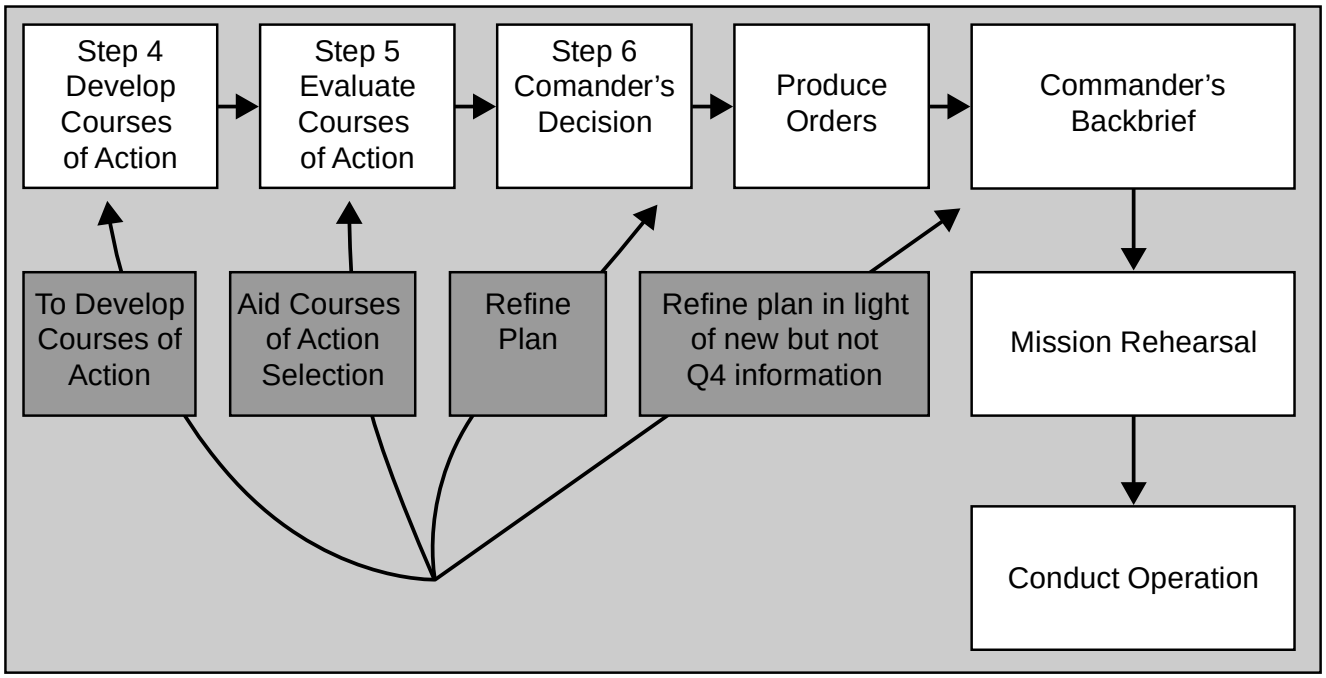


Figure 6.6 – **War-gaming Support to the Joint Operational Estimate**

[4] The Development, Concepts and Doctrine Centre's *A Guide to Red Teaming* contains more information on Red Teaming.

Case Study - Intelligence Support to Planning and Operations
The Battle of Midway June 1942

'The most stunning intelligence coup in all naval history.'

Sir John Keegan

In June 1942, the US Navy had a chance to contain the Imperial Japan's Navy at Midway Island in the Pacific Ocean. In the few weeks before the battle, the US Navy's Combat Intelligence Office, in charge of analysing and deciphering Japanese naval radio communications, received indications hinting that the Japanese Navy was preparing for a major attack. However, the deciphered Japanese messages referred to the attack target only by its code name, *AF*. There were several possible targets for such a major attack, and knowing which one was code named *AF* was critical. Commander Joseph P. Rochefort, head of the Combat Intelligence Office, thought that the intelligence indicated that *AF* was Midway Island, but needed proof. He called Midway via the underwater cable phone line, which the Japanese could not tap, and asked them to transmit a message that the water desalination facility in Midway was broken. Soon after, Rochefort's staff deciphered a Japanese radio message saying that target AF was suffering a water shortage problem. This was the proof he needed and an extremely important intelligence breakthrough. With this information, the American commander, Admiral Nimitz, could concentrate his smaller force in the right place, at the right time, knowing that he knew the enemy's outline plan, a rare advantage for a commander. Due to their intelligence success, the US was ready to defend Midway and won this critical battle.

Admiral Chester Nimitz, Architect and Commander of the Victory at Midway

Planning and execution for the Midway operation fully exploited the intelligence. Having integrated operational intelligence into his decision-making, Admiral Nimitz devised a plan that was the turning point in the Pacific theatre of operations. It demonstrated that the integration of intelligence is vital to operational success when the commander has the vision to use it in his decision-making. The insightful and confident use of fused operational intelligence provided Admiral Nimitz with the foresight to capitalise on his own force strength and exploit the weaknesses of the enemy.

LEXICON

This Lexicon contains acronyms/abbreviations and terms/definitions used in this publication. Many of the terms and their definitions detailed in Part 2 are either *new* or *modified* following a recent review of this. For fuller reference on all other UK and NATO agreed terminology, see the current edition of JDP 0-01.1 *The UK Glossary of Joint and Multinational Terms and Definitions*.

PART 1 – ACRONYMS AND ABBREVIATIONS

AAP	Allied Administrative Publication
ABCA	American, British, Canadian, Australian and New Zealand Armies' Program
ACOUSTINT	Acoustic Intelligence
ACINT	Acoustic Intelligence
AJP	Allied Joint Publication
CCIRs	Commander's Critical Information Requirements
CHEMEX	Chemical Exploitation
CI	Counter-intelligence
CIFT	Counter-intelligence Field Team
CI-INTREP	Counter-intelligence Intelligence Report
CI-INTSUM	Counter-intelligence Intelligence Summary
CI-SUPINTREP	Counter-intelligence Supplementary Intelligence Report
COMINT	Communications Intelligence
CPERS	Captured Persons
DCDC	Development, Concepts and Doctrine Centre
EEIs	Essential Elements of Information
EIR	Enduring Intelligence Requirement
ELINT	Electronic Intelligence
EU	European Union
F3EA	Find, Fix, Finish, Exploit, Analyse
FABINT	Forensic and Biometric Intelligence
FCOC	Future Character of Conflict
FININT	Financial Intelligence
GCHQ	Government Communications Headquarters
GEOINF	Geospatial Information
GEOINT	Geospatial Intelligence
HUMINT	Human Intelligence

IMINT	Imagery Intelligence
INTREP	Intelligence Report
INTSUM	Intelligence Summary
IRM	Intelligence Requirements Management
IRM&CM	Intelligence Requirements Management and Collection Management
ISR	Intelligence, Surveillance, and Reconnaissance
JDN	Joint Doctrine Note
JDP	Joint Doctrine Publication
JIIM	Joint Inter-agency Intergovernmental and Multinational
JOA	Joint Operations Area
JOE	Joint Operational Environment
LOAC	Law of Armed Conflict
MASINT	Measurement and Signature Intelligence
MEDINT	Medical Intelligence
MOD	Ministry of Defence
MPE	Materiel and Personnel Exploitation
MULTI-INT	Multiple Source Intelligence
NATO	North Atlantic Treaty Organization
NSC	National Security Council
NSS	National Security Strategy
OSINT	Open Source Intelligence
OSCE	Organization for Security and Co-operation in Europe
PIRs	Priority Information Requirements
PJHQ	Permanent Joint Headquarters
RFI	Request for Information
RIPA	Regulation of Investigatory Powers Act 2000
ROE	Rules of Engagement
SDSR	Strategic Defence and Security Review
SIGINT	Signals Intelligence
SMA	Seized Media Analysis
SOFA	Status of Forces Agreement
SUPINTREP	Supplementary Intelligence Report
TECHINT	Technical Intelligence
UN	United Nations

PART 2 – TERMS AND DEFINITIONS

acoustic intelligence
Intelligence derived from the collection and processing of acoustic phenomena. (AAP-6)

agency
In intelligence usage, an agency is an organisation or individual engaged in collecting and/or processing information. (AAP-6)

agility
The physical and structural ability that allows forces to adjust rapidly and decisively, especially when operating in complex situations or in the face of new or unforeseen circumstances. (JDP 0-01.1)

analysis
In intelligence usage, a step in the processing phase of the intelligence cycle in which information is subjected to review in order to identify significant facts for subsequent interpretation. (AAP-6)

applied intelligence
Intelligence which is tailored to provide direct support to the decision-making process. (JDP 0-01.1)

area of intelligence interest
The area in which a commander requires intelligence on those factors and developments likely to affect the outcome of his current and future operations. (JDP 0-01.1)

area of intelligence responsibility
An area allocated to a commander, in which he is responsible for the provision of intelligence, within the means at his disposal. (AAP-6)

basic intelligence
Intelligence, on any subject, that may be used as reference material for planning and as a basis for processing subsequent information or intelligence. (AAP-6)

battle damage assessment
The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective. (JDP 0-01.1)

chemical exploitation
Provides chemical intelligence on IEDs, improvised weapons and unknown substances by processing, examining and analysing samples of materials (JDP 2-00 3rd Edition)

collation
In intelligence usage, a step in the processing phase of the intelligence cycle in which the grouping together of related items of information provides a record of events and facilitates further processing. (AAP-6)

collection
In intelligence usage, the exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence. (AAP-6)

collection management
In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing, tasking or coordinating with appropriate collection sources and agencies, monitoring results and re-tasking, as required. (AAP-6)

communications intelligence (COMINT)
Intelligence derived from electronic communications and communication systems by other than intended recipients or users. (AAP-6)

contingency planning
A plan which is developed for possible operations where the planning factors have been identified or can be assumed. This plan is produced in as much detail as possible, including the resources needed and deployment options, as a basis for subsequent planning. (JDP 0-01.1)

counter-intelligence
Those activities that identify the threat to security posed by hostile intelligence services or organisations or by individuals engaged in espionage, sabotage, subversion, terrorism or other non-traditional threats (JDP 2-00 3rd Edition)

covert passive surveillance
The covert systematic observation of a person, place, object or activity from a covert static observation post or by use of foot, vehicle or aircraft, in order to gain or develop intelligence. (JDP 2-00 3rd Edition)

cultural awareness
Cultural awareness is an awareness of the current and historic values, norms and beliefs reflected in different social structures and systems, and in particular how they contribute to an actor's motives, intents and behaviours. (JDN 1/09)

current intelligence
Intelligence that reflects the existing situation at any level of command. (JDP 2-00 3rd Edition)

direction
The initial stage in the intelligence process and consists of the determination and prioritisation of intelligence requirements, planning the collection effort, the issue of tasks and requests to collection, exploitation and processing assets or external agencies, and maintenance of a continuous check on the progress of intelligence requirements throughout their lifecycle. (JDP 2-00 3rd Edition)

dissemination
Dissemination is the timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it. (AAP-6)

electronic intelligence (ELINT)
Intelligence derived from electromagnetic non-communications transmissions by other than intended recipients or users. (AAP-6)

enduring intelligence requirements
Intelligence requirements that require regular and repeated satisfaction over time. (JDP 2-00 3rd Edition)

environment
The surroundings in which an organisation operates, including air, water, land, natural resources, flora, fauna, humans and their interrelation. (AAP-6)

evaluation
A step in the processing phase of the intelligence cycle constituting the appraisal of an item of information in respect of the reliability of the source and the credibility of the information. (AAP-6)

financial intelligence
The gathering of information about the financial affairs of entities of interest, to understand their nature and capabilities, and predict their intentions. (JDP 2-00 3rd Edition)

forensic and biometric intelligence (FABINT)
Intelligence derived from the application of multi-disciplinary scientific and technical processes and can often, although not exclusively, be collected to an evidential standard. (JDP 2-00 3rd Edition)

fusion
In intelligence usage, the blending of intelligence and/or information from multiple sources or agencies into a coherent picture. The origin of the initial individual items should then no longer be apparent. (AAP-6)

geospatial information (GEOINF)
Facts about the Earth referenced by geographical position and arranged in a coherent structure. It describes the physical environment and includes data from the aeronautical, geographic, hydrographical, oceanographic and meteorological disciplines. (JDP 0-01.1)

geospatial intelligence (GEOINT)
Geospatial Intelligence (GEOINT) *is the spatially and temporally referenced intelligence derived from the exploitation and analysis of imagery intelligence and geospatial information to establish patterns or to aggregate and extract additional intelligence*. (JDP 2-00 3rd Edition)

horizon scanning
In intelligence usage, horizon scanning is the systematic search across the global environment for potential threats, hazards and opportunities. (JDP 04)

human domain
The totality of the human sphere of activity or knowledge. (JDP 04)

human intelligence (HUMINT)
A category of intelligence derived from information provided by, or collected on, human sources and individuals of intelligence interest, as well as systematic and controlled exploitation, by interaction with, or surveillance of, those sources or individuals. (JDP 0-01.1)

imagery intelligence (IMINT)
Imagery intelligence is derived from imagery acquired by sensors which can be ground based, sea borne or carried by air or space platforms. (JDP 0-01.1)

indicators
In intelligence usage, an indicator is an item of information which reflects the intention or capability of a potential enemy to adopt or reject a course of action. (AAP-6)

individual understanding
Individual understanding is our own personal interpretation of the facts as they are presented to us. (JDP 04)

information
Unprocessed data of every description that may be used in the production of intelligence (AAP-6)

information requirements
Those items of information regarding the enemy and his environment which need to be collected and processed in order to meet the intelligence requirements of a commander. (AAP-6)

integration
In intelligence usage, a step in processing phase of the intelligence cycle whereby analyzed information and/or intelligence is selected and combined into a pattern in the course of the production of further intelligence. (AAP-6)

intelligence
The directed and co-ordinated acquisition and analysis of information to assess capabilities, intent and opportunities for exploitation by leaders at all levels. (JDP 2-00 3rd Edition)

intelligence, surveillance and reconnaissance (ISR)
The activities that synchronises and integrates the planning and operation of collection capabilities, including the processing and dissemination of the resulting product. (JDP 2-00 3rd Edition)

intelligence requirement
A requirement for assessed information about any aspect of a situation needed to develop a commander's understanding. (JDP 2-00 3rd Edition)

interpretation
In intelligence usage, Interpretation is the final step in the processing phase of the intelligence cycle in which the significance of information and/or intelligence is judged in relation to the current body of knowledge. (AAP-6)

joint action
The deliberate use and orchestration of military capabilities and activities to realise effects on other actors' will, understanding and capability, and the cohesion between them to achieve influence. (JDP 01 2nd Edition)

joint operations area
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 (JDP 0-01.1)

joint operational environment
The overall space, conditions and surroundings within which military forces operate. (JDP 2-00 3rd Edition)

materiel and personnel exploitation
The systematic collection, information processing and dissemination of intelligence obtained by tactical questioning, interrogation and the extraction of data from recovered materiel. (JDP 2-00 3rd Edition)

measurement and signature intelligence (MASINT)
The scientific and technical Intelligence from the analysis of data obtained from sensing instruments for the purpose of identifying any distinctive features associated with the source, emitter or sender, to facilitate the latter's measurement and identification. (AAP-6)

Measurement of effect
The assessment of the realisation of specified effect. (JDP 3-00 3rd Edition)

medical intelligence
Intelligence derived from medical, bio-scientific, epidemiological, environmental and other information related to human or animal health. (JDP 4-03)

multiple source Intelligence (MULTI-INT)
The deliberate application of 2 or more discrete but supporting intelligence disciplines (e.g. GEOINT, HUMINT and SIGINT) seeking to improve the quality of the intelligence product. (JDP 2-00 3rd Edition)

non-dedicated ISR
Those assets not procured by MOD for specific ISR tasks but contribute to the intelligence picture as part of their routine operations. (JDP 2-00 3rd Edition)

open source intelligence (OSINT)
Intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access. (AAP-6)

operational intelligence (OPINTEL)
Intelligence required for the planning and conduct of campaigns at the operational level. (AAP-6)

priority intelligence requirements
Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decision-making. (AAP-6)

processing
In intelligence usage, processing is the conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation. (AAP-6))

reconnaissance
A mission undertaken to obtain, by visual observation or other detection methods, information about the activities, and resources of an opponent or potential opponent, or to secure data concerning the meteorological, hydrographical, or geographic characteristics of a particular area. (AAP-6)

resource tasking
The activity undertaken to complete the intelligence collection plan by selection of the most appropriate ISR resource types for which tasking authority has been allocated. (JDP 2-00 3rd Edition)

seized media analysis
The systematic exploitation of either hard copy documents or electro-magnetically stored data, including that found on hard drives, data discs and personal communications systems. (JDP 2-00 3rd Edition)

signals intelligence (SIGINT)
The generic term used to describe communications intelligence and electronic intelligence when there is no requirement to differentiate between these two types of Intelligence, or to represent fusion of the two. (AAP-6)

single intelligence environment
The overall space, conditions and surroundings within which the military intelligence structure interfaces and operates with other national and international information and intelligence agencies in order to support decision-makers at all levels. (JDP 2-00 3rd Edition)

situational awareness
In intelligence usage, situational awareness is the ability to identify trends and linkages over time, and to relate these to what is happening and what is not happening. (JDP 04)

source
In intelligence usage a source is a person, object, process or system from where information can be obtained. (JDP 2-00 3rd Edition)

strategic intelligence
Intelligence required for the formation of policy, military planning and the provision of indications and warning, at the national and/or international levels. (AAP-6)

surveillance
Surveillance is the systematic observation of aerospace, surface or subsurface areas, places, persons or things, by visual, aural, electronic, photographic, or other means. (AAP-6)

tactical intelligence
Intelligence required for the planning and execution of operations at the tactical level. (AAP-6)

target
The object of a particular action, for example a geographic area, a complex, an installation, a force, equipment, an individual, a group or a system, planned for capture, exploitation, neutralisation or destruction by military forces. (AAP-6)

targeting
The process of selecting and prioritising targets and matching the appropriate response to them taking into account operational requirements and capabilities. (AAP-6)

technical intelligence (TECHINT)
Intelligence concerning foreign technological developments, and the performance and operational capabilities of foreign material that may have, or may eventually have a practical application for military purposes. (AAP-6)

understanding
In the military context, understanding is the perception and interpretation of a particular situation in order to provide the context, insight and foresight required for effective decision-making. (JDP 04)

weapons intelligence
Intelligence concerning components, manufacture, origin and method of employment of all foreign and domestic conventional and improvised weapons, munitions and devices. (JDP 2-00 3rd Edition)

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 the North Atlantic Treaty Organization (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 JDPs.[1] From time to time, Interim JDPs (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 out of operations.

Urgent requirements for doctrine are addressed through Joint Doctrine Notes (JDNs). To ensure timeliness, they are not subject to the rigorous staffing processes applied to JDPs, particularly in terms of formal external approval. Raised by the DCDC, they seek to capture and disseminate best practice or articulate doctrinal solutions. This can subsequently be developed in due course as more formal doctrine.

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