Ministry of Defence

Joint Doctrine Publication 2-00

Intelligence, Counter-intelligence and Security Support to Joint Operations

Fourth Edition

Joint Doctrine Publication 2-00

Intelligence, Counter-intelligence and Security Support to Joint Operations

Joint Doctrine Publication 2-00 (JDP 2-00) (4th Edition), dated August 2023, is promulgated as directed by the Chiefs of Staff

Director Development, Concepts and Doctrine Centre

Authorisation

The Development, Concepts and Doctrine Centre (DCDC) is responsible for publishing strategic trends, joint concepts and doctrine. If you wish to quote our publications as reference material in other work, you should confirm with our editors whether the particular publication and amendment state remains authoritative. We welcome your comments on factual accuracy or amendment proposals. Please contact us via email at: DCDC-DocEds@mod.gov.uk

Copyright

Distribution

All DCDC publications can be demanded from the LCSLS Headquarters and Operations Centre.
LCSLS Help Desk: 01869 256197 Military Network: 94240 2197

Our publications are available to view and download on defnet (RLI) at: https://modgovuk.sharepoint.com/sites/IntranetUKStratCom/SitePages/development-concepts-and-doctrine-centre-dcdc.aspx

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

Preface

Purpose

1. The traditional military focus for intelligence and understanding was identifying and knowing about adversaries to either neutralise or defeat them. Operations across multiple operational domains now demand a broader understanding of all audiences, and intelligence supports commanders in gaining that understanding. Joint Doctrine Publication (JDP) 2-00, *Intelligence, Counter-Intelligence and Security Support to Joint Operations*, 4th Edition, reinforces the enduring cross-governmental nature of intelligence and the need to inculcate a spirit of collaboration, including with partners and allies, in an interdepartmental and inter-agency context. To support this approach, commanders at all levels require accurate and timely intelligence and understanding to inform their decision-making. They must also know and understand their own role and that of their staff in developing and delivering it.

Context

2. UK policy is to adopt North Atlantic Treaty Organization (NATO) doctrine wherever possible. The retention of JDP 2-00 as the UK's keystone intelligence publication is driven by several factors, including the implementation of integrated action and the concept of multi-domain integration, which impacts on intelligence and understanding. Additionally, the UK's intelligence community has pursued a significant programme of professionalisation in analysis and analytical tradecraft, establishing new national standards to which the Ministry of Defence (MOD) is subject.

Audience

3. JDP 2-00 is written with three audiences in mind. First, it provides the opportunity for commanders at all levels to gain an understanding of the value of intelligence and the intelligence process. Secondly, it provides a reference document for MOD intelligence specialists (both civilian and military) on which subordinate documents can be based. Finally, it provides external readers with an explanation of MOD intelligence functions.

Structure

4. JDP 2-00 is divided into seven chapters with a supporting lexicon. An outline of the chapter contents is described below.

a. **Chapter 1 – A contemporary approach to understanding and intelligence.** This chapter explains the strategic context and the challenges for intelligence in the contemporary operating environment.

b. **Chapter 2 – The fundamentals of intelligence.** This chapter considers a number of fundamental concepts that ensure commonality during MOD intelligence activities.

c. **Chapter 3 – The core functions and the intelligence cycle.** This chapter explains how intelligence is developed and provides detail on the principal intelligence functions.

d. **Chapter 4 – Intelligence disciplines and activities.** This chapter explains the core disciplines, specialisms and activities that collect information, which is subsequently processed into intelligence.

e. **Chapter 5 – Intelligence and counter-intelligence support to joint operations.** This chapter reviews intelligence support to joint operations. It concludes with a review of different approaches to intelligence development and an introduction to problem-centric approaches using activity-based intelligence.

f. **Chapter 6 – Underpinning joint intelligence: people, structures and training.** This chapter explores the role and specific responsibilities of the joint commander and the intelligence staff. It also considers joint operational intelligence architectures.

g. **Chapter 7 – Intelligence support to joint operational planning.** This chapter outlines intelligence support to operational planning. It also highlights the stages in which intelligence contributes significantly to the operations planning process.

Linkages

5. JDP 2-00 is intended to be read in conjunction with NATO's Allied Joint Publication (AJP)-2, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*. It should also be considered alongside AJP-01, *Allied Joint Doctrine*, JDP 0-01, *UK Defence Doctrine*, 6th Edition, the NATO AJP-2 series of publications, and AJP-10.1, *Allied Joint Doctrine for Information Operations* (with UK national elements).

Contents

Chapter 1

Chapter 1 explains the strategic context and the challenges for intelligence in the contemporary operating environment. In particular, the chapter introduces integrated action and audience analysis to this publication, with audience analysis a primary consideration for intelligence staff.

1

> Vital intelligence is no longer scarce, and it is easily accessible. The extraordinary capabilities of modern sensor technologies mean that the moves of prospective enemies can be monitored constantly ... While intelligence gathering has been transformed, and should alert civilian and military policymakers to dangers and opportunities, it is still not necessarily predictive – even the best intelligence can be subject to a range of interpretations.

Lawrence Freedman, *Command*

Chapter 1

A contemporary approach to understanding and intelligence

Section 1 – The strategic context and integrated action

1.1. The nature of war does not change, but the character of warfare is changing rapidly, driven by the pace and pervasiveness of information and technological change. Distinctions between public and private, foreign and domestic, state and non-state, and virtual and physical are blurred.[1] The continuum of competition, as explained in Joint Doctrine Publication (JDP) 0-01, *UK Defence Doctrine*, 6th Edition, highlights the challenge of how international relations is conducted in the modern world. Set against this context, it is essential to provide high quality intelligence to support decision-making.

1.2. **Multi-domain approach.** JDP 0-01, *UK Defence Doctrine* refers to the concept of multi-domain integration (MDI), where the greatest benefits come from being able to sense, understand, plan and then orchestrate combinations of activities across operational domains in concert with the other instruments of national power, the North Atlantic Treaty Organization (NATO) and other like-minded allies and partners. NATO refers to this framework as multi-domain operations and it is described further in Allied Joint Publication (AJP)-01, *Allied Joint Doctrine*.

1.3. **Integrated action.** Integrated action can be described as the audience-centric orchestration of military activities, across all operational domains, synchronised with non-military activities to influence the attitude and behaviour of selected audiences necessary to achieve successful outcomes.[2] Commanders need to: be clear about the outcome they seek; study the audiences relevant to the achieving the identified outcome; and analyse the

1 Joint Doctrine Publication (JDP) 0-01, *UK Defence Doctrine*, 6th Edition, Chapter 1.
2 JDP 0-01, *UK Defence Doctrine*, 6th Edition, Chapter 2.

effects they wish to create on those target audiences. Only then should the mix of capabilities that are required to create physical, cognitive and virtual effects across the operational domains to affect the understanding, physical capability, will and cohesion of the audiences to achieve a successful outcome be determined. Understanding the audience is the major consideration of integrated action in pursuit of the outcome.

1.4. **Audience analysis.** Competition among states (and other actors) pursuing perceived interests is an inherent feature of international relations. Recognising that people, their decisions and behaviours, are at the heart of how international relations is conducted and how competition is resolved, a key part of integrated action is analysis to understand audiences. Audiences are segmented into three general categories – public, stakeholders and actors – depending on their ability to affect our outcomes. Intelligence is critical to enabling the understanding that provides the focus for planning and executing activity to create or maintain the attitudes that constitute behaviour. Commanders, with an understanding of the strategic narrative, can then conduct target audience analysis to identify the effects they wish to create.

1.5. **Threats, challenges and competitors.** Intelligence supports the development of understanding across the spectrum of potential threats and challenges, and in understanding our competitors. Table 1.1 illustrates some of the most significant areas of intelligence focus.[3]

Threat	Description
Peer threats	An adversary with the capability and capacity to oppose UK Armed Forces across multiple operational domains worldwide or in a specific region, where they may also enjoy a position of relative advantage.
Hybrid threats	These occur where military and non-military conventional, irregular and asymmetric threats are combined at the same time and space.
Cyber threats and the information space	Adversaries may operate in the cyber and electromagnetic domain as well as the physical environments.
Terrorism	The unlawful use, or threatened use, of force or violence.
Espionage	Clandestine intelligence acquisition activity, typically conducted for or by a hostile intelligence service.

3 AJP-2, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*, Chapter 1.

Threat	Description
Vulnerable, failing, failed, post crisis or recovering states	Instability and violence may be more likely in those states that are less well-developed and where the state is unwilling or unable to provide security and basic services to a significant portion of the population.[4]
Climate change and environmental threats to humans	Unpredictable natural and human-induced phenomena can cause disease, forced migration and humanitarian disasters, which can result in a range of human insecurities. Climate change may also be a 'threat multiplier' given its potential to amplify traditional security challenges.
Weapons proliferation	The proliferation of weapons of mass effect and their means of delivery or manufacture may threaten severe consequences for global stability.
Organised crime	Transnational, national or local groupings of criminal enterprises engaging in illegal activity, commonly for money and profit. Organised crime may also have links to terrorist or violent extremist activity.

Table 1.1 – Areas of intelligence focus

1.6. **Human security.** Human security is an approach to national and international security that places the emphasis on human beings, rather than the traditional focus on the security of the state. It is a framework that considers pre-, inter- and post-conflict phases, examines early warning mechanisms and responds to violent and destabilising situations. It is applicable to situations above and below the threshold of armed conflict, across all operational domains and boundaries. Defence's approach uses the human security framework to understand root causes of crises and conflict, thereby: enabling better identification of opportunities for prevention and protection; mitigating the effects of harm; identifying enduring solutions; and strengthening the prospect of mission success.

4 For further detail see AJP-3.28, *Allied Joint Doctrine for the Military Contribution to Stabilization*, Section 4.

Intelligence must be able to respond dynamically in times of rapidly emerging crises

Section 2 – Purpose and aims of intelligence, counter-intelligence and security

1.7. **The relationship between intelligence and understanding.** Understanding comes from applying judgement to knowledge to gain a deeper level of awareness of a situation and implications for the future. Judgement is a purely human skill, based on experience, expertise and intuition. Understanding, therefore, concerns acquiring, developing and applying knowledge to prioritise information requirements, make sense of a given context, make better decisions, and adapt and influence behaviours. Understanding includes having a detailed view of our national interests, our strategic partners and our international obligations. Intelligence plays a critical role by providing the processed information required to develop understanding. This includes not only answering the main intelligence questions of who, what, where, when, why and how, which provide the context and narrative of events, but also the deductive and predictive analysis (also known as insight and foresight), which provides the added value in an assessment. Further terms that are relevant when considering the development of intelligence and understanding are as follows.[5]

5 For a more detailed review of understanding, insight and foresight, see JDP 04, *Understanding and Decision-making*.

data
A reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.
Note: Data can be processed by humans or by automatic means. (NATOTerm)

information
Data arranged to convey meaning. (NATOTerm)

intelligence
The product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and other opportunities for exploitation by decision-makers. (NATOTerm)

understanding
The ability to understand something; comprehension.
(*Concise Oxford English Dictionary*)

The purpose of intelligence, counter-intelligence and security

1.8. **Intelligence in Defence.** The intelligence-contributing organisations and departments across Defence help deliver effective and efficient intelligence in support of the UK's national security objectives. In meeting these objectives at a strategic and operational level, Defence must understand the nature of global military, socio-economic, cultural, physical, political and human security circumstances, situations and scenarios for which the intelligence community provides that insight. Similarly, the intelligence community delivers outputs that contribute to that understanding.

1.9. **Intelligence support to operations.** Operational complexities require commanders and decision-makers to regard intelligence, counter-intelligence and security as a critical prerequisite for the way UK Armed Forces are deployed and operate. Commanders need to provide clear direction on their intelligence requirements and the priority of those requirements to ensure all available intelligence resources can be drawn on to develop the commander's understanding. Intelligence specialists will then develop intelligence networks to reflect the nature of the operation, emphasising the need for and enabling

collaboration at all levels, whilst they may also need to include arrangements for the integration of intelligence provided by allies or other government departments.

The aims of intelligence, counter-intelligence and security

1.10. **Intelligence.** Intelligence contributes to a continuous and coordinated understanding of the operating environment, thereby supporting commanders in their decision-making by helping to increase their understanding. Commanders and staff at every level require intelligence to plan, direct, conduct and assess campaigns and operations. Intelligence is crucial in setting strategy, identifying and selecting specific objectives and targets, associating those objectives and targets with desired effects, and determining the means to accomplish the overall mission. The primary aims of intelligence are as follows.

a. **Enable understanding.** The intelligence staff present intelligence about the operating environment and audiences, including their intentions, capability and motivation. The intelligence staff should strive to put this intelligence into the context of the commander's critical information requirements to enhance their understanding of the situation.

b. **Provide support to strategy formulation.** This role is largely defined by providing support and assessments to generate understanding of the operating environment, including adversaries and neutral actors' capabilities and intent. It also includes helping to articulate a desired end state, goals, objectives and an appraisal of the resources needed.

c. **Produce predictive assessments.** Intelligence should be forward looking, enabling commanders to maintain the initiative. Predictive assessments involve assessing risks[6] and identifying opportunities. To provide these predictive assessments, intelligence staff will use a number of techniques to analyse past and present intelligence to create possible and realistic adversary courses of action. To assist the understanding of risks and opportunities that a situation presents to the commander, intelligence staff will seek to deliver a predictive assessment articulated in terms of the 'most likely' and 'most dangerous' adversary courses of action that could occur. This provides the commander with the ability to plan within realistic bounds.

6 Risk to force, risk to mission and risk to reputation.

d. **Provide indicators and warnings.** Intelligence activities detect and report time-sensitive intelligence and information on developments that could involve or constitute a threat. It includes forewarning of actions or intentions.

e. **Intelligence monitoring.** Intelligence monitoring provides an intelligence baseline on countries, regions and actors before a crisis arises. Open-source material, Defence relations and diplomatic activity contribute to monitoring. Normally based on the results of horizon scanning, the Chief of the Defence Staff determines Defence's priorities for monitoring based on the advice of the Chief of Defence Intelligence (CDI) and drawing on requirements identified by the Joint Intelligence Committee (JIC). Intelligence monitoring comprises futures and horizon scanning, and ongoing monitoring activity to review and update previous assessments.

1.11. **Counter-intelligence.** Counter-intelligence focuses on the understanding of terrorism, espionage, sabotage, subversion and organised crime threats and vectors, and contests the operating space through proactive and reactive counter-intelligence activities. It entails collection of information, analysis and investigation of both state and non-state actors' intelligence methods, capabilities and activities. It also contributes to security by depriving adversaries of accurate or detailed knowledge of the disposition and capabilities of friendly forces, whether through intelligence collection activities or unauthorised disclosure.

1.12. **Security.** Security focuses on protecting the confidentiality, integrity and availability of personnel, information and assets. Security risk management advice will allow commanders to determine their appropriate prioritisation of resources to minimise, manage and mitigate potential threats to their operations, personnel, equipment and infrastructure.

Futures and horizon scanning

1.13. 'Futures', or futures studies, refers to different approaches to thinking about the future and exploring factors that could give rise to possible and probable future characteristics, events and behaviours. 'Foresight' refers to a process of conducting futures work and 'horizon scanning' is one specific technique, although the terms are sometimes used interchangeably. Horizon scanning is defined as: the systematic search across the global environment

for potential threats, hazards and opportunities.[7] In relation to the UK government, it is viewed as having a horizon beyond parliamentary terms; for military purposes, it may mean examining factors beyond the operational planning window. Futures work helps staff to:

- spot patterns of change, emerging trends, surprises and disruptors earlier, giving more time to respond;
- focus on the external context within which we create effect, taking account of the 'big picture';
- bring in alternative points of view and assist in challenge;
- create a narrative of the future, based on structured frameworks and evidence;
- explore multiple versions of the future – this mitigates the potential threat of single-outcome forecasting; and
- develop indicators and warnings on high-impact potential futures.

Intelligence as a joint function

1.14. Common to joint operations at all levels, intelligence is one of the eight defined joint functions.[8] The joint functions are a framework that provides commanders and their staff with the means to visualise the activities of the force and to ensure all aspects of the operation are addressed. Intelligence, as a joint function,[9] is one of the main drivers of the operations planning process and should be used in any operation, although its level of contribution and the level of demands may vary depending on the type of operation and complexity of the operating environment.

7 JDP 0-01.1, *UK Terminology Supplement to NATOTerm*.
8 The joint functions are: manoeuvre, fires, command and control, intelligence, information, sustainment, force protection and outreach. Note that 'outreach' is termed 'civil-military cooperation' within NATO.
9 Intelligence as one of the joint functions has a different meaning from the 'function of intelligence' described at Section 4.

Section 3 – UK national intelligence architecture

1.15. **Structure and accountability.** The Prime Minister has overall responsibility for intelligence and security matters and is accountable to Parliament for matters affecting the intelligence agencies and organisations collectively. For the agencies and organisations shown in Figure 1.1 (within the dotted line), the Secretary of State for Foreign, Commonwealth and Development Affairs (Foreign Secretary), Secretary of State for the Home Department (Home Secretary) and the Secretary of State for Defence (Defence Secretary) have delegated responsibilities. In their day-to-day operations, the principal intelligence and security agencies (the Secret Intelligence Service (SIS), the Government Communications Headquarters (GCHQ) and the Security Service) operate under the immediate control of their respective heads, each of whom has a statutory duty to report annually on their Service's performance to the Prime Minister and their Secretary of State.

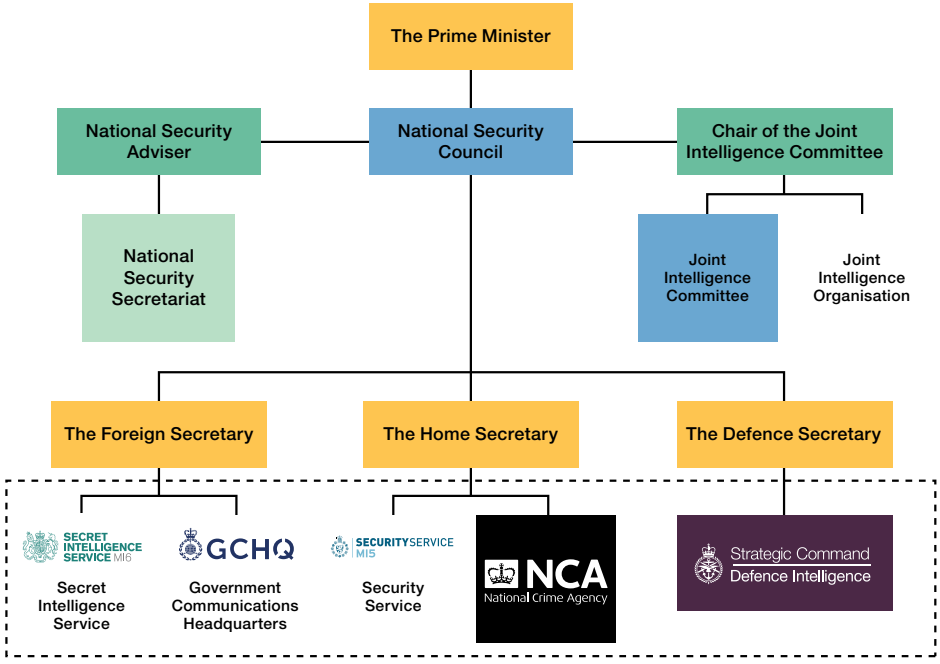


Figure 1.1 – National intelligence architecture

1.16. **Structure within Defence.** The Defence Secretary is ultimately responsible for Defence Intelligence. CDI reports to the Defence Secretary via Commander Strategic Command (Comd UKStratCom). Figure 1.1 shows only the major organisations; several other organisations contribute intelligence assessments on strategic issues including, for example, the Joint Terrorism Analysis Centre (JTAC) and National Cyber Security Centre (NCSC).

National structures

1.17. **National Security Adviser.** The National Security Adviser (NSA) is the central coordinator and adviser to the Prime Minister and Cabinet on security, intelligence, defence and some foreign policy matters. The NSA works in the Cabinet Office and works across departments to develop a coherent national security strategy.

1.18. **National Security Council.** Headed by the NSA, the National Security Council (NSC) is where ministers discuss national security issues at a strategic level. It is a Cabinet committee that coordinates policy decisions across departments, involving national security, foreign policy, defence, international relations and development, resilience, energy and resource security.

1.19. **National Security Secretariat.** The National Security Secretariat is also led by the NSA. It supports the NSC by coordinating cross-Whitehall preparations for weekly NSC meetings and implementing decisions.

1.20. **Joint Intelligence Committee.** The JIC provides all-source intelligence assessments on threats to the UK and UK interests overseas. It supports the Prime Minister, NSC and a wide range of policymakers across government.

1.21. **Joint Intelligence Organisation.** The Joint Intelligence Organisation (JIO) leads on intelligence assessment and the development of the UK intelligence community's analytical capability. The JIO incorporates the Cabinet Office Assessments Staff (COAS) and the Professional Head of Intelligence Analysis (PHIA).

National intelligence assessment in government

1.22. **Cabinet Office Assessments Staff.** The COAS consists of intelligence analysts seconded from a wide range of government departments and disciplines. It coheres the Current Intelligence Group (CIG), which brings together intelligence analysts, collectors, policymakers and other subject

matter experts. The CIG supports the COAS to draft consensus-based assessments of situations and issues of concern, providing warnings of threats to UK interests and identifying and monitoring countries at risk of instability.

1.23. **Cabinet Office – Professional Head of Intelligence Assessment.** The PHIA maintains oversight of the assessment of intelligence across government, implementing a professional standards framework and promoting best practice to improve the government's analytical capability. The PHIA heads up the cross-community intelligence assessment profession, comprising a wide range of government departments, organisations and joint task forces.

1.24. **Ministry of Defence – Defence Intelligence.** Defence Intelligence provides military-focused all-source intelligence assessment, geospatial intelligence and a range of other intelligence outputs for Defence and the wider UK government. It guides decisions on policy, strategy and the maintenance of operational commitments, informs Defence procurement decisions and supports military operations. Defence Intelligence also contributes to wider national assessment efforts, including the work of the JIC, at which it has a seat. It works closely with other intelligence organisations and provides support to other government departments. It works closely with Five Eyes nations, NATO, the European Union and other allies. Defence Intelligence is headed up by CDI and is accountable to Parliament via the Intelligence and Security Committee.

1.25. **Foreign, Commonwealth and Development Office Research Analysts.** Foreign, Commonwealth and Development Office (FCDO) Research Analysts are a specialist cadre of regional and thematic experts. They provide evidence-based research and analysis primarily to FCDO ministers and senior officials.

1.26. **Joint Terrorism Analysis Centre.** The JTAC analyses and assesses all intelligence relating to the international terrorist threat, at home and overseas. It sets threat levels and issues warnings of threats and other terrorist-related subjects.

1.27. **National Cyber Security Centre.** The NCSC provides cybersecurity support to the UK's most critical organisations, the wider public sector, industry, subject matter experts and the general public.

1.28. **Joint State Threats Assessment Team.** The Joint State Threats Assessment Team (JSTAT) is a cross-departmental assessment organisation that provides analysis on the hybrid state threats facing the UK and UK

interests. It assesses the national security threat posed by activities such as espionage, assassination, interference in the UK's democracy, and threats to the UK's economic security and the UK's people and assets overseas.

1.29. **National Crime Agency.** The National Crime Agency (NCA) seeks to protect the UK from the threat of serious and organised crime. NCA officers work with law enforcement to build an intelligence picture of all serious and organised crime threats and pursue the most serious and dangerous offenders.

1.30. **Home Office – Extremism Analysis Unit.** The Extremism Analysis Unit's (EAU's) remit is to analyse extremism in the UK and overseas where it has a direct impact on the UK or UK interests. The EAU is a cross-government resource.

National intelligence collection in government

1.31. **Secret Intelligence Service.** The SIS exists to protect the UK's people, economy and interests from overseas threats. It is commonly known as MI6.

1.32. **Government Communications Headquarters.** GCHQ is responsible under the Intelligence Services Act 1994 for the collection of signals intelligence to support the government's policymaking and operations in the fields of national security, military operations, law enforcement and economic well-being. GCHQ also undertakes information assurance to help protect government data (communication and information systems) from threats.

1.33. **Security Service.** More commonly known as MI5, the Security Service operates within UK territory and is responsible under the Security Service Act 1989 for the protection of national security. It is responsible for protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers, and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.

North Atlantic Treaty Organization intelligence organisation and responsibilities

1.34. **NATO intelligence architecture.** NATO has its own intelligence organisation led by the Assistant Secretary General for Intelligence and Security. The NATO intelligence architecture, its organisation and responsibilities are described in detail in AJP-2, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*.

The Ministry of Defence and the Foreign, Commonwealth and Development Office

Section 4 – The function of intelligence

1.35. The 'function of intelligence' (hereafter 'the function') was established in July 2020 as one of 16 functions in the Ministry of Defence (MOD).[10] They cover cross-cutting activities that need to be carried out in a coherent way across all the organisations in Defence, provide horizontal integration and enable MOD business to be done effectively, efficiently, legally and in compliance with wider government policy. This aligns Defence with the government-wide approach and replaces the Defence Authorities construct.

1.36. **Purpose.** The purpose of the function is to lead and cohere intelligence activities across Defence and it serves the interests of Defence's work to support national security. Under the 3* CDI as functional owner, the function provides leadership of Defence's intelligence enterprise. It delivers assured and trusted understanding for decision-makers, as well as effective and efficient employment of Defence's intelligence people, assets and capabilities. It supports the breadth of Defence's intelligence requirements, enabling MDI to support decision advantage.

10 Currently there are eight unique to Defence, the remaining eight are cross-government functions. This is separate from intelligence being one of the eight joint functions described in Section 2.

1.37. **Delivery.** The function is delivered by many elements of the MOD, including Defence Intelligence, Head Office and the front line commands, and encompasses people, processes and systems across the MOD engaged in intelligence activities. The function's authority does not extend outside of Defence.

1.38. **Priorities.** Six priority activities have been identified to strengthen intelligence delivery across Defence. These priority activities are:

- intelligence, surveillance and reconnaissance (ISR) management;
- capabilities;
- policies;
- people;
- training; and
- events and enterprise plans.

1.39. **Policy.** Across Defence there are several business areas and avenues through which intelligence-related policy is created, managed and assured. Defence benefits from the fact that CDI can mandate intelligence discipline policies across Defence, whilst MOD Head Office advises on the sensitive political and presentational aspects of intelligence operations. The main areas of responsibility are as follows.

a. **Ministry of Defence Head Office, Security Policy and Operations Specialist Intelligence Policy.** They are responsible for administering the ministerial rules for intelligence collection and for handling approvals for certain intelligence operational activity. Security Policy and Operations Specialist Intelligence Policy is also the supervisory authority for Defence intelligence activities that are conducted in accordance with the Regulation of Investigatory Powers Act (RIPA) across the MOD.

b. **Defence Intelligence, Joint User Intelligence and Cyber.** They are responsible for preparing and managing single intelligence policies for use across the MOD. Their remit applies to all intelligence disciplines.

c. **Defence Intelligence, Defence Intelligence Resources and Policy.** They are responsible for the management of policy relating to the Investigatory Powers Act in the MOD, including handling warrant

applications under the Act. Defence Intelligence Resources and Policy also issue policy relating to the use of bulk personal data.

d. **Defence Intelligence, Chief Information Officer.** Defence Intelligence's Chief Information Officer leads Defence Intelligence's information and data services to deliver the digital and data function across Defence Intelligence through innovation, data operations and information governance, assurance and management. The Chief Information Officer also champions information behavioural changes and digitisation across Defence Intelligence so that data and information is valued, owned, appropriately managed, quality improved and better exploited in a timely manner.

Section 5 – The single intelligence environment

1.40. The single intelligence environment (SIntE) is a collaborative environment in which coherence is intrinsic through continuous, multi-domain capability development and delivery between MOD Head Office, front line commands, partners across government and allies. The SIntE aims to harmonise all elements of the intelligence process to achieve the optimal use of intelligence specialists, agencies, sources, technology and activities to produce the best possible outcomes.

1.41. **Vision.** The SIntE vision is to enable leaders at all levels to conduct effective decision-making on the basis of comprehensive understanding derived from all sources of intelligence. The SIntE facilitates and enables actionable content and advice to inform UK Defence, the UK government and decision-making with allies. It allows success to be measured against Defence's ability to objectively produce accurate and timely assessments of possible events and their likelihoods, indicators and warnings, together with associated dissemination to decision-makers.

1.42. **Ownership and direction.** CDI, as the functional owner for intelligence across Defence, provides the strategic demand and the direction and guidance for the development, delivery and assurance of coherent intelligence capability. CDI is also responsible for: policy and standards; ensuring the coherence of Defence's intelligence activities across the single Services; and managing risk within the SIntE.

1.43. **Method of operating.** The SIntE is a collaborative endeavour with Defence linked to all the members of the UK intelligence community. The SIntE, when fully realised, supports an enterprise that anticipates and predicts, rather than responds to, events as they unfold. It will support the use of big data, artificial intelligence and cloud-based technologies that will dominate the future landscape. Cultures, behaviours and processes are also as fundamental to realising the benefits of the SIntE as the ability to keep pace with rapidly changing technological solutions. The SIntE's method of operating and principles are detailed in the *SIntE Sub-Strategy*.[11]

Section 6 – Factors affecting intelligence in the contemporary operating environment

1.44. **Operating in complexity.** Contemporary operations are likely to be complex with adversaries being potentially more difficult to identify. There are also likely to be a greater range of actors that will influence operations and multiple interested audiences. It is not sufficient just to know about actors and their capabilities, although identifying, neutralising, countering or defeating adversaries remains one of the primary areas of military focus. There is a need to understand the context within which actors operate, the institutions within which they live and detailed information about their cultures, fears, perceptions, motivations and history, as well as the human security context and related conflict drivers.

1.45. **Contextual understanding.** The complexity of modern operations produces a greater need for contextual understanding of the operating environment.[12] This relies on a wide range of sources and geospatial, cultural and linguistic capabilities for information collection and the subsequent analysis of that information to convert it 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. There is a requirement to pull in deep specialists from across Defence when required.

11 See also the *SIntE Sub-Strategy*; this document is produced by Joint User and classified at OFFICIAL-SENSITIVE.

12 Understanding the context as well as the intentions and capability of any potential adversary is reinforced in the MOD's *The Good Operation – A handbook for those involved in operational policy and its implementation*, page 21.

1.46. **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, within and outside Defence, including those living within the affected state. Non-UK experts, particularly those from an affected country, can provide a great deal of context and access to support intelligence analysis.

1.47. **The orchestration of intelligence.** The way that we orchestrate intelligence will increasingly need to be agile and dynamic. There are two approaches: conventional and adaptive. The conventional approach has fixed lines and boundaries between departments that include rules for inter-agency cooperation. The adaptive approach requires a more flexible and open system, where agencies work together to focus their efforts at a point of need; the requirement for common protocols between agencies remains, but these should be agile and based on the principle of collaboration – how can we work together rather than articulating the obstacles to working together.

1.48. **Intelligence and the levels of operations.** Traditional boundaries of the strategic, operational and tactical levels of operations have less relevance when related to intelligence. The point at which intelligence becomes strategic, operational or tactical is the point when a decision is made, or activity is undertaken at one of these levels. Tactical military commanders may require access to intelligence that originates at the strategic level and tactically derived intelligence may have strategic importance.

1.49. **Cultural capability.** Cultural capability is the ability to understand culture, including tangible and non-tangible artefacts, and to apply this knowledge to understand and engage effectively with the full range of actors in different environments. Cultural capability is critical to understanding and requires us to develop cultural expertise for the areas in which we operate or are likely to operate, together with a general awareness of other cultures and of how culture influences perceptions.

1.50. **Information security and protection.** Protecting and securing our intelligence and the information and data on which it is based is essential in ensuring the protection of individuals, organisations and intelligence sources. Adherence to security procedures is essential for ensuring continued access to intelligence derived from partners across government and international allies. Defence Intelligence is also responsible for establishing common Defence guidelines for collaboration with other government agencies to enable effective intelligence sharing.

1.51. **Deception and counter-deception.** The fundamental nature of deception may not have changed (i.e. hide the real and show the false), but the ways in which deception can be created and executed within the contemporary operating environment have changed. Deceptive stratagems can be used in three distinct roles: the offensive role (attack to defeat), the defensive role (protect the force – its people and its assets), and counter-deception (the detection of an adversary's use of deception). The intelligence function can support all these roles, with the detection of deception against friendly forces being a specific intelligence responsibility. Intelligence staff also have a significant role in advising the commander and their J3/5 staff on their response to countering deception against friendly forces.[13]

1.52. **Intelligence and gaining advantage through information.** Information is a critical enabler to mission command and a multi-domain approach. It enables understanding, decision-making, and command and control. The ever-increasing volume of information and data available represents one of the biggest challenges for producing intelligence and will continue to challenge available human analytical capacity. Technological developments to assist analysts within the intelligence cycle will therefore continue to increase in their significance. Equally, adapting analytical tradecraft techniques, processes and methodology is vital to ensure the volume of data collected is processed and analysed to its maximum potential.

1.53. **Digital and data developments.** The character of intelligence analysis and the vast availability of data in the contemporary operating environment is such that there will continue to be a significant dependency on information systems and supporting technology. Intelligence needs to be able to cope with big data (high velocity data, data of increasing variety, growing volume and of varying veracity) that is difficult for Defence to process, store and analyse using traditional analytical methods and information management architectures. Further developments in the fields of automation, artificial intelligence, machine learning and other data-related technologies will provide significant opportunities to enhance how intelligence business is conducted.

13 Further detail is in AJP-3.10.2, *Allied Joint Doctrine for Operations Security and Deception*.

Key points

- Understanding the audience is the major consideration of integrated action.
- An audience-centric approach places people at the heart of competition. Audience analysis segments audiences into three categories: public, stakeholders and actors. The position of individuals and groups within the range of audiences is not fixed, and therefore the requirement for audience analysis is enduring.
- Intelligence aims to contribute to a continuous and coordinated understanding of the operating environment, supporting commanders in decision-making by helping them to increase their understanding.
- The primary aims of intelligence are to enable understanding, produce predictive assessments, provide indicators and warnings, and to support strategy formulation.
- The 'function of intelligence' is one of 16 functions in the MOD. Its purpose is to lead and cohere intelligence activities across Defence.
- The SIntE aims to harmonise all elements of the intelligence process to achieve the optimal use of intelligence resources, technology and activities to produce the best possible outcomes.
- Meeting the challenge of big data will continue to require technological advances, incorporating automation, artificial intelligence, machine learning and the development of the digital ecosystem to support Defence's intelligence community.

Chapter 2

Intelligence enables commanders to understand their audiences and environment and then exploit that to their advantage. Chapter 2 considers a number of fundamental concepts that ensure commonality during Ministry of Defence intelligence activities.

2

> If you know the enemy and know yourself, you need not fear the result of a hundred battles.

Sun Tzu, *The Art of War*

Chapter 2

The fundamentals of intelligence

Section 1 – The principles of intelligence

2.1. Intelligence development at all levels is guided by several principles. These should govern the mindset, organisation and activities of those involved.

2.2. **Command or decision-maker led.** Setting the conditions for effective intelligence is a fundamental responsibility of command. If decision-makers are unable to sufficiently express their critical information and intelligence requirements, this can lead to a lack of understanding and degradation of decision advantage.

2.3. **Objectivity.** Intelligence should always be unbiased and it requires staff to be open-minded. Intelligence staff should not distort assessments to fit preconceived ideas or to provide answers that they think commanders or planners want.

2.4. **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.

2.5. **Agility.** Intelligence staff should continuously adapt their activities to the changing environment and the requirements of their commanders. This particularly implies mental and organisational agility. Agility is further supported by resilience, adaptation and flexibility.

a. **Resilience.** Not all activity will immediately be successful. It is essential to be persistent, adapt quickly and exploit opportunities when they arise.

b. **Adaptation.** Learning and adaptation can only occur through a comprehensive review of results. This enables us to reduce negative unintended consequences, exploit positive unintended consequences and pursue those outcomes originally intended.

c. **Flexibility.** Flexibility allows the redirection of effort to meet changing circumstances. It also shuns the notion that there is only one way of working.

2.6. **Timeliness.** Intelligence should be delivered in time. It is better to provide 80% of the intelligence in time, with appropriate caveats on confidence levels, than 100% of the intelligence too late.

2.7. **Collaboration.** Sharing individual understanding to achieve greater collective and common understanding is a powerful tool in joint and coalition operations.[14] The 'need to know' principle may endure to maintain security, but a collaborative environment relies on a 'duty to share' culture across and possibly outside government, underpinned by pragmatic risk management.

2.8. **Continuity.** Experience is gained slowly but can be lost quickly. Some skills are enduring and transferable, particularly in ongoing operations. Maintaining access to subject matter experts is one way to achieve continuity of understanding.

2.9. **Security.** Security permeates the entire intelligence enterprise. Security risks are mitigated by technical measures, enforcing rules and procedures, discipline (including self-discipline) and effective counter-intelligence operations.

2.10. **Additional NATO principles.** The principles of intelligence detailed in the North Atlantic Treaty Organization's (NATO's) Allied Joint Publication (AJP)-2, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security* are broadly similar to the UK principles. However, NATO has the following additions.

a. **Interoperability.** Common or interoperable processes, networks and systems are required to support intelligence direction, collection, processing and dissemination. They are also required to manage the intelligence organisation.

b. **Sharing/collaboration.** Intelligence has the capability to draw on the skills of a wide spectrum of experts and specialists in a variety of organisations, across all commands and at all levels of operations. It should be noted that any sharing of intelligence with foreign authorities must comply with the UK government's policy *The Principles* to ensure compliance with UK domestic and international law and guard against shared intelligence contributing to unacceptable conduct.

14 Individual understanding may be described as our own personal interpretation of the facts; see Joint Doctrine Publication (JDP) 04, *Understanding and Decision-making*.

c. **Accessibility.** Relevant information and intelligence must be processed by intelligence staff and be readily available to intelligence users. Intelligence is of no value if it is not disseminated or accessible to those who require it.

d. **Anticipation.** Intelligence is as much about warning and forecasting possible future developments for decision-makers as it is about delivering for current circumstances.

Section 2 – Guidelines

2.11. The challenges of complex operations force intelligence staff to adapt in the ways they plan and operate. The following guidelines should be considered when designing and implementing intelligence structures to support operations.

a. **Commanders and their intelligence staff.** The trust between commanders and their intelligence staff must be strong and immediate. Commanders must drive their critical information requirements and enable the intelligence staff to work them through independently.

b. **Common aim.** Intelligence production is not an end in itself. The staff must maintain sight of the commander's end requirements.

c. **Synchronisation with planning and operation cycles.** The intelligence process must support the operational and planning cycles. Intelligence is only of value if it supports operational outcomes.

d. **A comprehensive view of the dynamics of situations is required.** Intelligence assessments should include the physical, cognitive and virtual dimensions of the information environment and should consider all actors and threats within the wider area of interest.

e. **Data centricity.** The key to a data-centric approach to intelligence is access to data to truly understand intelligence gaps whilst reducing the burden on finite resources (both analytical and intelligence, surveillance and reconnaissance (ISR) assets) and fully supporting decision-making in a timely manner. A data-centric approach must be supported by the appropriate architecture, security and information policies and the correct skill sets.

f. **Fusion at the point of need.** An all- or multiple-source approach to intelligence development (considering every available relevant source/data/information) uses the concept of intelligence fusion to optimise the value of various sources of information. Fusion is the blending of information and data from multiple sources or agencies into a coherent picture. Intelligence consisting of all relevant and available data, information, ISR results and other assessments provides higher accuracy and confidence levels. Source referencing in multiple-source approaches further enhances confidence and auditability.

g. **Precision and accuracy.** Adversaries are as likely to be low-contrast or low-resolution as they are to be clearly defined and categorised. Precision and accuracy in analysis and assessments is therefore essential.

h. **Intelligence sharing.** Intelligence should be shared horizontally as well as vertically within a command structure. The key to effective data and intelligence sharing is an information environment where intelligence can be accessed.

Precision and accuracy: extensive surveillance established Daesh's use of former Iraqi presidential palaces as headquarters and training centres

Section 3 – The levels of intelligence

2.12. As stated in Chapter 1, traditional boundaries of the strategic, operational and tactical levels of operations have less relevance when related to intelligence, but they can still provide a helpful indicator of its function.[15] Strategic, operational and tactical intelligence are formally defined in Allied joint doctrine, with the definitions for the levels of intelligence as follows.

a. **Strategic intelligence.** Strategic intelligence is defined as: intelligence required for the formation of policy, military planning and the provision of indications and warnings at the national and/or international levels.[16] This is typically gathered in response to government requirements, focusing on national threats, supra-national issues and conflict drivers. The nature of strategic intelligence means that a wide variety of intelligence sources and assets outside national capabilities are used.

b. **Operational intelligence.** Operational intelligence is defined as: intelligence required for the planning and conduct of campaigns at the operational level.[17] The primary users of this type of intelligence 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.[18] Tactical intelligence normally supports specific activities by tactical-level commanders or units. In most cases, intelligence assets providing tactical intelligence belong to the tactical headquarters involved.[19]

2.13. **Non-military views of the strategic, operational and tactical.** Commanders and intelligence staff must consider that non-military organisations may have different definitions for strategic, operational and tactical levels. This is especially true when working with civilian organisations and law enforcement agencies.

15 See JDP 0-01, *UK Defence Doctrine*, 6th Edition, paragraph 3.8 for additional detail on the levels of operations.
16 NATOTerm.
17 NATOTerm.
18 NATOTerm.
19 For example, UK intelligence collection units assigned to support UK forces within the UK area of operations.

Section 4 – Categories of intelligence assessment

2.14. Intelligence assessments reflect their intended use and include periodic intelligence summaries, specific intelligence reports and threat assessments. The naming conventions are broad but there are three categories of intelligence assessment.

a. **Basic intelligence.** Basic intelligence is defined as: intelligence derived from any source, that may be used as reference material for planning and as a basis for processing subsequent information or intelligence.[20] Basic intelligence includes details of orders of battle, equipment capabilities, personalities, infrastructure, socio-political, economic, cultural and human security, and environmental aspects. Some UK intelligence agencies use the term 'building-block intelligence' when referring to basic intelligence. Basic intelligence provides the context and backdrop against which current intelligence is reviewed.

b. **Current intelligence.** Current intelligence is defined as: intelligence that reflects the current situation at strategic, operational and/or tactical levels.[21] It can offer greater granularity than basic intelligence, but generally reflects a moment in time and it is perishable.

c. **Applied intelligence.** This may be described as intelligence that is tailored to provide direct support to the decision-making process. It involves analysis of basic and current intelligence to meet specific and normally predictive intelligence requirements with a particular focus on future situations to enable timely planning and/or provide a warning. It includes: an adversary's probable courses of action; how to influence audiences; specific reports on adversary capabilities which may influence the conduct of operations; and actions by other agencies.

20 NATOTerm. Basic intelligence is fused from all available data, information, joint ISR results, single-source intelligence and all-source intelligence and it is fundamental to current intelligence.
21 NATOTerm.

Section 5 – The limitations of intelligence

2.15. Intelligence production has limitations. This list is not exhaustive, but some of the limitations are outlined below. Additionally, it is essential to ensure that intelligence, counter-intelligence and security activities are conducted in accordance with the applicable law. Intelligence planners must know what is legally permissible when formulating intelligence planning to develop intelligence architectures and ensure that appropriate limitations are placed on permitted activity to ensure compliance. See Chapter 4 for further detail on legal considerations.

2.16. **Human judgement.** Human beings have limits making exacting analytical judgements in complex and rapidly changing environments. This impacts not only assessment but also decisions made because of them. Intelligence may also not meet the commander's requirements exactly or be entirely accurate, complete or easily corroborated, but the commander will have to make judgements and decisions based on it.

2.17. **Audience intentions.** It has always been exceptionally difficult to determine an adversary's intentions. In the contemporary and future operating environments, where the size of an adversary'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 an adversaries' and other audiences' capabilities and intentions.

2.18. **Uncertainty.** Decision-makers and practitioners should accept that intelligence must be bounded with degrees of probability and confidence due to levels of uncertainty associated with assessments. Confidence expresses an analyst's judgement about the robustness of their assessment, whereas probability is an assessment of the likelihood of certain events occurring. No future course of events can be known in advance, meaning that predictive judgements can only be expressed as probabilities. At the same time, the problems of incompleteness and potential deception mean that there are always limitations to the confidence of analytic judgements. Intelligence staff must state where there are knowledge gaps to enable a commander to place appropriate weight on the assessment.[22]

22 For more information on uncertainty, see Defence Intelligence, *Quick Wins for Busy Analysts*.

2.19. **Extent of available capability.** All collection, exploitation and processing assets have limitations. These limitations may arise from availability, volume and the ability/capacity to process, exploit or disseminate in a timely manner. Intelligence staff must closely engage with the ISR staff for a realistic appraisal of collection, exploitation and processing capability. Information obtained rarely provides a complete picture and any sources of information must be liable to doubt and additional scrutiny.

2.20. **Relevance/obsolescence.** All intelligence is time-bound and subject to expiry. Constant evaluation and updating of the existing current intelligence, as well as the production of new intelligence, will preserve the relevance of information given to commanders and their staff. The continuous updating of basic intelligence is also necessary.

2.21. **Source protection.** Source protection is critical where sensitive or covert collection capabilities are involved. However, source protection should not become a reason for withholding intelligence from those who need to know. The compromise of a source could result in the information no longer being available, the source being used to pass deceptive information or the source being physically harmed or removed. Often, authority for release for information derived from sensitive or covert collection capabilities will be controlled through higher authorities, including potentially at the national level.

2.22. **Management of expectations.** Even when exploited fully, intelligence will not produce complete certainty. Intelligence staff must be realistic about what intelligence activity can achieve and they must manage the commander's expectations while doing all they can to optimise available resources.

Key points

- The UK principles that underpin intelligence are: command or decision-maker led, objectivity, perspective, agility, timeliness, collaboration, continuity and security. NATO's additional principles are: interoperability, sharing/collaboration, accessibility and anticipation.
- The levels of intelligence are strategic, operational and tactical.
- There are three categories of intelligence assessment: basic, current and applied.
- The principal limitations of intelligence are: human judgement; determining audience intentions; uncertainty; collection, exploitation and processing limitations; relevance/obsolescence of information; source protection; and the management of expectations.

Chapter 3

The purpose of Chapter 3 is to explain how intelligence is developed and to provide detail on the core intelligence functions. These functions are referred to as the 'intelligence cycle'. This publication places particular emphasis on the processing and analysis undertaken within the intelligence cycle.

> A good intelligence assessment has explanatory value in helping deepen real understanding of how a situation has arisen, the dynamics between the parties and what the motivations of the actors involved are likely to be.

Sir David Omand, *Securing the State*

Chapter 3

The core functions and the intelligence cycle

Section 1 – The intelligence core functions

3.1. The intelligence process is the collection, processing and analysis of information to answer specific questions and contribute to wider understanding. It 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 a systematic approach, but it demands that we approach the development of intelligence differently – imagination and a spirit of collaboration are critical.

3.2. **The intelligence cycle.** There are four overarching core functions in the intelligence cycle: direction, collection, processing and dissemination (DCPD). Information must be acquired from all sources available, it must be properly understood and its significance for decision-making assessed. All of this must be conducted based on clear and methodical requirements for information and the subsequent assessments must be conveyed to those who need them to support their decision-making. All these activities take place concurrently and interact with one another, overlap and coincide but, ultimately, they are intended to meet information requirements provided by direction. As a result, they are often seen as an intelligence 'cycle', with requirements from decision-makers giving direction to collection, analysis and processing with the final product being disseminated to decision-makers to meet those requirements. The intelligence cycle is visualised at Figure 3.1.

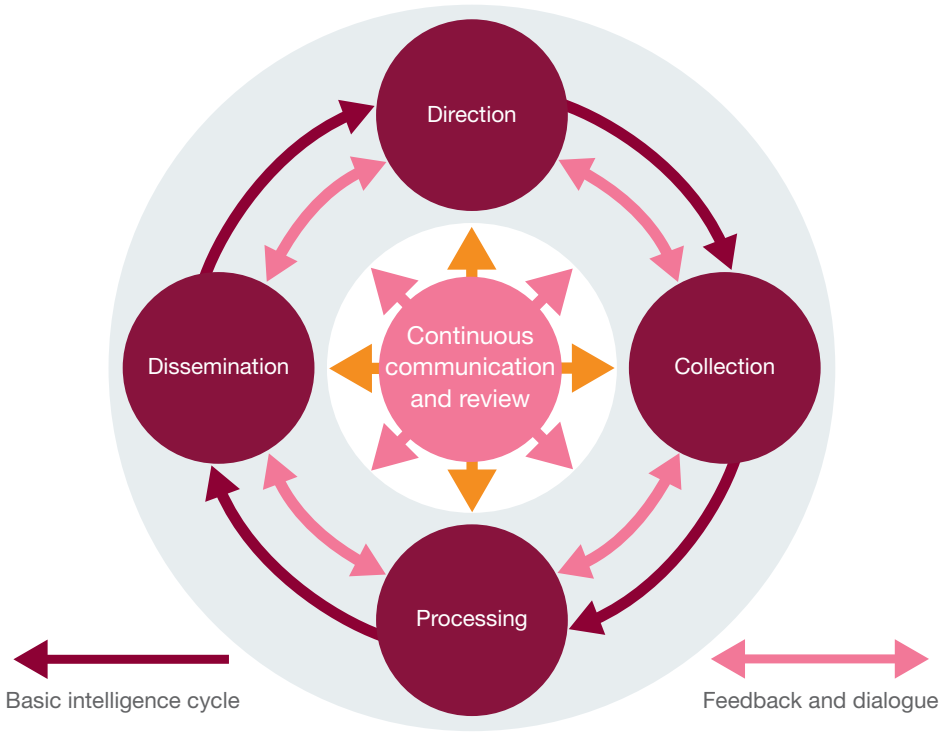


Figure 3.1 – The intelligence core functions and the intelligence cycle[23]

3.3. **Variations in approach.** The core functions provide an approach for how to undertake intelligence activity and should be seen as principles that will be applied in different forms in different areas of intelligence activity. The UK and the North Atlantic Treaty Organization (NATO) explain these core functions with a four-step model, as described in this chapter, although for clarity in this publication, the processing step has been subdivided into processing and analysis. The United States uses a five-step model, with analysis as a separate function from the UK/NATO processing core function. Additionally, the intelligence, surveillance and reconnaissance (ISR) community work from a five-step model, referred to as task, collect, process, exploit and disseminate (TCPED); ISR TCPED can operate as part of, in addition to, or independently from the intelligence cycle depending on the situation, and is described in greater detail in Chapter 4. The variations on the core approach do not present a problem, merely a different emphasis in describing the same activities.

23 This diagram is based on an interpretation of the intelligence cycle by Professor Philip Davies from Brunel University.

Section 2 – Direction

3.4. Direction within the intelligence cycle is defined as: the determination of intelligence requirements, planning of collection effort, issuance of orders and requests to agencies and continuous monitoring of the productivity of such agencies.[24] Direction is concerned with identifying information requirements, assigning priorities to those requirements, and allocating collection capabilities, systems and assets[25] to meet those requirements.

3.5. **Principal components.** In accordance with the commander's direction, the intelligence staff must ensure that intelligence requirements are factored into operations and planning staff activities. The collection process is then directed by the ISR staff to meet the commander's requirements. This involves the following activities.

a. At the outset of the operations planning process, the commander and their staff will begin to formulate questions. More questions will be posed and existing questions amended as planning evolves, intelligence is received and the subsequent operation develops. These questions, many of which fall outside the remit of the intelligence staff, are the commander's critical information requirements (CCIRs).

b. Ensuring intelligence requirements are captured, processed and actioned by the ISR staff for collection and process, exploit and disseminate activity.

c. Monitoring intelligence activity to ensure that the right information is being collected, analysed and disseminated.

d. Ensuring that intelligence activities are conducted in a timely manner and where delays are occurring, re-tasking or reprioritising as required.

e. Planning the production, in combination with intelligence requirements management and collection management (IRM&CM).

24 NATOTerm.
25 Allocation of collection capabilities, systems and assets will be undertaken by ISR staff, and integrated with operations and plans outputs.

Intelligence and information requirements

3.6. Intelligence and information requirements and priorities are captured and communicated in differing ways in different organisations and at levels of command. These can be expressed in a number of formats, as described below.

3.7. **Information requirements.** An information requirement is defined as: in intelligence usage, information regarding an adversary or potentially hostile actors and other relevant aspects of the operational environment that needs to be collected and processed to meet the intelligence requirements of a commander.[26] Information requirements consist of the following.

a. **Specific information requirements.** A specific information requirement is a refined and more specific requirement, which forms a component part of a larger intelligence problem. For example, an originating information requirement of 'where will the enemy attack from?', could in a specific information requirement be 'what capability does the enemy have to cross the river on the eastern flank?'.

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

3.8. **Intelligence requirements.** The portion of the CCIRs that intelligence staff will seek to answer are referred to as intelligence requirements. An intelligence requirement is defined as: a statement that provides the rationale and priority for intelligence activity, as well as the detail to allow the intelligence staff to satisfy the requirement in the most effective manner.[27] Intelligence requirements articulate gaps in knowledge that must be filled or levels of understanding that must be maintained so that a commander can conduct planning. Intelligence requirements may be further categorised as follows.

a. **Priority intelligence requirements.** A priority intelligence requirement (PIR) is defined as: an intelligence requirement for which

26 NATOTerm.
27 NATOTerm.

the commander has an anticipated and stated priority in their task of planning and decision-making.[28] PIRs are a vital part of the CCIR development process and are usually formulated by the intelligence staff in close consultation with the commander, and the operations and planning staff. PIRs encompass those intelligence requirements for which the commander has an anticipated and stated priority for enabling planning and decision-making.[29] They should be limited in number and provide a comprehensive grouping of the main issues. They may be enduring or limited to a particular temporal phase or situation. PIRs should reference the original question and be written specifically to support the commander's decisions, intent and to focus on gaps in understanding. Due to the importance of this intelligence to the commander's decision-making, these questions are designated PIRs. PIRs are managed locally, but also shared up and down the chain of command, and laterally. The commander should prioritise PIRs and keep them under continual review.

b. **Specific intelligence requirements.** PIRs are supported by more detailed specific intelligence requirements (SIRs). An SIR is defined as: an intelligence requirement that supports and complements each priority intelligence requirement and provides a more detailed description of the requirement.[30]

3.9. **Expressing intelligence requirements.** Intelligence requirements should be expressed in a clear and concise form. Intelligence requirements should be formatted to be: specific, measurable, realistic and timely.

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.

b. **Measurable.** It must be possible to determine when a sufficient level of confidence in assessment is achieved to consider when an intelligence requirement has been filled.

28 NATOTerm.
29 For more information see Allied Joint Publication (AJP)-2.1, *Allied Joint Doctrine for Intelligence Procedures*, paragraph 3.6.
30 NATOTerm.

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.

3.10. **Requests for information.** Where a unit cannot answer an intelligence question from within their own data, information and intelligence accesses, a request for information (RFI) can be sent to a higher, adjacent or subordinate unit, formation or headquarters to ask if they hold relevant information which can assist. A formalised RFI management process manages the flow of RFIs and responses. On receipt, an RFI manager will check holdings against the question and provide an answer back to the RFI originator, including nil responses. Where existing information and data is not held, the receiver can assign this as an intelligence requirement, which will then go through the intelligence requirements management (IRM) process at that level.[31] The receiving organisation will treat the informing RFI as an intelligence requirement (and usually a one-off requirement unless it is a standing task), the only difference being that the intelligence requirement is being undertaken on behalf of another organisation. This may include onward passage from IRM to collection management and generate collection activity where it falls within the recipient's priorities and capacity. Intelligence requirements passed between coalition partners are passed as RFIs. A single intelligence requirement may generate a number of separate RFIs for different providers. RFIs are not a mechanism for directly requesting collection and should not be used as such. It should be noted that the term RFI is also widely used outside the intelligence specialisation.

Intelligence requirements management and collection management

3.11. The definition of IRM&CM is: a set of integrated processes and services to manage and satisfy the intelligence requirements by making best use of the available collection, processing, exploitation and dissemination capabilities.[32] IRM&CM is often seen as the point of contact between direction and collection phases of the intelligence cycle, but it is an ongoing activity throughout

31 Where possible, intelligence architectures should be as transparent as possible, which ensures relevant data, information and intelligence can be discovered at every level. This greatly reduces the volume of RFIs required.
32 NATOTerm.

the cycle. 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, IRM is the main internal activity and provides the linkage to collection management, which sits outside of the intelligence cycle and within the ISR process.[33] IRM&CM provides a central focus for the management of all intelligence and operational requirements for ISR. It harnesses the collection and processing capabilities by translating cognitive intelligence tasks into physical collection tasks where a collector can be applied against a problem located in time, space and on the electromagnetic spectrum. The roles of IRM&CM are to:

- synchronise intelligence collection and processing, exploitation and dissemination efforts;[34]
- ensure maximum advantage is made of collection and processing, exploitation and dissemination capabilities;
- coordinate the tasking, processing, exploitation, analysis and dissemination of intelligence, including accesses to it, using the underlying tenets of 'duty to share' and 'collect once and use often';
- integrate intelligence into planning procedures across Defence; and
- manage collaboration with partners at all levels.

3.12. **Intelligence requirements management.** IRM is defined as: the management function that develops, validates and prioritizes intelligence requirements, forwards validated intelligence requirements to the collection management function, and oversees dissemination of the intelligence products.[35] The IRM staff have the following responsibilities.

a. Assess an intelligence requirement's relative priority, based on the commander's intent, direction and the PIRs.

33 IRM&CM is practised at every level and provides the mechanism for seeking intelligence and collection from higher, lateral and subordinates formations. While best practice dictates a separation of the function between J2 and ISR staff at the tactical level where there are few organic collection capabilities, the functions may be compressed into one cell.
34 In this sense, intelligence collection refers to how the intelligence staff source finished intelligence on which they can base their assessments. Intelligence is not collected; data and information are collected and it only becomes intelligence when it has been processed, exploited and disseminated.
35 NATOTerm.

b. Search existing databases and publications to negate unnecessary collection or processing activity if an answer to the intelligence requirement already exists. This includes submission of RFIs to higher, lateral and subordinate levels who may hold data, information and intelligence.

c. Determine if the intelligence requirements constitute a valid gap and require tasking of collection capabilities.

d. Convert cognitive intelligence requirements into EEI that can be answered by collection. IRMs state EEI in terms of an effect required. IRMs should not request specific assets, platforms or sensors. To help coordinate and monitor intelligence requirements, the 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 requirements manager will consult the demander to ask if a later delivery is acceptable or if the task should be cancelled, thereby 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 requirements 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 for subsequent intelligence requirements and made available to as wide an audience as possible.

3.13. **Collection management.** Collection management is defined as: in intelligence usage, the process of satisfying collection requirements by tasking, requesting or coordinating with appropriate collection sources of agencies, monitoring results and re-tasking, as required.[36] Collection management operates independently from the IRM process with collection management directly supporting both the intelligence cycle and operations cycle. It is often required to balance competing requirements between the two. Collection management optimises the deployment and tasking of finite collection resources to meet demands from all users and requesters. It matches EEIs to the most appropriate available collector, accounting for the type of outcome required.

36 NATOTerm.

The Royal Marine Surveillance and Reconnaissance Squadron exercise deploying from a Royal Navy submarine in Northern Norway

3.14. **Intelligence collection plan.** Operations place an enormous demand on collection, processing, exploitation and dissemination capabilities. Information is required to support situational awareness, force protection, target acquisition and battle damage 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.[37] It articulates the priorities and constraints for each intelligence requirement. In the intelligence collection plan, the IRM staff deconstruct intelligence requirements into their constituent priority or enduring intelligence requirements and EEIs.

3.15. **Review of the intelligence collection plan.** IRM staff should continuously review the intelligence collection plan, monitoring the productivity of sources and agencies. It should be distributed to higher, lower and lateral levels of command, including multinational partners, to inform them and facilitate coordination.

37 Although 'intelligence collection plan' is the commonly used term, 'intelligence requirements plan' more accurately reflects what the intelligence collection plan is – essentially a cognitive analytical tool for breaking down complex intelligence problems into more manageable components.

Indicators and warnings

> Military men look for three surefire clues that an enemy force is preparing to attack. Is it moving its artillery forward? Is it laying down communications? Is it reinforcing its forces logistically, with stocks for fuel and ammunition? By 31 July [1990] all three conditions were present in southern Iraq.
>
> Colin Powell, *A Soldier's Way, An Autobiography*

3.16. **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. Selecting indicators that are 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. Indicators are normally categorised under three headings.[38]

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 resupply or redeployment of adversary capabilities.

b. **Tactical or combat indicators.** These 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 PIRs. For example, tactical indicators could include the increasing number of naval ships in port or weapons purchases by insurgents.

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.

3.17. **Strategic warning problems.** Defence Intelligence maintains a set of strategic 'warning problems' as part of its indicators and warnings enterprise.

38 Indicators and warnings is defined as: intelligence activities to detect and report time-sensitive information on developments that could threaten the multinational force, including forewarning of adversaries' intentions or actions, insurgency, terrorism and other similar events. Joint Doctrine Publication (JDP) 0-01.1, *UK Terminology Supplement to NATOTerm*.

Using formal methodology, these monitor critical indicators for scenarios that would have negative implications for Defence and the wider UK government. Defence Intelligence publishes 'warning reports' when there are changes to critical indicators, or in response to customer requests. The purpose of establishing a 'warning problem' is to focus attention, collection and analysis on a specific threat and to monitor it closely for a potentially indefinite period. Warning problems use indicator-based methodology to provide a framework for detecting changes or anomalies in activity that would raise or lower the level of concern. This level of concern is expressed as a 'watch condition'. Warning problems are deactivated upon the threat having completely subsided or the warning issue coming to pass.

Section 3 – Collection

3.18. Collection may be described as the gathering and exploitation of data and information by specialists and agencies and the delivery of the results obtained to the appropriate processing unit for use in the production of intelligence.[39] It comprises search, retrieval and receipt of data, information and intelligence from external sources. Collection within the intelligence cycle does not refer to the application of sensors and collection capabilities against requirements; this falls within the ISR TCPED process. Collection refers to the harvesting of the results and outputs from the ISR process and other sources for use by intelligence staff and analysts.

3.19. **Sources.** A source is defined in NATO as: in intelligence usage, a person from whom or thing from which information can be obtained.[40] The UK has a broader interpretation of the term 'source', which includes processes and systems. There are three types of sources: controlled, uncontrolled and casual.

a. **Controlled.** Controlled sources are people, processes and systems that are under direct control of an intelligence agency or organisation, specifically nominated intelligence staff, or under the control of an organisation, headquarters or headquarters hierarchy in which the intelligence staff reside.

b. **Uncontrolled.** Uncontrolled sources are those not under formal command and control of a suitably empowered headquarters. The term largely refers to external third party sources such as the media

39 This is also a proposed definition awaiting agreement by NATO.
40 NATOTerm.

and other nations' intelligence apparatus. Information provided by uncontrolled sources is treated with caution as it may be intended to deceive or influence.

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.[41]

3.20. **Agencies.** An agency is defined as: in intelligence usage, an organization or individual engaged in collecting and/or processing information.[42] An agency is different from a source because a source produces raw data while an agency, which has a collection capability, also possesses some degree of processing capability and can provide intelligence. Agencies can be national (for example, Secret Intelligence Service) or multinational (for example, NATO).

3.21. **Agency and source selection.** Selection of a source or agency for a particular task is the responsibility of the collection management staff. The collection management staff will need to consider the following.

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 in either the loss of the source or its compromise.

b. **Capability.** An agency tasked to collect an item of information or produce data, information or 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. The collection management staff will 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 employing a particular source or agency. The risk involved must be weighed against the value of the information sought.

41 These personnel receive special training in the legal implications of their actions.
42 NATOTerm.

e. **Engagement space.** External factors within the engagement space may limit the ability of a source or agency to collect information. Such factors include, for example, political constraints, weather or terrain.

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.** The commander's deadline is critical. Collection management staff must ensure that sources and agencies selected to meet a collection requirement will be able to achieve the task before the deadline.

Relationship between the intelligence cycle and intelligence, surveillance and reconnaissance

3.22. The ISR process is synchronised with the intelligence and operations cycles. Although the ISR process is frequently aligned with the collection and processing phases of the intelligence cycle, it is not exclusively aligned, especially where ISR assets are supporting operations directly and in real time. Figure 3.2 illustrates the alignment of the ISR process and the intelligence and decision cycles.

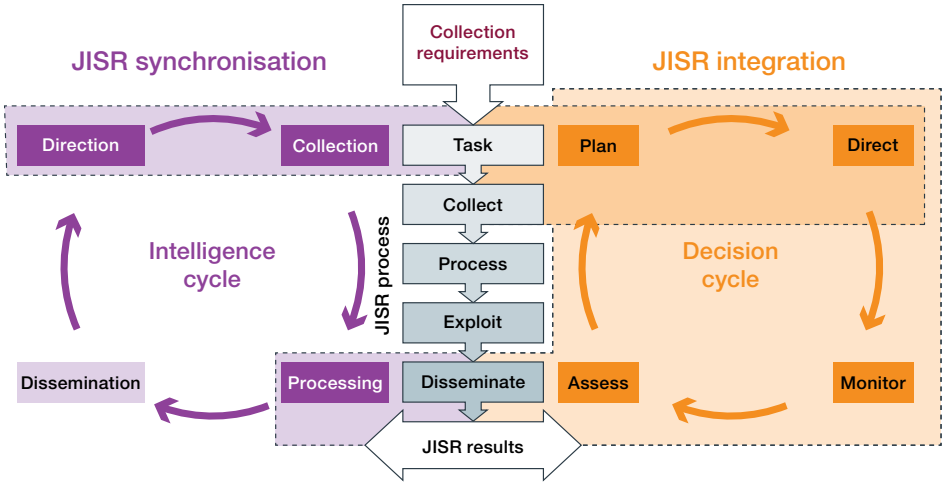


Figure 3.2 – Intelligence, surveillance and reconnaissance synchronisation and integration[43]

43 AJP-2.7, *Allied Joint Doctrine for Intelligence, Surveillance and Reconnaissance*, Figure 1.2.

3.23. **Selection of collection assets – tasking.** Resource tasking is described as the activity undertaken to select the most appropriate ISR resource types for which tasking authority has been allocated. This process occurs outside of the intelligence cycle as part of collection management in the ISR cycle. Collection managers select assets according to suitability and availability rather than ownership. For tasks involving complex targets, multiple collection capabilities may be necessary to satisfy a single collection requirement. Collection managers will collaborate closely with resource owners to identify the most appropriate assets to meet the collection requirement. In some instances, it may be preferable to modify the constraints of the collection requirement to match an available asset rather than pass an unachievable collection requirement to another organisation. In addition to knowledge of dedicated ISR assets and non-dedicated ISR assets organic to their organisation, collection managers should have a thorough understanding of assets within other operational domains and components, higher, national or allied organisations, and the process to task them.

3.24. **The intelligence, surveillance and reconnaissance collection requirements list.** The collection requirements list (CRL) is generated by the collection management staff and integrates requirements from both the operations staff and the intelligence staff. It aims to match requirements with specific collection assets and directly supports the intelligence collection plan and the operational and targeting requirements. Having determined which assets best suit the task, collection management staff allocate the appropriate resources on a priority basis.

3.25. **Allocation of collection assets.** Coordination is required to prioritise competing demands on the same collection capability. Coordination also ensures coherence between the collection and alternative functions of dual-role or multi-role assets.

3.26. **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.

Carrier Strike Group 21 operations required shared understanding between allies

Multiple-source intelligence and multidisciplinary intelligence

3.27. A source is a line of reporting such as a human agent or intercepted communications channel. A discipline represents a method or technique of collection (for example, human intelligence or signals intelligence). One may have multiple sources from a single discipline, such as more than one agent or a number of decrypted ciphers. Therefore, multidisciplinary intelligence fuses information drawn from more than one source or from across two or more collection disciplines. Multiple-source intelligence is defined as: the deliberate application of two or more discrete but supporting intelligence disciplines, seeking to improve the quality of the intelligence product.[44] Note: supporting intelligence disciplines include, for example, geospatial intelligence, human intelligence and signals intelligence.

3.28. **Corroboration.** 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.

44 This is a modified definition and will be updated in JDP 0-01.1, *UK Terminology Supplement to NATOTerm*.

3.29. **Fusion.** Multiple-source intelligence will often have a higher degree of confidence than single-source intelligence, but deception staff now recognise this and will plan multiple-source deception. To gain additional benefit, intelligence staff should fuse material, blending intelligence and information from multiple feeds, including open sources, into a coherent picture. 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.

Section 4 – Processing

> True genius resides in the capacity for the evaluation of uncertain, hazardous, and conflicting information.
>
> Sir Winston Churchill

3.30. **Processing and analysis.** Processing is defined as: the conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation.[45] Processing is the function of the intelligence cycle in which collected information and data is converted into intelligence to meet intelligence requirements. For clarity in this doctrine, it has been subdivided into processing and analysis, with the processing steps describing how information is made usable for the analyst and the analysis steps covering how the analyst then makes this valuable for the customer. Both steps must occur to achieve the overall aim. Processing and analysis are iterative and may generate further collection requirements before the intelligence is disseminated.

3.31. **Doctrinal approaches.** As outlined above, there are variations in how the core functions of the intelligence cycle are expressed, particularly around processing. NATO describes processing as the conversion of information into intelligence through collation, evaluation, analysis, integration and interpretation. Along with some nations, this approach means processing and analysis are treated as a single topic under 'processing', while other nations treat them separately. This publication is consistent with the NATO view of a single overarching function, while emphasising different steps in how to

45 NATOTerm.

achieve it. Analysts should be conscious of the differences in terminology when collaborating with colleagues in other organisations.

3.32. **Uncertainty.** One of the defining characteristics of intelligence analysis as a whole is the need to deal with uncertainty. Uncertainty is present at every stage of the intelligence cycle, but it is most prevalent in processing and analysis. Uncertainty may arise from:

- incomplete, ambiguous, conflicting or potentially incorrect information;
- the presence of subjectivity or bias in the source material;
- the presence of subjectivity or bias in how information is treated by analysts and customers;
- the extent to which the information is knowable; and
- the potential for denial and deception.

The impact of uncertainty is exacerbated when dealing with future-focused requirements as these examine events that have yet to occur and may therefore still change. Futures analysis can enable more timely, effective and comprehensive preparation for a variety of futures, including high-impact events, and it is therefore extremely valuable for decision-makers. However, it requires particular care because of the greater reliance on assumptions to fill gaps, making it more susceptible to subjective thinking and cognitive bias. In all cases, it is important for analysts to understand and address sources of uncertainty so that their analysis is as rigorous as possible and decision-makers receive the best quality intelligence for their requirement. This can be assisted by drawing on a wide range of sources and collection disciplines, consciously thinking both creatively and critically, and being open to constructive challenge.

3.33. **Structured analytical techniques.** Structured analytical techniques (SATs)[46] are methods of organising and stimulating thinking about intelligence problems and they can be useful tools for understanding and addressing uncertainty. Their use has been increasingly championed since prominent intelligence failures and the subsequent investigations, such as the Butler and

46 'Structured analytical techniques' as a term is not formally defined but it is commonly abbreviated to SATs.

Chilcot inquiries.[47] These highlighted the difficulties of unaided judgements and lack of transparency, leading to the promotion of SATs and their inclusion in professional standards and training.

a. **Benefits.** The benefits of SATs can be summarised as promoting the following.

- Conscious and deliberate thinking – SATs compel users to actively think about information, including evidence, assumptions and judgements, rather than relying on intuition or mental shortcuts that are more susceptible to bias.

- Structured and systematic thinking – SATs provide frameworks to assist users in thinking logically, consistently and broadly, minimising the risk of overlooking or missing steps and/or information.

- Transparency of thinking – SATs expose normally opaque, internal cognitive processes, making them transparent and external and therefore easier to understand and examine.

b. **Complementary uses.** As a result of these benefits, SATs have multiple complementary uses when applied in processing and analysis activities. However, it is important to note that they assist, rather than replace, human reasoning. As such, they are tools to aid the analyst's creative and critical thinking, not a substitute for that thinking, and they will not provide 'answers' in their own right. SATs assist in the following.

- Mitigating bias – making thinking conscious and systematic reduces the probability of errors caused by cognitive biases such as anchoring, confirmation bias or groupthink.

- Enabling testing and challenge – exposing the rationale behind judgements allows the analyst to check their own thinking and facilitates constructive external challenge, thereby strengthening rigour.

47 *The Review of Intelligence on Weapons of Mass Destruction* and *The Report of the Iraq Inquiry* respectively.

- Organising and planning – the structured frameworks can help identify what information is known, what is assumed and where there are gaps. This aids interpretation and evaluation, enables collection requirements to be prioritised and makes subsequent analysis more efficient.

- Improve impact on decision-makers – the outputs of analysis may be more positively received if consumers see and understand how they are justified.

- Supporting quality assurance processes – the structure and transparency provided by SATs facilitates review by supervisors.

- Providing an audit trail – SATs can form part of the audit trail, capturing the intellectual reasoning underpinning a judgement in a way that can be replicated later if required.

- Enabling sharing and information knowledge management – SATs provide a common framework in which reasoning can be easily updated and shared with peers, including forming part of the handover between analysts.

How and when to apply SATs in Defence Intelligence can be found in Defence Intelligence's *Quick Wins for Busy Analysts* and other UK government products, such as the *GOScience Futures Toolkit*. The application of SATs is also taught on various Defence Intelligence and Professional Head of Intelligence Analysis (PHIA) training courses. Further academic and commercial literature is also available.

Processing and analysis – subordinate functions

3.34. Processing and analysis can each be broken into three subordinate functions, as illustrated in Figure 3.3. Processing consists of collation, interpretation and evaluation, and analysis comprises synthesis, assessment and production.

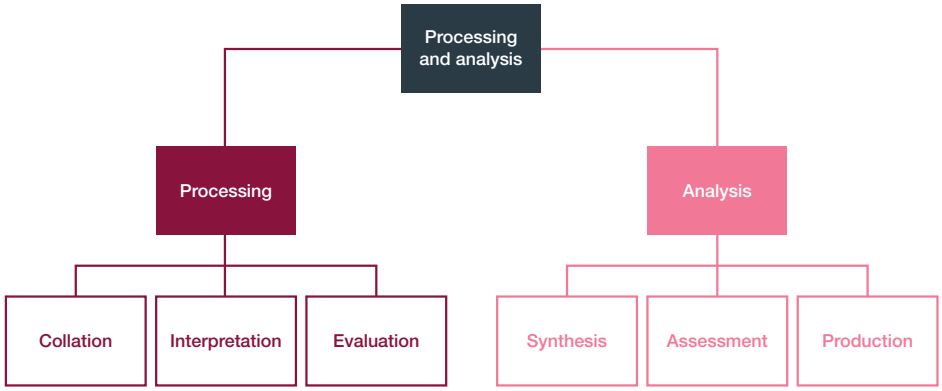


Figure 3.3 – Processing and analysis

Processing

3.35. Contemporary collection platforms and systems produce vast volumes of data, but all are still operating in the presence of denial, deception and the 'noise' of cluttered environments. Rarely can the information and data acquired during collection be understood without considerable effort. Processing forms the interface between collection and analysis, and between the ISR process and the intelligence cycle. The ISR process collects, processes and exploits data before disseminating it to the processing and analysis phase of the intelligence cycle. This ensures potentially highly technical data is presented in a useable form for subsequent usage. A further stage of processing may, however, be required within the intelligence cycle to enable analysis, for example, the translation of reports into a common format and their storage in a common location.

3.36. **Components.** Processing within the intelligence cycle consists of collation, interpretation and evaluation. Both interpretation and evaluation depend on collation, but the three components are not necessarily conducted in a specific sequence, and are often developed in parallel as the data and information are examined and reviewed.

3.37. **Collation.** Collation is defined as: in intelligence usage, an activity 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.[48] Collation draws together information from disparate sources that are relevant to the same intelligence requirement. It establishes the foundation for both interpretation and evaluation by providing a structure in which the

48 NATOTerm.

information gathered can be contextualised and cross-referenced and, in doing so, underpins analysis. This structure records what information was available at a given time, where it originated and its classification, minimising the risk of information getting missed or mishandled. By incorporating the results of interpretation and evaluation, it can also capture the value assigned to different information rather than simply its presence, further supporting the analysis phase. As such, it forms the basis of a strong audit trail by recording the extent to which information was used in generating a specific intelligence output and what influenced this. Collation involves receiving and recording all incoming information and intelligence, then grouping them appropriately. This is applicable to intelligence activity at all levels, with groups or categories determined by the intelligence requirements and type of operation. At its simplest, collation may involve no more than the maintenance of a log or a marked map or chart. However, it is increasingly common to use electronic databases due to the nature and volume of information and the need to sustain the system across multiple sites or for longer durations. In the future, collation systems should grow in sophistication in line with collection and analysis practices, linking to graphic interfaces and making more use of automation. In all cases, the collation process must be monitored and maintained to ensure it is carried out rapidly, efficiently and in line with legal and security requirements.

3.38. **Interpretation.** Interpretation is defined as: in intelligence usage, an activity in the processing phase of the intelligence cycle during which the significance of information or intelligence is judged in relation to the current body of knowledge.[49] Interpretation extracts meaning from collection products so they can be fully and appropriately used during the analysis phase. These products may have been partially processed electronically beforehand, such as the conversion of 'raw' technical data into imagery or searchable databases. Interpretation goes beyond this though to draw out the relevance of information for later analysis. Technical data acquired from electromagnetic intelligence, imagery or measurement and signature intelligence must be converted into a form that non-specialist consumers can understand. Intercepted communications may need to be decrypted, or translated if in a different language, and potentially further clarification and explanation added if the subject matter is highly technical. A human source may witness activity such as a movement of vehicles or equipment that they can describe but not identify. This may be meaningless to them but could provide an important indication for warning intelligence if interpreted appropriately. Similarly, objects observed on imagery require interpretation to identify them and enable further analysis. The increasing availability of data, particularly from open sources,

49 NATOTerm.

means interpretation is vital for understanding what the data is telling us about and therefore what it can add to analysis of a subject. Effective interpretation may rely on specialists with subject matter-specific or technical expertise and methods (including data scientists, linguists, etc.) but can also be achieved by using prior experience or other information for context.

3.39. **Evaluation.** Evaluation is defined as: in intelligence usage, an activity in the processing phase of the intelligence cycle consisting in an appraisal of the quality of the reported information, which is key to determining the reliability of the originator or source and the credibility of the information.[50] Evaluation is vital for all aspects of intelligence analysis because it determines the weight that can be placed on a specific source and its reporting when forming analytic judgements. Sources must be evaluated for the accuracy and trustworthiness of their information, an activity sometimes referred to as validation. Every form of intelligence collection has limitations in terms of coverage and accuracy. Coverage may be limited by technical constraints, opportunity and an adversary's operations security and other denial measures. Inaccuracy can arise from sensor artefacts, human error and cognitive bias during interpretation. Moreover, all collection activities are susceptible to the risk of detection by an adversary's counter-intelligence measures and, consequently, deception as well as denial. It is vital, therefore, to evaluate whether the interpretation of a collection product can be trusted or if it is somehow erroneous or misleading. The main considerations in conducting evaluation are therefore the reliability of the source, the credibility of the information and the requirement to review and re-evaluate previously evaluated sources.

a. **Reliability of the source.** This concerns the level of trust or confidence that can be placed on the source of the information. For human sources, it is necessary to consider their motivation, expertise and level of access. This includes organisational sources such as media platforms as well as individual human sources. Judgements of reliability in human and organisational sources largely depend on the reporting history of the source in terms of accuracy and correlation with other sources over time. These need to be continually reviewed and updated, especially for new indications of adversary influence or control. For technical sources, reliability relates to the operational capabilities and limitations of a system. Regular review is also necessary to identify if capabilities are degrading due to age or system faults and to ensure that the source is not being systematically manipulated by an adversary, for

50 NATOTerm.

example, through the use of signals that take advantage of a collection system's specific capabilities and characteristics.

b. **Credibility of the information.** This concerns the level of trust or confidence that can be placed on the information or specific reporting from the source. Credibility of reports can be evaluated in isolation, internally by identifying content that is factually incorrect or logically implausible, or externally by considering outside influences on the collection effort, such as weather or the electromagnetic environment for technical sources. However, credibility is usually best assessed by corroborating with other sources that may confirm or disconfirm the substance of that report. Corroboration is important when making analytic judgements, but care should be taken to mitigate against bias. Contradictory information should still be evaluated and analysed, not discarded simply because it is different, and operators must be alert to the possibility of circular reporting.

c. **Review and re-evaluation.** Reliability and credibility must be evaluated separately. A previously reliable source may still provide inaccurate information through sincere error or coming under hostile control, and occasionally highly credible information can come from a usually unreliable source. It is also good practice to review evaluated sources to avoid confirmation bias, as information initially deemed improbable through lack of corroboration could become more credible. Alternatively, credible reporting could be placed in doubt, as additional information is received.

3.40. **Intelligence grading.** Intelligence grading refers to the process used to provide a commonly understood way of describing initial evaluations of the reliability of a source and the credibility of the information. As well as an initial evaluation, gradings should be reviewed as further intelligence is acquired to update evaluation judgements about both the source and their reporting, especially if the source is liable to produce additional reporting. Additionally, the grading of a source and its reporting may also need to be reviewed when examined in a wider context or with deeper subject matter expertise during the analysis phase. Whilst the NATO Intelligence Grading System is widely used, other approaches are also possible.

a. **NATO Intelligence Grading System.** This framework is sometimes referred to as the 'Admiralty Code' and is shown at Table 3.1. It captures the separate judgements of reliability and credibility in a single

alphanumeric digraph with reliability graded from A to F and credibility from 1 to 6. A usually reliable source providing improbable information would result in B5, and confirmed information from an unreliable source would be E1. The two ratings do not need to 'match' on the scales (for example, B2 or E5). It is also important to note that a grading of F6 (or either element separately) does not render the information useless or mean it has no value. It simply means that there is insufficient internal evidence or independent confirmation to make a judgement on reliability and/or credibility and the analyst will have to evaluate the information themselves in the context of their requirement.

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

Table 3.1 – The NATO Intelligence Grading System

b. **Alternative approaches to intelligence grading.** Different organisations may use different forms of grading that may be variations on the 'Admiralty Code' or be significantly different, such as being limited to a broad description of the nature of the source, its level and quality of access and some sense of its reporting history. It is especially important in the integrated environment to have a good understanding of the evaluation methods and standards used by other agencies, and particularly allies and partners.

Analysis

3.41. Analysis is defined as: in intelligence usage, an activity in the processing phase of the intelligence cycle in which information is subjected to review in order to identify significant facts for subsequent interpretation.[51] Analysis turns processed information into intelligence that has value for decision-makers. It reduces uncertainty for decision-makers in terms of what is happening or

51 NATOTerm.

may happen next by determining the significance of processed information against specific requirements and purposes. Analysis can be focused on past, present or future events, or a combination, so analysts must consider what the decision-maker intends to use the intelligence for when determining their approach. For example, a range of potential outcomes may be more valuable and less risky for planning activities than a single, specific prediction. Similarly, this range of potential outcomes may be sufficient for general long-term planning but may need to be developed into sets of indicators and warnings for monitoring specific threats. While some commanders'/decision-makers' requirements can be met by single source analysis, most requirements will benefit from reference to other sources to increase corroboration and confidence. As a rule, analysis should therefore draw on as wide a range of sources and collection disciplines as is required to meet information needs whilst minimising the risk of deception.

3.42. **Analysis – components.** Analysis consists of synthesis, assessment and production. Synthesis and assessment may take place separately or together in the mind of the individual analyst. They should also link back to processing as gaps are revealed or information needs to be re-evaluated in the light of links identified. While production naturally forms the last stage, it is good practice to plan production in parallel with other activities for efficiency and to keep focused on the commander's/customer's requirements. Synthesis and assessment are principally human cognitive functions, depending on creative thinking to address gaps in information or understanding and critical thinking to assess implications for the requirement. Analysts should remain aware of, and consciously address, the impact these personal and subjective intellectual functions may have on their judgements. As described earlier, SATs are useful methods for improving rigour in synthesis and assessment by mitigating bias, adding structure and enabling challenge.

3.43. **Synthesis.** Synthesis (also referred to as 'integration') is the basis of sound analysis, assembling the core pieces of the intelligence picture. During this step, analysts make sense of the body of processed information available to them (as opposed to interpretation, which is more about making sense of individual pieces of unprocessed information). This should normally be done in the context of an SIR but it is also applicable when producing a general summary for situational awareness. Synthesis is achieved by identifying links, patterns and anomalies in the processed information, resulting in descriptive explanations of what something does, how it works, what is happening in a situation, etc. As such, it can be an end in its own right, generating basic and current intelligence (see paragraph 2.14 a–b). However, it can also be

used to underpin assessments depending on the intelligence requirement. For example, synthesis may result in an order of battle of adversary forces for reference purposes, but this may later become vital to a net assessment of the balance of forces between two belligerent parties.

3.44. **Assessment.** Assessment builds on synthesis to answer the linked questions of 'so what?', 'what next?' and 'what if?'. It involves making judgements about what the explanations mean for customers in the context of their SIR, providing insight and foresight. This is often associated with predictive analysis, but also includes judgements about the implications of a subject (for example, a particular capability, situation or event) for a decision. The two primary considerations for analysts in conducting assessment are probability and their level of analytical confidence. PHIA methodologies to support analysts conducting this work are described in detail in paragraphs 3.46–3.48.

a. **Probability.** Since assessments are generated using incomplete, potentially unreliable and/or unknowable information, judgements should include the probability that each hypothesis is true or that outcomes (future hypotheses or scenarios) will occur. Factors influencing this probability are the frequency of comparable events, the strength and reliability of related indicators, the reliability and credibility of the source material (source confidence), and the extent of coverage.

b. **Analytical confidence.** Judgements are inherently subjective, introducing further uncertainty from the impact of individuals' cognitive biases. Actively challenging judgements, exploring alternatives and seeking to disprove rather than confirm can improve confidence in the assessment as a whole, increasing its value to a decision-maker. The use of appropriate analytical standards and methods is essential to ensuring that judgements are rigorous and justifiable, including by providing an audit trail of decisions that underpin them.

3.45. **Production.** Production captures the results of synthesis and, where appropriate, assessment in forms that will clearly and effectively communicate those results and judgements to decision-makers. Production lies on the interface between processing and dissemination, and is integral to making analysis truly valuable to customers. Production may result in verbal briefings, textual reports and/or audiovisual digital media, whichever is most appropriate for the principal customer, and other collateral customers if required. These may be stand-alone products, updates or part of a series. Regardless of

format, it is essential to provide assurance that processing and analysis has achieved its purpose of meeting intelligence requirements and has delivered valuable, impactful support to decision-makers. The following checks have different but related purposes and, depending on resources and time, can be conducted by the analyst, peers, supervisors/managers or by independent challenge, or through a combination. They can occur in any order, and separately or concurrently but they need to address each of the three purposes.

a. Check the analysis against the requirement, considering the needs, knowledge and position of the intelligence consumer. This should include practicalities such as classification, form and format, but should focus on whether the output will have the desired impact.

b. Check the analytical reasoning to make sure that the analysis and judgements being conveyed are logical and justifiable, supported by evidence wherever possible and with clear rationale for why alternative outcomes were rejected.

c. Check for clarity, ensuring that facts/evidence, assumptions and judgements are sufficiently differentiated and uncertainty appropriately communicated, including key remaining gaps. This ensures not only that intelligence analysis is understood by the consumer, but also cannot be misunderstood.

Analysis and production standards

3.46. **The Professional Head of Intelligence Assessment Analytic Standards.** The PHIA Analytic Standards set expectations and best practice for how analysis and assessment should be conducted. These are mandated for use by all-source analysts working across Defence, but they will also be useful for staff working in other disciplines. The eight standards shown in Figure 3.4 direct that analysis and assessment should be independent, clear, comprehensive, auditable, relevant, rigorous, objective and timely, primarily covering activities in the processing and analysis stage of the intelligence cycle. Within this, they are most directly applicable to synthesis and assessment, but are also valuable as part of the quality assurance conducted under production.

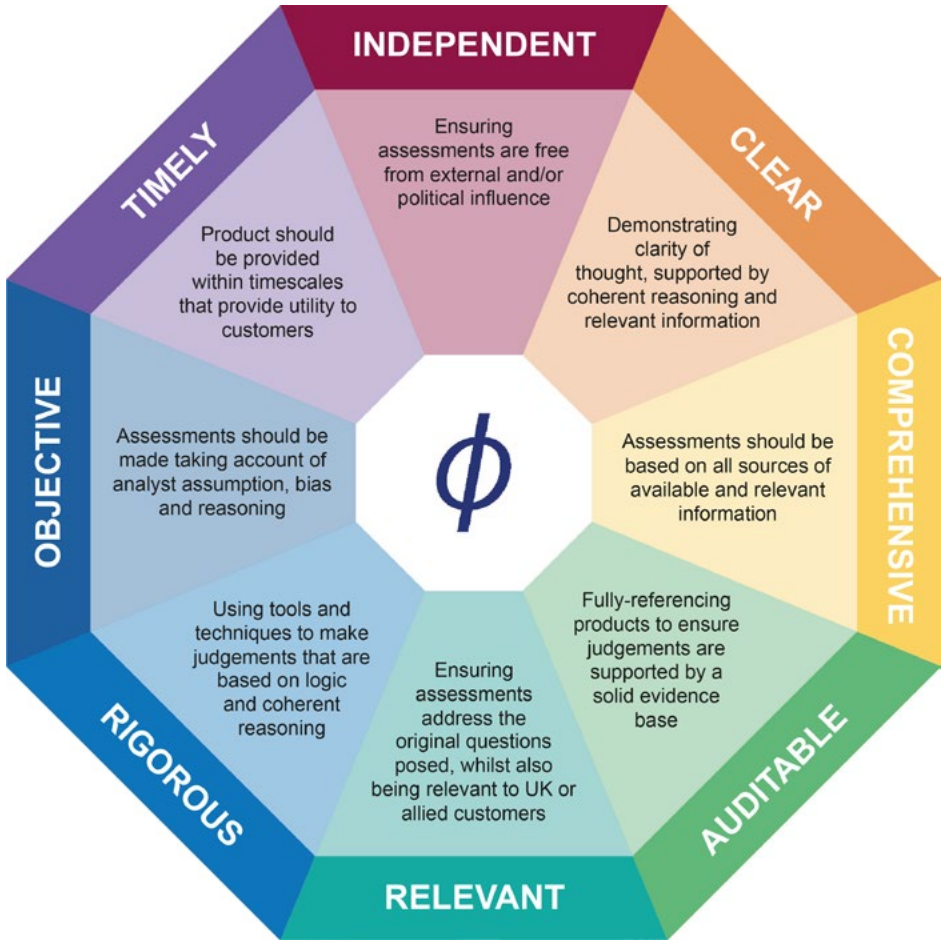


Figure 3.4 – Professional Head of Intelligence Analytic Standards

3.47. **Probability yardsticks.** Accurate depiction of probability is key in the production of analytical judgements. All intelligence products provided to consumers of intelligence must convey explicitly the probability of this event or events occurring. To avoid miscommunication between the analyst and the consumer of intelligence, Defence mandates the use of the PHIA Probability Yardsticks shown at Table 3.2 and Figure 3.5 for subjective probability judgements. This provides a standardised set of probabilistic language that equate to numeric ranges, making it clear what is meant by different terms so that consumers interpret the terms as the analyst intended. The Probability Yardstick is intended for the communication of probability only, not analytic confidence, and it is expected that analysts arrive at their probabilistic judgement using suitable robust methods.

Probability range	Judgement terms	Friction range
≤ ≈5%	Remote chance	≤ ≈1/20
≈10% – ≈20%	Highly unlikely	≈1/10 – ≈1/5
≈25% – ≈35%	Unlikely	≈1/4 – ≈1/3
≈40% – < 50%	Realistic possibility	≈4/10 – < 1/2
≈55% – ≈75%	Likely or Probably	≈4/7 – ≈3/4
≈80% – ≈90%	Highly likely	≈4/5 – ≈9/10
≥ ≈95%	Almost certain	≥ ≈19/20
≈ approximately equal to	≥ is greater than or equal to < is less than	≤ is less than or equal to

Table 3.2 – Defence Intelligence and Professional Head of Intelligence Assessment Probability Yardstick

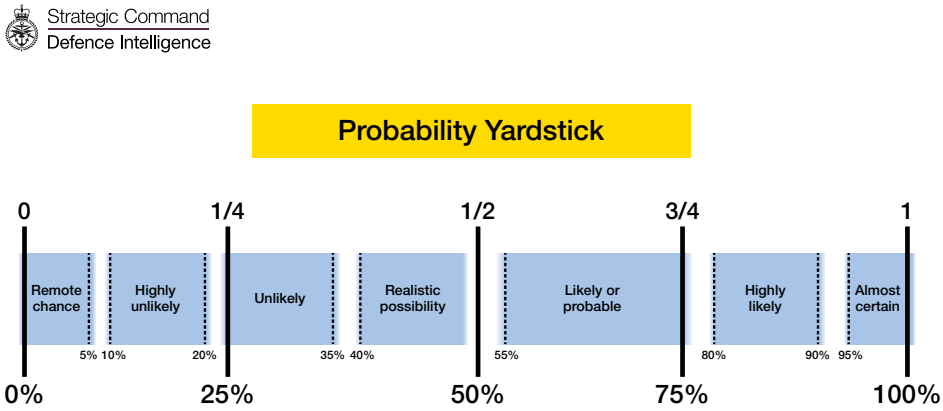


Figure 3.5 – Defence Intelligence and Professional Head of Intelligence Assessment Probability Yardstick

3.48. **Analytical confidence.** An expression of analytical confidence can be described as a statement on the extent to which there is determined to be a sound and stable basis for assessing the probability of an occurrence taking place. The PHIA standard for evaluating and communicating analytical confidence is to be used by all-source analysts across Defence. If assessments of analytical confidence are to be made or communicated, they must use the standardised form of words and supporting criteria, rather than any local alternative. However, unlike the Probability Yardstick, it is not mandated for all assessments, with organisations free to choose which

activities and products it applies to. Analytical confidence is divided into three categories, each of which comprise different sets of criteria for evaluation.

- Information base – the information and sources on which an assessment is based.
- Analytical rigour – the analytical processes and tools/methods applied to the information.
- Complexity and volatility – the inherent properties of the environment being analysed (that may influence judgement stability).

The main purpose of evaluating analytical confidence is to enable articulation of the strengths and weaknesses of analytical judgements. In addition to communicating this to decision-makers, evaluations of analytical confidence can be used for quality assurance and preparing for follow-up work as it highlights aspects of analysis that could be improved.

Section 5 – Dissemination

> Intelligence without communication is irrelevant.
>
> General A M Grey, United States Marine Corps

3.49. Dissemination is defined as: the timely conveyance of intelligence, in appropriate forms and means, to those who need it.[52] Getting intelligence to the user at the right time and in the appropriate format is essential for successful intelligence operations.

3.50. **Requirement management.** 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. The process must be able to track the status of each intelligence requirement to confirm whether it has been satisfied or if it requires further tasking. This mechanism will also ensure that the demander confirms receipt of the report. Intelligence dissemination should include provision for feedback and dialogue from the decision-maker and users, between peers and from analyst to collector.

52 NATOTerm.

3.51. **Dissemination management.** It is important for intelligence staff to manage the dissemination process continuously. Without effective management, communications paths can become saturated by information. For example, single-source reporting may be retransmitted by many intermediate collection agencies, resulting in circular reporting.[53] Advances in technology are also transforming dissemination through enhancing the means available for storing and accessing information, whilst some collection systems can disseminate collected information to requesters on a real time or near-real time basis, vastly increasing their responsiveness.

Factors affecting dissemination

3.52. **Push and pull principles.** Dissemination has traditionally consisted of both push and pull control principles, but their application will continue to be modified by rapid advances in storing and accessing information and data, and the resulting intelligence assessments. Technological advances will continue to see a move away from reliance on end product reporting to a position where intelligence personnel will be able to search and discover all available data relevant to their requirements.

a. **The push and pull concepts.** The push concept allows for 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 using cloud storage, knowledge repositories, databases, intelligence files or other data and information repositories that are accessible to intelligence organisations at all levels of command. Intelligence products should be organised and presented using web-based technologies and universally recognised standards within Defence.

b. **Dynamic access.** This is a data-centric methodology centred around subscription and alerting services. This requires neither the 'shotgun' push of large volumes of data to any and all interested parties nor the requirement for analysts to actively hunt for relevant data, information and intelligence. Instead, it allows for a high level of situational awareness by alerting users to the availability of new information without the need to immediately disseminate it. As artificial

53 Circular reporting occurs where material is conveyed and then repeated a number of times in separate assessments when in fact it has just come from one source. The repetition gives the appearance that the material may be new or additional corroboration when it had actually been reported previously.

intelligence and machine learning technologies mature, this will provide a learning system that is able to predict and signpost the most relevant, timely and important information to the right user at the right time.

3.53. **Dissemination methods.** Intelligence is disseminated by three core methods: verbal briefing, printed material and electronically.[54] Electronic means of storing and accessing information have and will continue to develop at pace, thereby enhancing the ability of intelligence users at all levels to access material directly rather than being reliant on receiving cascaded information, data or assessments. The Defence Digital Defence Information Environment will underpin future developments in storing, managing and accessing information, data and assessments.

3.54. **Formatting.** After determining who needs to receive each report, intelligence staff must determine how much of the report each user requires and in what format. Considerations include the decision-makers requirements or preferences, user requirement, speed of transmission, the available bandwidth, legal restrictions and security classification.

3.55. **Principles of dissemination.** Dissemination is governed by the principles of: latency, appropriateness, urgency, distribution and security. These are explained below.

a. **Latency.** There are two aspects to latency. 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 products must detail when any truncation of processing to meet deadlines was required so that the user may treat it with an appropriate level of discretion.

b. **Appropriateness.** Disseminated intelligence should enhance understanding and be in an accessible format. IRM staff will ensure the appropriateness of intelligence to meet the user's needs, and make

54 Printed material may include intelligence reports, intelligence summaries, maps and imagery intelligence reports. Cloud-based storage, knowledge repositories and websites can store multiple forms of information and may allow demanders to conduct their own IRM. The effectiveness of any form of electronic storage and retrieval is dependent on its management and the quality of the inputs, including any underlying coding.

sure 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 obtained to meet an intelligence requirement should be converted into intelligence before dissemination. However, when time is at a premium, the full processing and analysis of information may not be possible and dissemination should be undertaken as quickly as possible, with the caveat that it is unprocessed and may not be reliable.[55] Data-centric approaches now allow for the assessment of a wider range of information and data, without reliance on the judgement of the value of a single piece of information.

d. **Distribution.** Intelligence staff are responsible for ensuring that all intelligence is disseminated to those who need it. The commander and intelligence staff may require the distribution of additional summaries of intelligence to other agencies and formations outside the normal chain of command, such as partners across government. Commanders should ensure that suitable capabilities and processes are in place to enable effective distribution. Technological advances in information and data storage and accessibility also allow intelligence staff greater access to data and assessments relevant to their requirements.

e. **Security.** Intelligence should be classified at the level required and not be over-classified. Over-classification causes delays in handling and transmission. The use of 'tear-lines' can balance the requirement to maintain security and protect the source whilst allowing for the greatest possible distribution. There may be occasions when the risk of compromising the source has to be weighed against the value of the information. On such occasions, the intelligence staff must make recommendations on the impact of possible compromise to assist the commander in making a decision; such decisions must not be taken without J2 advice, including consultation with the originator of the intelligence. Special arrangements are 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 is the agency supplying the information.

55 This applies particularly to urgent operational information and intelligence at the tactical level.

Dissemination procedures

3.56. **Knowledge repositories.** Interconnected intelligence repositories are required to simplify access to intelligence in digital storage, from multiple databases, whilst guaranteeing data integrity and speed of dissemination. Increasing the connectivity between information and data repositories is essential to enable the integration, sharing and fusion of data across operational domains, disciplines and platforms. Ongoing Defence programmes will further enable analysts to access information, data and assessments from across the spectrum of single-Service information storage systems.

3.57. **Dissemination issues.** Dissemination is reliant on the availability of suitably accredited systems to process the information and the availability of sufficient bandwidth to enable the movement of data between locations. The IRM 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.

3.58. **Evaluating reports.** Evaluating reports will determine how well the intelligence process is satisfying the commander's and others' intelligence requirements. IRM staff should review the relevance, completeness and timeliness of intelligence reporting.

3.59. **Quality control.** Intelligence must be in a form that the recipient readily understands and can directly use. Intelligence staff should consider the clarity, relevance, currency, brevity, ease of assimilation – ideally by using fused products assimilated from multiple sources – and adherence to security procedures before disseminating an assessment.

Reporting formats

3.60. **NATO reporting formats.** The UK uses NATO standards for report formats and message sets to guarantee multinational interoperability.[56] Wherever possible, written and web-based intelligence reports should be consistent with the NATO formats in Table 3.3.

56 AJP-2, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*, Chapter 4.

Report	Description
Intelligence report (INTREP)	Sent whenever information or intelligence is urgent and contains any deductions that can be made in the time available. INTREPs can comprise threat reporting containing unprocessed data and information.
Intelligence summary (INTSUM)	A concise, periodic summary of intelligence about the current situation within the joint operations area. 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.
Supplementary intelligence report (SUPINTREP)	A stand-alone summary of intelligence for a given subject or situation. It updates the current intelligence picture, addressing a specific issue or highlighting important developments inside the normal reporting cycle.
Single-source reports	Other intelligence reports and summaries are periodically generated to address specific subjects, for example, interrogation reports and technical intelligence reports.
Counter-intelligence reports	Similar to INTREPs, counter-intelligence (CI) reports comprise CI-INTREPs, CI-INTSUMs and CI-SUPINTREPs. Counter-intelligence staff may also produce threat assessments and threat warnings to inform commanders of specific security threats.
Thematic reports	These address aspects of the operating environment, such as a geographic location, a political or religious movement or a particular adversary organisation.

Table 3.3 – NATO reporting formats

3.61. **Other intelligence reporting formats.** In addition to the formal NATO Alliance, the UK is a party of a large number of political and military agreements on both a bilateral and multilateral basis. Comprehensive intelligence exchange arrangements already exist between most of our allies and partners. When conducting multinational operations, the basic principle is for each nation to deploy with its own intelligence infrastructure and then adapt to any coalition requirements. In respect of reporting formats, intelligence specialists must be aware of other reporting formats they may need to use. A standardised approach is much easier to achieve if these have been decided from the outset prior to deployment.

Key points

- The four core functions in intelligence are: direction, collection, processing and dissemination.
- Multiple-source intelligence comprises more than one line of reporting from one or more collection disciplines. One can have multiple sources within a single collection discipline.
- Multidisciplinary intelligence fuses information drawn from more than one source from across two or more collection disciplines.
- Intelligence evaluation examines reliability of the source and credibility of the information. A widely used framework is the NATO Intelligence Grading System, which grades reliability and credibility in an alphanumeric digraph.
- The Defence Intelligence all-source analytic standards direct that analysis and assessment should be independent, clear, comprehensive, auditable, relevant, rigorous, objective and timely.

Notes


06
05
ZP805

Chapter 4

Chapter 4 explains the principal disciplines, specialisms and activities that generate information that is subsequently processed into intelligence. The chapter also includes legal considerations.

> “... one should make a conscious decision as to the collection: there is an abundance of data surrounding us all now, most of it freely available, but there is only so much time and so many resources to handle it. Effort must therefore be focused on the specific items and issues necessary for you ...”

General Sir Rupert Smith, *The Utility of Force*

Chapter 4

Intelligence disciplines and activities

4.1. Intelligence production is organised into a range of specialised activities or disciplines. There are three main categories.

- Collection disciplines – specific groups of related methods of acquiring data and information from technical and human sources.
- Analytical specialisms – fields of subject matter expertise that draw on information acquired through the various collection disciplines to produce analysis and assessments to support understanding and decision-making.
- Multiple-intelligence activities – these draw on combinations of collection and analytic disciplines, typically directed towards specific operational effects.

Section 1 – Collection disciplines

4.2. **Signals intelligence.** Signals intelligence (SIGINT) is defined as: intelligence derived from electromagnetic signals or emissions.[57] It is the generic term used to describe communications intelligence (COMINT) and electromagnetic intelligence (ELINT) when there is no requirement to differentiate between these two types of intelligence, or to represent their fusion.[58] COMINT and ELINT are respectively defined as follows.

a. **Communications intelligence.** COMINT is defined as: intelligence derived from electromagnetic communications and communication systems by other than intended recipients or users.[59] COMINT is typically derived through the interception of communications and data links. Such information may be collected in verbal form by receiving broadcast

57 NATOTerm.
58 This discipline is described further in Allied Joint Publication (AJP)-2.4, *Allied Joint Doctrine for Signals Intelligence*.
59 NATOTerm.

radio messages, by intercepting point-to-point communications, such as telephones and radio relay links, or as data by intercepting either broadcast or point-to-point data downlinks.

b. **Electromagnetic intelligence.** ELINT is defined as: intelligence derived from electromagnetic non-communications transmissions by other than intended recipients or users.[60] ELINT is derived from the technical assessment of electromagnetic non-communications emissions such as those produced by radars and by missile guidance systems. It also covers lasers and infrared devices when used for sensing and any other equipment that produces emissions in the electromagnetic spectrum. By comparing information about the parameters of the emission that has been intercepted with equipment signatures held in databases, valuable intelligence can be derived about the equipment and its operator.

4.3. **Measurement and signature intelligence.** Measurement and signature intelligence (MASINT) is defined as: intelligence derived from the scientific and technical 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.[61] MASINT capabilities use detailed measurements and signatures and a comparison of specific phenomena to detect, track, identify and/or otherwise characterise a sample, object or event. MASINT capabilities can exploit geophysical, electromagnetic or material properties. Examples of MASINT information include, but are not limited to, intelligence derived from advanced processing of radar emissions returns, nuclear air sampling and acoustic or seismic signatures.[62]

a. **Acoustic intelligence.** Acoustic intelligence (ACINT) is defined as: intelligence derived from acoustic signals or emissions.[63] ACINT capabilities are primarily used to detect, classify and track the acoustic sources associated with maritime units and to enable strategic understanding through the exploitation of platform signatures. ACINT is predominately obtained in the underwater engagement space from the overt and/or covert collection by submarines, ships, aircraft and fixed systems. ACINT is a specific application of MASINT's geophysical sub-discipline.

60 NATOTerm.
61 NATOTerm.
62 This discipline is described further in AJP-2.8, *Allied Joint Doctrine for Measurement and Signature Intelligence*.
63 NATOTerm.

b. **Measurement and signature intelligence sub-disciplines.** Allied Joint Publication (AJP)-2.8, *Allied Joint Doctrine for Measurement and Signature Intelligence* outlines eight MASINT sub-disciplines, as detailed in Table 4.1, acknowledging national variations in the categorisation of capabilities and sub-disciplines in this field.

North Atlantic Treaty Organization measurement and signature intelligence sub-disciplines							
Biometrics	Radio	Geophysical	Electro-optical	Nuclear	Materials	Multi/hyper-spectral	Radar
Identification of facial features, scars, tattoos Voice Iris Fingerprint DNA	Radio waves Electromagnetic pulse detection Unintentional radio frequency	Seismic/acoustic/vibrometric sensing Very low frequency Extremely low frequency	Non-imaging infrared Visible light Non-imaging ultraviolet LASER	X-rays Gamma ray detection Neutron detection Cosmic ray detection	Chemical/biological sensing - Liquid - Solid - Aerosol - Gas	High spectral resolution across multiple narrow bands - Infrared - Visible - Ultraviolet	Microwave Over-the-horizon radar Synthetic aperture radar Polarimetric

Table 4.1 – Examples of measurement and signature intelligence sub-disciplines[64]

4.4. **Geospatial intelligence.** Geospatial intelligence (GEOINT) is defined as: intelligence derived from the exploitation and analysis of geospatial information, imagery and other data to describe, assess or visually depict geographically referenced activities and features.[65] GEOINT includes imagery intelligence (IMINT) and the production or analysis of geospatial information; it underpins understanding, planning, navigation and targeting. Geospatial information is defined as: facts about the earth referenced by geographic position and arranged in a coherent structure.[66] Assured geospatial information, which has been subject to quality assurance checks by a specialist geospatial centre,[67] is known as foundation GEOINT. It describes the physical environment and includes data from the aeronautical, geographic, hydrographic, oceanographic and meteorological disciplines. GEOINT includes IMINT reports, which may be provided as machine-readable data or in more traditional formats (paper or digital maps and charts) and digital geospatial information, which may be

64 Table derived from AJP-2.8, *Allied Joint Doctrine for Measurement and Signature Intelligence*, page 2-2.
65 Joint Doctrine Publication (JDP) 0-01.1, *UK Terminology Supplement to NATOTerm*.
66 NATOTerm.
67 See Joint Service Publication (JSP) 465, *Defence Geospatial Intelligence Policy*, Part 1.

provided as web services. It also defines the geospatial reference framework, consisting of a common datum and coordinate system, which enables other data or information (including intelligence mission data) to be linked and visualised in space and time as interactive layers – this forms the foundation for a common operating picture.

4.5. **Imagery intelligence.** IMINT is defined as: intelligence derived from imagery acquired from sensors that can be ground-based, seaborne or carried by air or space platforms.[68] IMINT can be both still imagery or full motion video, across various electromagnetic bands, including visible light and infrared. IMINT can be supported by, as well as support, other intelligence collection disciplines, thereby increasing the level of confidence in the resulting product. IMINT products are the result of a deliberate effort to collect, process and exploit imagery to answer intelligence requirements.[69] Technological developments in both the military and commercial world have further expanded the range of sources available. Advances in artificial intelligence and machine learning are becoming capable of supporting some aspects of imagery analysis. Imagery, in and of itself, is not intelligence; IMINT is produced by imagery analysts who have conducted appropriate analysis of individual image sequences using specific tools and techniques. Image sensors can also provide information directly that is operationally useful, for example, for overwatch or general situational awareness/ground orientation imagery that has not been formally analysed and is not categorised as IMINT.[70]

4.6. **Human intelligence.** Human intelligence (HUMINT) is defined as: intelligence derived from information collected by human operators and primarily provided by human sources.[71] It is achieved through observing or directly communicating with people. It encompasses debriefing, source handling, tactical questioning, interrogation, military intelligence liaison, and covert passive surveillance, which are all conducted by trained personnel.[72] The direction, coordination and supervision of deployed military HUMINT elements are the responsibility of the J2X cell as part of collection management. J2X staff will maintain the register of sources and deconflict both HUMINT and counter-intelligence activity. In addition, they will provide

68 AJP-2, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*.
69 AJP-2.6, *Allied Joint Doctrine for Imagery Intelligence*.
70 This discipline is described further in AJP-2.6, *Allied Joint Doctrine for Imagery Intelligence*.
71 NATOTerm.
72 Tactical questioning and interrogation of captured persons must comply with the applicable international and domestic law. See JDP 1-10, *Captured Persons*, and JSP 383, *The Joint Service Manual of the Law of Armed Conflict*.

advice to commanders on HUMINT and the Regulation of Investigatory Powers Act 2000 (RIPA). 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.[73]

4.7. **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.[74] This encompasses the processes of collection and analysis of publicly available information (PAI) to support intelligence functions, as well as the production of dedicated OSINT products. As such, anyone conducting research using PAI specifically for intelligence purposes would be conducting OSINT. PAI is described as any information where there is a reasonable basis to believe that it is lawfully made available to the general public. This includes:

- all information available online, including that often referred to as open-source information;
- any material published or broadcast for general public consumption;
- information available on and by request to a member of the general public;
- information lawfully seen or heard by any casual observer or made available at a meeting open to the general public; and
- information that is access limited, as a result of being behind a paywall, members-only forums or deemed 'proprietary information having been collected by a commercial company'.[75]

73 HUMINT is explained in further detail in AJP-2, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security* and AJP-2.3, *Allied Joint Doctrine for Human Intelligence*.
74 NATOTerm.
75 *MOD Policy for Open-source Intelligence*, 17 June 2021.

4.8. **Open-source intelligence and media.** 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.[76] OSINT and media monitoring 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 true 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.[77]

Section 2 – Analytical specialisms

4.9. Analytical specialisms are approaches that exploit specialist knowledge or expertise, and often make use of highly developed analytical frameworks originating in the social, human and hard sciences, or other bodies of professional knowledge such as medicine or finance. Analytical specialisms are usually all-source, or not dependent on any single collection source. 'All-source' simply means that the intelligence analysis and assessment uses all available information, classified and unclassified, and includes government information as well as academic journals and media reports.[78]

4.10. **Defence Intelligence all-source intelligence assessment.** Within the UK intelligence community, we specifically identify high-level all-source intelligence assessment as a unique analytical discipline. Intelligence assessment adds an additional layer of judgement to existing analysis from across the single intelligence environment, aimed at supporting the decision-making of the highest-level customers in government.[79] The standards for all-source intelligence assessment are set by the Joint Intelligence Organisation of the Cabinet Office.[80]

76 OSINT may also require authorisation under RIPA-compliant procedures.
77 This discipline is explained in further detail in AJP-2, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security* and AJP-2.9, *Allied Joint Doctrine for Open-source Intelligence*.
78 Professional Head of Intelligence Assessment (PHIA), *Professional Development Framework for all-source intelligence assessment*, January 2019.
79 PHIA, *Professional Development Framework for all-source intelligence assessment*, January 2019.
80 All-source analysis is explained in greater detail in AJP-2, *Allied Joint Doctrine for Intelligence Counter-Intelligence and Security* and Allied Intelligence Publication (AIntP)-18, *Intelligence Processing*.

4.11. **Specialisms.** The list of specialisms below is not exhaustive and further examples may be found in AJP-2, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*. These specialisms can provide stand-alone assessments or be used by analysts conducting all-source intelligence analysis, allowing them access to information, data and specialist intelligence assessments from the widest range of available sources. The range of specialisms includes the following.

a. **Human factors analysis.** This fuses all-source intelligence analysis with a wide range of specialist behavioural and social science expertise. This includes areas such as psychology, anthropology, human geography, sociology and communication studies. Assessments are made from the perspective of that audience to understand the influence of psychological, social, cultural and environmental factors of attention, perception, sense-making, decision-making and world view. These assessments use a systems approach, focusing on both individuals and groups within organisations and states of interest.

b. **Human network analysis.** Human network analysis is an all-source intelligence analytic methodology that provides basic intelligence in the form of detailed information on networks, relationships and intentions. These networks can be complex, multi-tiered and transnational; they try to create physical and psychological effects by using both physical and cyber capabilities. They are not generally organised in a manner of conventional armed forces. The capability to understand these physical and virtual networks and to influence important individuals and groups, their network connections and specific roles is crucial to achieving objectives and to protect interests, forces and security.

c. **Financial intelligence.** Financial intelligence focuses on defence economics and threat finance. Defence economics is the analysis of economies and economic trends that are of interest to the Ministry of Defence (MOD). Specifically for countries of interest, the analysis of defence spending, the domestic economy and the economic influence wielded over other nations. Threat finance is the analysis of threat entities' financial activity to understand capabilities, intent and vulnerabilities.

d. **Chemical, biological, radiological and nuclear-related intelligence.** Chemical, biological, radiological and nuclear (CBRN) intelligence relates to all aspects of CBRN material. It includes,

for example, capabilities, locations, movement, means of delivery, infrastructure, key persons, use of, proliferation and other types of weapons of mass effect.

e. **Scientific and technical intelligence.** Scientific and technical intelligence is defined as: intelligence derived from foreign developments in basic and applied scientific and technical research and development, including engineering and production techniques, new technology, weapons systems and their capabilities.[81] Technical intelligence is defined as: intelligence concerning foreign technological developments, and the performance and operational capabilities of foreign materiel, which have or may eventually have a practical application for military purposes.[82] There are intelligence products derived from the scientific examination and testing of materiel, including computer hardware and operating system software.

f. **Cultural heritage intelligence.** Cultural heritage intelligence (CHINT) comprises awareness of both tangible remains, such as historic buildings and archaeological artefacts, and intangible heritage, such as rituals, customs and crafts, as it relates to human terrain analysis, human security and actions by state and non-state actors. CHINT permits understanding of how actors can exploit cultural heritage to achieve military, information, political, economic and diplomatic advantage.

Section 3 – Materiel and personnel exploitation

4.12. **Materiel and personnel exploitation.** Materiel and personnel exploitation (MPE) is a multi-intelligence fusion activity,[83] and is defined as: exploiting materiel and personnel by scientific, technical and specialist intelligence activities.[84] By comprehensively exploiting materiel and personnel we can gain valuable information and intelligence, either as a specific operation or as supporting activity in routine intelligence production. It contributes to understanding target development, as well as tactics, techniques and procedures of the deployed force. It can also assist with legal prosecutions for UK Armed Forces, partners

81 NATOTerm.
82 NATOTerm.
83 Multi-intelligence fusion can be multidisciplinary. Additionally, the term 'multiple-source' can represent the potential existence of multiple sources from within one discipline.
84 JDP 0-01.1, *UK Terminology Supplement to NATOTerm*.

across government, as well as allies and host nations. MPE is critical in both force protection and in enabling freedom of manoeuvre.

4.13. **Core components.** There are a series of MPE activities regarded as core components, which together deliver the overall intelligence value. Joint Doctrine Note (JDN) 2/21, *Materiel and Personnel Exploitation* is the definitive source of UK MPE doctrine and should be read in conjunction with any planning activity in which MPE is involved. The core components of MPE are shown in Figure 4.1 and further detailed in JDN 2/21.

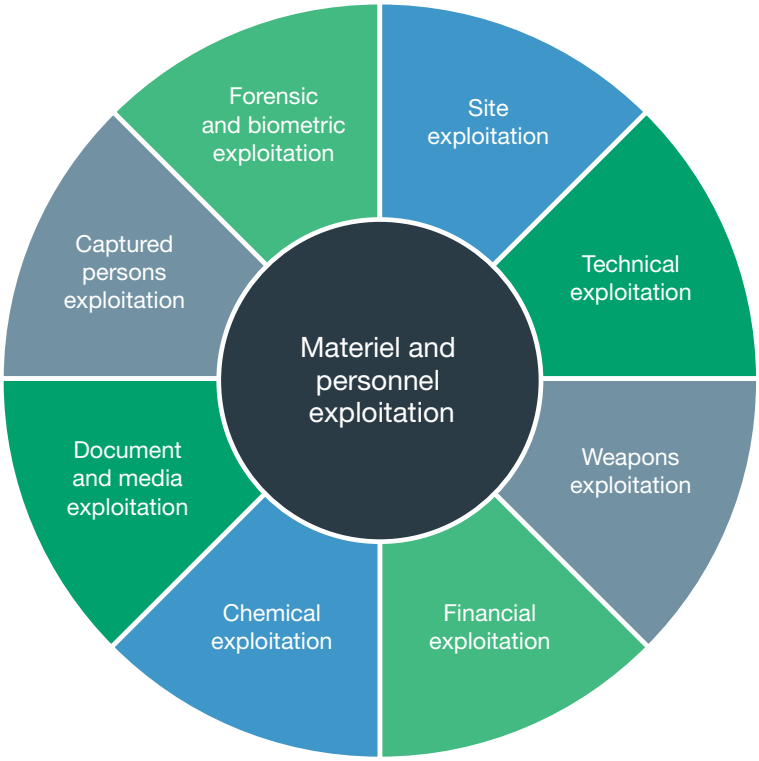


Figure 4.1 – Materiel and personnel exploitation components

4.14. **Multi-intelligence fusion.** Multi-intelligence fusion covers those military activities where multiple intelligence sources can be fused within a single organisation to create direct operational effect in support of the commander. Where intelligence is principally developed to support a commander's decision-making process, and may secondarily be used directly for operational reasons, multi-intelligence fusion may change this priority: supporting decision-making may be secondary to supporting directed military activities.

UK RC135 Rivet Joint – one of the Royal Air Force's primary intelligence, surveillance and reconnaissance platforms

4

Section 4 – Intelligence, surveillance and reconnaissance

4.15. Intelligence, surveillance and reconnaissance (ISR) is an integrated activity and a process rather than an intelligence discipline. It receives operational tasking, provides direction to ISR capabilities, collects data and information, translates this into a useable format and sends it for use by decision-makers, effecters and intelligence analysts. ISR has three primary outputs: support to operations; support to targeting; and support to knowledge development.

4.16. **Intelligence, surveillance and reconnaissance process.** ISR draws primarily on technical collection capabilities, potentially fusing non-technical and technical collection data in real and near-real time. ISR employs a five-step process comprising task, collect, process, exploit and disseminate (TCPED). These processes are outlined below, with ISR further detailed in JDN 1/23, *Intelligence, Surveillance and Reconnaissance*. In this publication, the relationship between the intelligence cycle and ISR is explained in Chapter 3, Section 3. The five-step ISR process comprises the following steps.

a. **Task.** Tasking comprises receiving external direction, internal planning, resourcing, management and allocation of ISR capabilities

(including processing, exploitation and dissemination capabilities) against the outcomes required.

b. **Collect.** Collection is the gathering of information by ISR capabilities. These assets can include technical and human sources to provide raw data.

c. **Process.** Processing is the conversion of collected raw data into a useable format for further exploitation, storage or dissemination. Depending on the data collected, processing may be undertaken by humans or machines.

d. **Exploit.** Processed data and information are exploited to derive value and attribute value to and from it. This process may also identify the requirement for additional data or information.

e. **Disseminate.** Dissemination is the process of providing access to data, information and intelligence resulting from the collect, process and exploit processes. Access may be enabled in near-real time or following more rigorous processing and exploitation activity.

4.17. **Joint intelligence, surveillance and reconnaissance.** Allied joint doctrine refers to joint intelligence, surveillance and reconnaissance (JISR). JISR is defined as: an integrated intelligence and operations set of capabilities, which synchronises and integrates the planning of operations of all collection capabilities with the processing, exploitation, and dissemination of the resulting information in direct support of the planning, preparation, and execution of operations.[85] JISR is further detailed in the three levels of Allied joint doctrine: AJP-2, *Allied Joint Doctrine for Intelligence, Counter-intelligence and Security*; AJP-2.7, *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*; and Allied Intelligence Publication (AIntP)-14, *Joint Intelligence, Surveillance and Reconnaissance Procedures in Support of NATO Operations*.

Section 5 – Counter-intelligence

4.18. Counter-intelligence is an all-source intelligence function that provides commanders at all levels with a detailed understanding of threats and vulnerabilities to enable them to make well-informed decisions on security

85 NATOTerm.

measures. Counter-intelligence is defined as: those activities concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations or by individuals engaged in espionage, sabotage, subversion or terrorism.[86]

4.19. The main thrust of the counter-intelligence effort is to counter hostile intelligence threats to personnel, information, plans, activities, capabilities and resources, both in the UK and overseas. Counter-intelligence investigations will be conducted against persons or groups believed to be engaged in terrorism, espionage, subversion and sabotage activity. Counter-intelligence investigations provide commanders with the information required to address vulnerabilities, aiming to provide knowledge and understanding to keep privileged information secure, equipment secure and personnel safe. Counter-intelligence operations further enable a commander to contest and counter terrorism, espionage, subversion and sabotage threats. A core activity within counter-intelligence is counter-espionage – the investigation, understanding and mitigation of the risk posed by and to UK nationals from a hostile intelligence service, where the UK national has access to classified material or sensitive information that could be used by a hostile intelligence service.

4.20. **Counter-intelligence – aims.** The outcomes that counter-intelligence aims to achieve are outlined in Table 4.2. This list is not exhaustive but represents the main aims.

Aim	Description
Understanding	Understand the intelligence threat from our adversaries.
Detection	Discover an intelligence threat in time to take the appropriate action.
Denial	Deny an adversary the access or influence that they seek to successfully carry out their aim.
Mitigation	Reduce the severity of the impact of an adversary's actions.
Disruption	Disrupt an adversary's hostile intelligence service's ability to threaten Defence capabilities and personnel.
Deterrence	Activity that deters adversary hostile activity.
Exploitation	Identify an adversary's intent and/or capabilities to provide opportunities for further exploitation and build our understanding of the intelligence threat posed.

Table 4.2 – Counter-intelligence – aims

86 NATOTerm.

4.21. **Counter-intelligence principles.** Underpinning all counter-intelligence aims and activities are several principles, which are central to the effectiveness and success of counter-intelligence activity. These principles are explored further below.

a. **Proactiveness.** The primary role of counter-intelligence staff is to proactively find, understand and contest intelligence threats to the force. They will then subsequently identify, in collaboration with risk owners, vulnerabilities to maintain operational resilience and freedom of action.

b. **Early engagement.** The assistance of counter-intelligence staff at the outset of the initial planning phase of the operation is essential. During operational-level planning, counter-intelligence personnel should ensure commanders understand the intelligence threats and threats to security posed by hostile adversaries.

c. **Continuity.** The counter-intelligence process needs to be sustainable in nature. The process needs to ensure continuous monitoring, awareness and understanding, as well as maintaining the ability to contest threats to security.

d. **Sensitivity.** Counter-intelligence products and activities often do not merit the widest dissemination. This is especially important when they contain sensitive information that may detrimentally impact any current investigation or operation.

e. **Interoperability.** Common or interoperable processes, networks and systems are required to support counter-intelligence direction, collection, processing and dissemination, and to manage the counter-intelligence organisation.

f. **Exchange of information.** During operations, the need to counter the existing and constantly changing threat will require the timely exchange of all available counter-intelligence information.

g. **Counter-intelligence partnerships.** Liaison between national and allied counter-intelligence organisations at the various levels and the appropriate military commands will lead to greater awareness and understanding of the overall threats and related problems in peacetime.

4.22. **Counter-intelligence activities.** Counter-intelligence is delivered through five basic counter-intelligence functions: foundational services; investigations; collection; analysis, assessment and dissemination; and operations. These are explained below.

a. **Foundational services.** The foundation of an effective counter-intelligence programme is a proactive counter-intelligence awareness programme that identifies threats and vulnerabilities against the supported unit. The programme should incorporate a broad range of counter-intelligence support functions, such as: threat education; threat briefings; counter-intelligence surveys; support to threat vulnerability assessments; and providing counter-intelligence advice or assistance to commanders and unit security officers to ensure counter-intelligence indicators are reported and investigated.

b. **Counter-intelligence investigations.** Counter-intelligence investigations provide commanders and policymakers with the information required to address vulnerabilities. Counter-intelligence investigations can provide a basis for counter-intelligence operations and collection; counter-intelligence investigations can also be developed from counter-intelligence operations, collection or analysis but must be conducted in strict accordance with applicable national laws of the respective nations involved. Counter-intelligence investigations are only to be conducted by suitably qualified and experienced personnel in accordance with Joint Service Publication (JSP) 440, *The Defence Manual of Security*.

c. **Counter-intelligence collection.** Counter-intelligence collection is the systematic gathering of information concerning threats to commands, personnel, activities, forces, installations, facilities, systems, information and capabilities from terrorism, espionage, subversion and sabotage or other intelligence activities. Counter-intelligence collection assets have the responsibility to collect and provide threat information to the commander in a timely and appropriate manner. Collection reporting can often be event-driven and thus should be transmitted without regard to a specific time schedule.

d. **Counter-intelligence analysis, assessment and dissemination.** Counter-intelligence analysis equates to the processing stage of the intelligence cycle. Counter-intelligence entities may employ an embedded analytic support element to provide readily available subject

matter expertise to entities performing the other counter-intelligence functions. The analysis process and counter-intelligence reports produced from it are disseminated as an intelligence product. Dissemination is the critical function of providing counter-intelligence assessments to the appropriate recipients in a secure and timely fashion.

e. **Counter-intelligence operations.** Counter-intelligence operations are a means of countering terrorism, espionage, subversion and sabotage threats. Counter-intelligence operations are handled on a need-to-know basis and cover a spectrum of activities during peacetime, including activity below the threshold of armed conflict, and international and non-international armed conflicts. They can make a significant input to force protection and operations security, or they can deliver operational outcomes in their own right.

4.23. **Routine and non-routine functions.** Counter-intelligence operations are categorised between routine and non-routine functions. These functions include the following activities.

a. **Routine functions.** Routine functions include counter-intelligence awareness and outreach, and establishing and maintaining liaison with appropriate entities. They also include restricted countries list travel briefings and debriefings,[87] as well as counter-intelligence debriefings. Counter-intelligence staff will also conduct counter-intelligence investigations and insider threat detection.

b. **Non-routine functions.** Non-routine functions include: offensive and defensive counter-intelligence operations; recruiting sources in support of investigations and operations;[88] using special investigative techniques as part of either counter-intelligence investigations or operations; and conducting compromise assessments. Counter-intelligence personnel may also support national security interventions.

87 Travel briefings and debriefings are routine activities for a security practitioner, however, counter-intelligence may also contribute through providing the threat understanding. Similarly, the outcomes of travel briefings and debriefings may initiate counter-intelligence work.

88 This activity operates under specific authority, requires explicit permissions and may only be undertaken by specially trained personnel.

4.24. **Counter-intelligence personnel.** Counter-intelligence personnel are responsible for countering the threat posed by hostile intelligence services and subversive, criminal or terrorist groups or individuals. This requires identifying the potential targets of, and any vulnerabilities to, an adversary's intelligence gathering operations. This information is used to inform operations security, counter-surveillance and deception planning, including protective security policy. It also supports force protection efforts, cyberspace operations, information operations, security, psychological operations, targeting and biometric exploitation.

4.25. **Counter-intelligence across multiple operational domains.** Counter-intelligence operates in all operational domains, but significantly within the cyber and electromagnetic domain. Counter-intelligence is responsible for those activities that are concerned with identifying and countering threats to Defence operations, activity and personnel from hostile intelligence services, or other hostile actors or organisations engaged in terrorism, espionage, subversion or sabotage in both the real and virtual worlds. Counter-intelligence will inform cybersecurity as an aspect of protective security and will contribute to cyber threat assessments. Cybersecurity can also identify threats and vulnerabilities leading to proactive counter-intelligence operations and investigations.

4.26. **Counter-intelligence coordination.** The Defence Counter-Intelligence Coordinating Authority (CICA) is responsible for the overall coherence and deconfliction of counter-intelligence activity across Defence. This role is performed by Defence Intelligence, Counter-Intelligence. The Defence CICA will work closely with internal and external counter-intelligence leads to deliver strategic direction and guidance, provide operational counter-intelligence updates, and track and align counter-intelligence activities and priorities between force elements. The nature of coalition operations will determine the authorities in place for deployed counter-intelligence activity and operations.

Section 6 – Security

4.27. Security is not itself an intelligence discipline or function but is an activity which seeks to protect the confidentiality, integrity and availability of people, information and assets. Security is defined as: the condition achieved when designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion, terrorism and damage,

as well as against loss or unauthorized disclosure.[89] Security is not the same as counter-intelligence, but security functions underpin counter-intelligence efforts and support counter-intelligence outcomes.

4.28. **The threat to security.** Threats to security can originate from both external and internal sources, with or without outside influence in any operational domain. Threats to security include the following.[90]

terrorism
The unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives. (NATOTerm)

espionage
In intelligence usage, an activity directed towards the acquisition of information through clandestine means and forbidden by the law of the country against which it is committed. (NATOTerm)

sabotage
In intelligence usage, acts intended to injure, interfere with, or cause physical damage in order to assist an adversary or to further a subversive political objective. (NATOTerm)

subversion
Action or a coordinated set of actions of any nature intended to weaken the military, economic or political strength of an established authority by undermining the morale, loyalty or reliability of its members. (NATOTerm)

organized crime
Sustained illegal activities by an enterprise or group of persons, irrespective of national borders, and that have as their primary purpose the generation of profits. (NATOTerm)

89 NATOTerm. Further detail on security is available in AJP-2.2, *Allied Joint Doctrine for Counter-intelligence and Security Procedures*.
90 JSP 440, *The Defence Manual of Security* abbreviates terrorism, espionage, sabotage, subversion and organised crime to TESSOC.

4.29. **Security intelligence.** Security intelligence is defined as: intelligence on the identity, capabilities and intentions of hostile organizations or individuals who are or may be engaged in espionage, sabotage, subversion, terrorism and organized crime.[91] Security intelligence covers intelligence support across the full range of terrorism, espionage, subversion, sabotage, organised crime and other security threats.

4.30. **Insider threat.** Defence personnel should pay particular attention to insider threats. The 'insider threat' comes from personnel who have privileged access to classified or official data and subsequently abuse this access to destroy, damage, remove or disclose the data. It also includes those personnel who have legitimate access to Defence facilities and use this access to conduct acts of terrorism or sabotage. Insider threats can potentially cause grave damage to information, resources and personnel and have a critical impact on operations.

4.31. **Threat assessment.** A threat assessment evaluates the range of identified threats and provides a basis to determine physical and operational mitigation measures for protection against those threats. Threat assessments should contain the following as a minimum: identification of the threat; the main intelligence judgements concerning the threat; and the degree of confidence in the assessment of the specific threat.

4.32. **Countering the threat to security.** All personnel involved in Defence business, including military, civilians and contractors, have a personal responsibility to counter the threat to security by applying good security behaviours.[92] At a higher-level, commanders and security staff have specific responsibilities and outputs.

a. **Commanders.** The ultimate responsibility for intelligence and security rests with the commander, who should be familiar with the intelligence and security processes and have sufficient situational awareness to articulate their critical information requirements. Commanders set the command climate regarding security and the security posture to be adopted in accordance with threat advice from security staff.

b. **Security staff.** The principal responsibility of security personnel is to advise commanders on security threats, including those assessed

91 NATOTerm.
92 See the *Defence Personnel Security Strategy* for further detail.

by counter-intelligence. Security staff manage and support operations to counter the security threats. Specifically they: collect, process, analyse and disseminate information related to counter-intelligence requirements; produce and disseminate current threat assessments; contribute to the operations security process, including the planning, coordination and application of protective security measures throughout the formation; establish and maintain liaison with civil law enforcement and counter-intelligence authorities; and ensure there is a clear classification guide and disclosure procedure that complies with the Defence security policy.

4.33. **Security – core principles.** Commanders are ultimately responsible for security. Additionally, security operations are conducted according to the following principles.

- There should be a single focus at each command level for security policy and incident reporting.
- Security teams must be established to engage threats and to give security advice to commanders at each level of command.
- Security operations must be coordinated and integrated with the intelligence effort, in consultation with the operations and other staff.
- The collection of security-related information should be coordinated at each level of command and integrated with the overall intelligence collection effort.
- Counter-intelligence and security threat warnings and assessments should be produced at the lowest possible security classification, and disseminated as widely as possible.

4.34. **Security awareness and education.** All individuals who have authorised access to classified material must be trained in the dangers to security arising from indiscreet conversations, relationships with the media, and the threat presented by hostile intelligence service activity. Individuals must be aware of the requirement to report any approach or manoeuvre that they consider suspicious or unusual.

4.35. **'Need-to-know'.** This describes the legitimate requirement of a prospective recipient of data to know, access or possess any sensitive

information represented by this data. The principle is that knowledge or possession of classified information should be strictly limited to those who are cleared to the appropriate security level and who clearly have a need-to-know to carry out their duties, regardless of rank or position. However, the responsibility to share information with coalition partners requires products to be written for release, balancing the need-to-know principle with the requirement to share.

> The threats to our security are complex and rapidly evolving as criminals, hackers, malicious insiders and hostile foreign states continually find new ways of staying one step ahead of us. … At the same time, we are continually creating new vulnerabilities as we adopt new technologies and new ways of working.
>
> Paul Martin, *The Rules of Security, Staying Safe in a Risky World*

Section 7 – Legal considerations in the employment of intelligence disciplines

4.36. The activities of the UK Armed Forces are subject to national and international law.[93] Intelligence activity conducted within the context of a military operation will have a legal dimension; there must be a legal 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 any Chief of Joint Operation's Operational Directive provides further guidance for specific operations. Intelligence activity must be consistent with 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 law (IHRL). To these may be added rights and obligations under United Nations (UN) Security Council resolutions or bilateral and multilateral agreements.

4.37. **Rules of engagement.** ROE, provided as part of a Chief of the Defence Staff's Directive, will specify the permissions and limitations under which forces undertaking any military operation will operate. They serve as a policy and operational guidance tool and must reflect and be consistent with the legal

93 JDP 0-01, *UK Defence Doctrine*, 6th Edition, paragraph 2.49.

framework of the operation. The creation of enabling ROE is a vital part of the direction function of the intelligence process. The responsibility for compliance with ROE is a command function. Use of covert actions and collection of biometric data must be authorised within an ROE profile for them to be undertaken on an operation. ROE may also restrict the use of some collection capabilities.[94] The formulation of ROE is a particular challenge for multinational missions, where the interpretation of international law obligations, domestic laws and policies of the contributing nations adds complexity. It is the responsibility of the operational commander to ensure, through consultation with the relevant operational higher authority (for example, the Permanent Joint Headquarters), that the ROE profile enables the desired intelligence activity.

4.38. **Legal framework.** All intelligence activity must be conducted within the correct overarching legal framework. Domestic law, international law (for example, the law of armed conflict (LOAC) or IHRL, such as the European Convention on Human Rights (ECHR)) may be applicable, as illustrated in Figure 4.2.

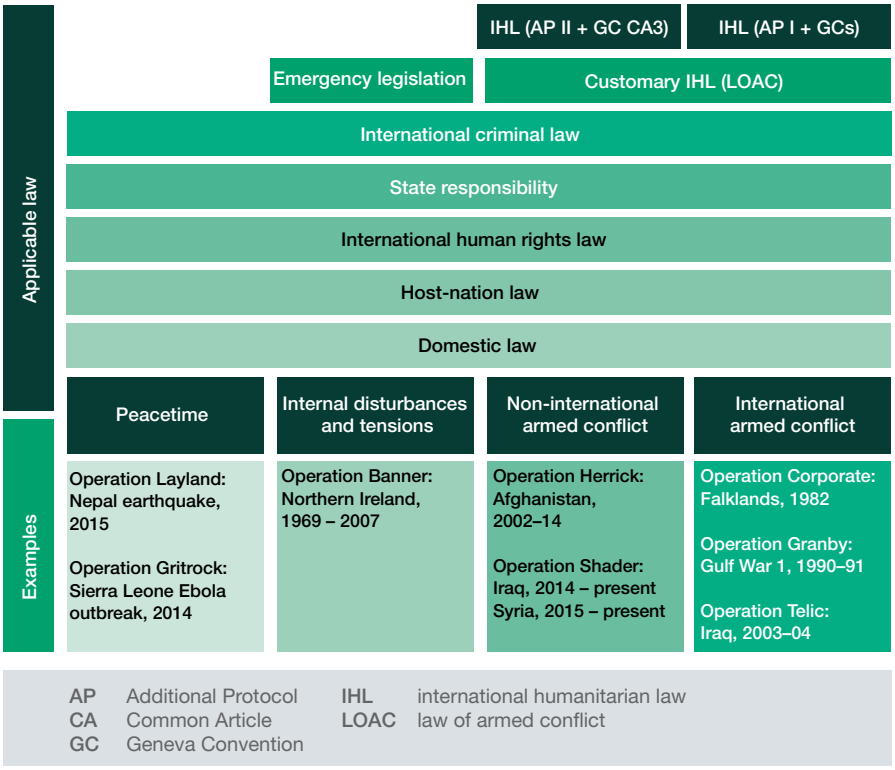


Figure 4.2 – Applicable law[95]

94 For example, an active collection radar system may be prohibited from use over a border.
95 See JDP 3-46, *Legal Support to the Joint Operations*, Chapter 2.

4.39. **International law.** In most operations of an international nature, the legal mandate will be founded in international law and if there is an armed conflict, it will involve the application of LOAC.[96] A conflict between states is an international armed conflict (IAC), whereas an armed conflict not between states (typically between governmental forces and non-governmental armed groups or between multiple non-governmental armed groups) is a non-international armed conflict (NIAC). The law relating to IACs is far more developed than NIACs, as set out in Figure 4.2. UK Armed Forces are directed, as a matter of policy, to apply broadly the same rules to a NIAC that they are legally bound to apply during an IAC.[97]

4.40. **International human rights law.** IHRL governs the obligations of states towards citizens and other individuals within their jurisdiction. The UK is bound by UN human rights treaties and the ECHR. The Human Rights Act gives effect to ECHR rights within UK law. The extraterritorial application of the ECHR and Human Rights Act has been the subject of extensive litigation in the UK domestic courts. ECHR jurisdiction is extended extraterritorially where: there is state agent authority and control (for example, in UK run detention facilities); or there is effective control over an area (for example, the UK is in occupation of an area or by exercising control in a specific area such as a checkpoint); or through '*espace juridique*' (i.e. where the territory of one convention state is occupied by the armed forces of another convention state).[98] With regards to state agent authority and control, this can arise as a result of: the acts of diplomatic and consular agents, through the exercise of public powers; or through the exercise of physical power and control over individuals (for example, custody).[99] However, its application on operations elsewhere and at other times remains subject to legal and judicial scrutiny. Other IHRL provisions may also be applicable to operations.

4.41. **Host-nation law.** Host-nation law may be a factor in identifying freedoms and constraints for intelligence activities. A status of forces agreement 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 the applicable host-nation law.

96 JSP 383, *The Joint Service Manual of Law of Armed Conflict*.
97 JDP 3-46, *Legal Support to Joint Operations*, paragraph 2.4.
98 See House of Lords, Al Skeini (2007) UKHL 26, 13 June 2007 and Jaloud v The Netherlands [2014] App. No. 47708/08.
99 See Al-Saadoon & Others v Secretary of State for Defence [2016] EWCA Civ 811.

4.42. **Domestic law.** When planning and conducting intelligence collection activity, adherence with relevant UK domestic law is essential to ensure both that criminal liability[100] does not arise and that activity is compatible with the UK human rights obligations. The following UK domestic law may be relevant to intelligence activity, but depending on the circumstances other laws may also apply.

a. **Bribery Act 2010.** In accordance with Section 1 of the Bribery Act 2010, a person (including a member of the UK Armed Forces) is guilty of an offence where they offer, promise or give financial or other advantage to another person intending to induce that person to perform a function improperly or to reward them for improper performance. It is a defence for a person charged with a relevant bribery offence to prove that the person's conduct was necessary for the proper exercise of any function of the armed forces when engaged on active service (i.e. an action or operation against an enemy, an operation outside the British Islands for the protection of life or property, or the military occupation of a foreign country or territory). Accordingly, where activity could amount to an offence under the Bribery Act the circumstances and necessity for that action must be effectively recorded.

b. **Computer Misuse Act 2010.** The Computer Misuse Act 2010 creates offences of unauthorised access to computer material and unauthorised modification of computer material. The offence of unauthorised access (hacking) is committed by a person who causes a computer to perform a function intending to secure unauthorised access to any program or data held in any computer. Unauthorised modification of computer material is committed when a person carries out an action which causes unauthorised modification of the contents of a computer intending to impair operation of a computer or program (denial of service attacks). Obtaining lawful authority for the activity in accordance with the Investigatory Powers Act 2016 (IPA) will ensure that it is lawful for all purposes, provided it is within the scope of the authorisation.

c. **Human Rights Act 1998.** UK intelligence activities must be compliant with UK obligations under the ECHR, which are enshrined within domestic law through the Human Rights Act 1998. These include, for example, the absolute right under Article 3, the prohibition

100 Through Section 42 of the Armed Forces Act, a person subject to Service law or civilian subject to Service discipline remains subject to the criminal jurisdiction of the law of England and Wales when operating in the UK or elsewhere.

of torture and inhuman and degrading treatment, which underpins captured persons (CPERS) activity and intelligence sharing. Of particular relevance to investigative intelligence activity is ECHR Article 8, which concerns the (qualified) right to private and family life and provides that there can be no interference by a public authority except as is necessary on one of the specified grounds. For the purposes of Defence, interference with the right to privacy needs to be in accordance with one or more of the legitimate aims prescribed in Article 8.[101] Compliance with relevant statutory provisions (see below) may, in the circumstances, demonstrate that the interference is in pursuit of a legitimate aim, is in accordance with the law and the activity is proportionate to the interference. The territorial extent of the Human Rights Act is in line with that of ECHR.

d. **Regulation of Investigatory Powers Act 2000.** The RIPA enables lawful use, by specified public authorities (including the UK Armed Forces), of covert investigative techniques, namely covert surveillance (intrusive and directed) and use of covert HUMINT sources. Under the 2021 Covert Human Intelligence Source Criminality Act, this may even include source activities that would be illegal unless authorised under RIPA. The RIPA authorisation process ensures that all-source activity satisfies the requirements of necessity (for example, on the grounds of national security) and proportionality, and is compatible with ECHR Article 8 (right to privacy). All Defence conduct amounting to covert surveillance or use of covert human intelligence source activity (including activity outside of the UK) must be appropriately authorised in accordance with MOD policy.

e. **Investigatory Powers Act 2016.** The IPA governs investigative activity relating to communications and communications data. It enables lawful interception of communications, equipment interference and other acquisition of communications data subject to a rigorous statutory regime for authorisation, oversight and accountability of such activities. Failure to comply with the IPA may incur criminal liability and/or amount to a breach of the UK's responsibilities under ECHR Article 8 and Human Rights Act (the right to privacy).

101 Defence could also rely on other grounds such as that the activity is necessary for the purpose of preventing or detecting serious crime.

f. **UK data protection legislation.** In the UK, data protection is governed by the Data Protection Act 2018 and UK General Data Protection Regulation. All collection, exploitation and sharing of intelligence must comply with UK data protection legislation, which includes provision for limited exemption only when required for national security or defence purposes. Commanders must ensure the legal framework for exploitation activities and information sharing is established before starting an operation or as soon as feasible thereafter.

g. **National Security Investment Act 2021.** This legislation enables the UK government to review transactions and investments on national security grounds. It applies to any acquisition of a 'material influence' in a company. It imposes a mandatory notification obligation where transactions involve specified activities in the energy, transport, communications, defence, artificial intelligence and other technology-related sectors. Defence will likely support the process by providing assessments. In addition to a risk over general information security, there is likely to be a significant risk of litigation as claimants seek to challenge any decisions.

h. **Copyright.** The Copyright, Designs and Patents Act (CDPA) 1988 gives creators of original work the right to control the ways in which their material can be used. The protection is automatic. While the CDPA 1988 does allow for limited use of copyright material for non-business purposes or private study, this exception does not apply when the purpose is to disseminate to more than one person at substantially the same time and for the same purpose. Consideration should be given as to whether material can be obtained from a Crown copyright source, under a MOD licence agreement or in accordance with a Public Domain Creative Commons License.

i. **Public records.** The Public Records Act 1958, as amended by the Public Records Act 1967, dealt with the release of government papers. The Acts provided that material would be released to the National Archives, initially after 50 years, before this was reduced to 30 years. The Freedom of Information Act 2000 substantially changed how government records are accessed. The position now is that records can be accessed from their creation unless they are subject to an exemption, which may be relied upon to prevent release.

Specific considerations

4.43. **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 staff should advise the commander to seek early legal advice.

4.44. **Captured persons.** One of the purposes of CPERS 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.[102] 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.[103] 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. These basic principles are to be applied at all stages of the CPERS process from point of capture to release or transfer. In an IAC, Geneva Conventions III (regarding prisoners of war) and IV (regarding the protection of civilians who are detained or interned) are of particular relevance. In a NIAC, Common Article 3 to the Conventions and Additional Protocol II apply. 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. UK personnel must treat CPERS humanely and conduct their detention and exploitation with all the protections provided by international and domestic human rights law. For more information see JDP 1-10, *Captured Persons*.

4.45. **Intelligence sharing.** In tandem with data protection law and policy are other MOD policies concerning the sharing of intelligence. Personnel should be aware of and apply the following.

a. **The Fulford Principles.** This policy relates to the detention and interviewing of detainees overseas and the passing and receipt of intelligence relating to detainees and is designed to ensure the

102 JDP 1-10, *Captured Persons*, 4th Edition, paragraphs 11.10 and 11.13.
103 See JDP 1-10, *Captured Persons*, 4th Edition, Chapter 2.

UK remains compliant with its human rights obligations. The policy enables UK Armed Forces to manage legal risk in respect of the International Law Commission's draft articles on state responsibility for internationally wrongful acts. Where a state aids or facilitates an internationally wrongful act (examples include murder, torture, extraordinary rendition or any treatment that is cruel, inhuman or degrading) through the sharing of intelligence, the aiding state can be held equally liable with the state that carries out the internationally wrongful act. In this context, the risk will most likely arise where actionable intelligence is shared (name, location, etc.). Any proposed sharing of intelligence must take into account the Fulford Principles.

b. **Overseas Security and Justice Assistance Guidance.** Similar to the Fulford Principles and linked to the International Law Commission's draft articles on state responsibility for internationally wrongful acts, this policy assists in ensuring that UK overseas security and justice assistance work meets the UK's human rights obligations and values. Where UK Armed Forces are engaged in capacity building, or case-specific activity (i.e. assistance may lead to individuals being identified, interviewed, investigated, apprehended, detained, prosecuted, ill-treated and/or punished by foreign authorities), this policy is likely to be engaged and needs to be adhered to.

Key points

- The main collection disciplines are: signals intelligence – principally, communications intelligence and electromagnetic intelligence; geospatial intelligence, including imagery intelligence; measurement and signature intelligence; human intelligence; and open-source intelligence.
- Analytical specialisms draw on specialist knowledge or expertise, for example: human factors analysis; human network analysis; and scientific and technical intelligence.
- All-source intelligence assessment is identified within Defence Intelligence as a unique analytical discipline, adding an additional layer of judgement to existing analysis to support the decision-making of the highest level customers in government.
- Multi-intelligence activities cover those military activities where multiple intelligence sources can be fused within a single organisation to create direct operational effects.
- Counter-intelligence assessments and investigations provide the commander with an understanding of the hostile intelligence service threat. In conjunction with security measures, this allows the commander to counter the threat with offensive and defensive measures.
- Intelligence activity conducted within the context of a military operation will have a legal dimension; there must be a legal basis for the activity and it must be conducted in a lawful manner.

Notes

Chapter 5

Chapter 5 explains intelligence support to joint operations, specifically describing the use of intelligence support to gain an understanding of the human and information environments, and support to targeting and to operations evaluation. Chapter 5 concludes with a review of different approaches to intelligence development and an introduction to problem-centric approaches.

> When information was a scarce commodity, it could be considered in similar ways as other vital commodities ... Acquiring and protecting high-quality information made it possible to stay ahead of opponents and competitors ... As more information began to be digitised ... and communications became instantaneous, the challenges became those of plenty rather than scarcity ... If they had bought into the idea that fast-flowing data streams could eliminate the fog of war, they could be in for a rude shock. Even without enemy interference, a fog could be caused by a superfluity of information – too much to filter, evaluate, digest – rather than the paucity of the past.
>
> Lawrence Freedman, *Strategy*

Chapter 5

Intelligence and counter-intelligence support to joint operations

Section 1 – Intelligence and operations across multiple operational domains

5.1. **Multi-domain integration.** Multi-domain integration (MDI) is a conceptual approach that seeks to better compete with our adversaries in an era of persistent competition. It seeks to generate advantage through integration across the three levels of operations (tactical, operational and strategic) and the five operational domains to create multi-domain effect that adds up to far more than simply the sum of the parts. MDI will highly likely include elements of more than one Service and may involve maritime (including amphibious), land, air, space, cyber and electromagnetic, and special forces. UK joint operations are commanded by the Joint Commander, Chief of Joint Operations (CJO), supported by the staff within the Permanent Joint Headquarters (PJHQ). PJHQ issues CJO's orders and direction through operational orders and fragmentation orders which synchronise and coordinate forces in the operational theatre or for a specific operation.[104] Operations spanning multiple operational domains are an evolution of joint operations, reflecting the introduction of the space, and cyber and electromagnetic domains.

5.2. **Joint operations area.** Operations may be conducted in a designated joint operations area (JOA).[105] The term JOA represents the area of land, sea and airspace defined by a higher authority in which a joint task force commander plans and conducts military operations to accomplish a specific mission.

104 See also Joint Doctrine Publication (JDP) 0-01, *UK Defence Doctrine*, 6th Edition, paragraph 3.9 for detail on component commanders.

105 The term joint operations area is defined in Allied joint doctrine as: a temporary area within a theatre of operations defined by the Supreme Allied Commander Europe, in which a designated joint task force commander plans and executes a specific mission at the operational level. NATOTerm.

5.3. **Focus of operational intelligence and operational intelligence planning.** Operational intelligence provides commanders with the information and analysis to make decisions and contributes to the planning and execution of operations within the JOA. Additionally, operational intelligence staff are responsible for: joint intelligence preparation of the operating environment (JIPOE) and other associated inputs to the operational estimate process; planning and refining intelligence personnel structures; designing intelligence architectures and flows; and integration with the Defence single intelligence environment, partners across government, Five Eyes partners and allies.

5.4. **Joint intelligence areas.** To enable the focusing of the intelligence effort, the JOA is divided into two areas – the area of intelligence responsibility and the area of intelligence interest. These are explained below.

a. **Area of intelligence responsibility.** The area of intelligence responsibility is defined as: a geographical area allocated to a commander, in which the commander is responsible for the provision of intelligence.[106] It encompasses the area in which adversary actions can directly affect the commander's forces and to which the commander can respond using available 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 defined as: a geographical area for which commanders require intelligence on the factors and developments that may affect the outcome of operations.[107] The commander is not responsible for intelligence capability in the area; however, higher or neighbouring formations should provide answers to the 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 the commander is not required to respond with their assets. The area need not be geographically next to each other and there may be areas outside the main area of intelligence interest that could exert influence on the JOA.

106 NATOTerm.
107 NATOTerm.

Section 2 – Analysis of the human and information environments

5.5. Analysis of the human environment has traditionally focused on understanding areas such as cultural practices, societal norms, beliefs and values, and social, political and economic organisation. At the operational level, human terrain analysis focused on conflict drivers across the three levels of operations, likely adversary actions (and how these could be targeted) and how our own actions would have impact (and how this may be mitigated if required).

5.6. Integrated action now requires a much greater understanding of audiences to inform all aspects of planning. An audience is defined as: an individual, group or entity whose interpretation of events and subsequent behaviour may affect the attainment of the end state.[108] To gain an understanding of the drivers of instability and audience behaviours, a human security analysis[109] should be conducted and maintained, alongside audience and human factors analyses. The information environment must also be considered, with intelligence staff making a significant contribution to enabling the understanding that provides the focus for planning and execution of information operations activity. Commanders who understand the strategic narrative can then request target audience analysis (TAA) to identify the effects that they wish to create. Working with information operations staff, intelligence personnel will also consider potential negative influence outcomes in particular audiences, including those not deliberately targeted, when developing courses of action.

Human environment

5.7. **Audience analysis.** Audience analysis[110] represents the fusing of foundation military intelligence (human terrain analysis, human terrain mapping, sociocultural analysis), human security,[111] stakeholder analysis and audience segmentation. Audience analysis is defined as: the understanding and segmentation of audiences in support of the achievement of objectives.[112] This

108 NATOTerm.
109 See Joint Service Publication (JSP) 985, *Human Security in Defence*.
110 See also Joint Tactics, Techniques and Procedures (JTTP) 3.81, *Integrated Action: An operational level guide to the audience-centric approach for commanders and staff*, Edition 3.
111 Within human security, this includes consideration of how and why individuals and groups are discriminated against by society and/or the adversary or as a result of conflict. This allows us to develop an understanding of how conflict impacts men, women, boys and girls differently and what can be done to mitigate this.
112 NATOTerm.

informs joint operations by providing a deeper understanding of all persons affected by and influencing an operation. Commanders and staff should work out how to synchronise and orchestrate all the relevant levers to impart effects onto the audience to achieve the outcome. Once this process has taken place, it is important that there is an assessment of whether the intended effects were created as expected and whether there were any unintended consequences. To mitigate negative second and third order consequences of military activity, audience analysis also identifies all audiences who will be impacted by activity, regardless of whether they were the intended target. Understanding audiences, their influences and perceptions is therefore intrinsic to the intelligence picture. Audiences are segmented into three general categories – public, stakeholders and actors – depending on their ability to affect our outcomes. This is illustrated in Figure 5.1.

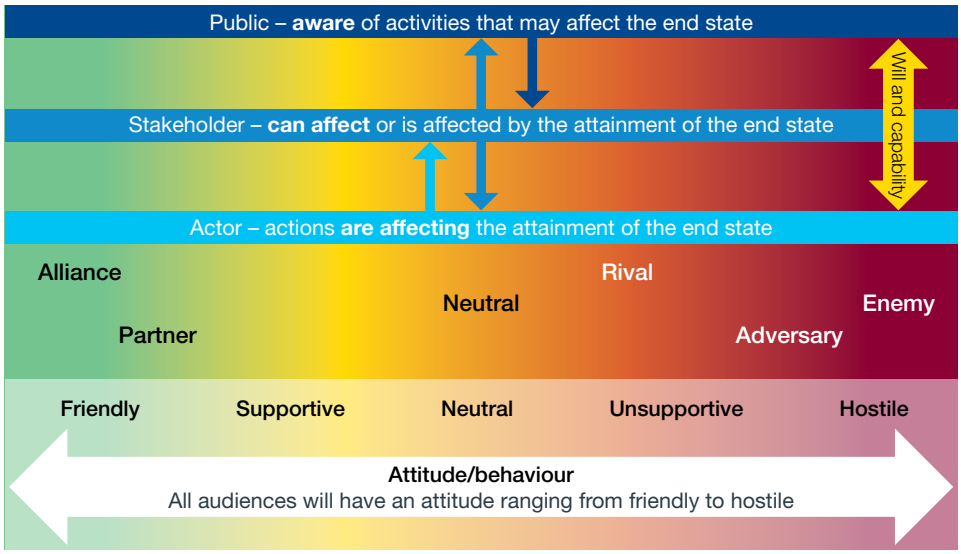


Figure 5.1 – Audience-centric approach

a. **Public.** A public audience is defined as: an individual, group or entity who is aware of activities that may affect the attainment of the end state.[113] The public's attitude may range from hostile to supportive.

b. **Stakeholder.** A stakeholder is defined as: an individual, group or entity who can affect or is affected by the attainment of the end state.[114] Our activities may encourage or develop supportive stakeholders to

113 NATOTerm.
114 NATOTerm.

become partners, whilst discouraging or denying unsupportive or hostile stakeholders from becoming actors.

c. **Actors.** An actor is defined as: an individual, group or entity whose actions are affecting the attainment of the end state.[115] The spectrum of actors is further underpinned by attitude and behaviours: these may be friendly, supportive, neutral, unsupportive or hostile. Audience analysis is required to understand points of influence that may change or reinforce attitudes or behaviours. Changes in behaviours may be because of persuasion, or be short-term, because of coercion. It must be remembered that the position of individuals and groups within the range of audiences is not fixed and therefore the requirement for audience analysis is enduring. Table 5.1 details the spectrum of actors.

Name	Description
Alliance	The relationship that results from a formal agreement between two or more nations for broad, long-term objectives that further the common interests of the members.
Partner	An actor belonging to a declared, presumed or recognised friendly nation, organisation, faction or group sharing a common goal.
Neutral	An actor whose characteristics, behaviour, origin or nationality indicate that it is neither supporting nor opposing either side.
Rival	Actors who are competing with another actor for the same objective for advantage without hostile intent and compete in accordance with the rules-based international order. Rivals are usually found in the rivalry zone of the continuum of competition.
Adversary	An actor whose intentions or interests are opposed to those of friendly parties and against which legal coercive political, military or civilian actions may be envisaged and conducted. They may have many different motivations and may be subject to a broad range of influences and are usually found in the confrontation zone of the continuum of competition.
Enemy	An actor whose actions are hostile and against which the legal use of armed force is authorised.

Table 5.1 – Spectrum of actors[116]

115 NATOTerm.
116 See Allied Joint Publication (AJP)-01, *Allied Joint Doctrine* (with UK national elements), Table 4.1.

5.8. **The conceptual model of audience analysis.** Whilst Allied joint doctrine refers to TAA, Defence has identified three conceptual layers of audience analysis to support integrated action. These are baseline audience analysis (BAA) and mission audience analysis (MAA), which lead to TAA.[117]

a. **Baseline audience analysis.** BAA is defined as: the foundational level of audience analysis to support planning and inform mission and target audience analysis.[118] This is the underpinning analysis of audiences on which MAA and TAA can be based.

b. **Mission audience analysis.** MAA is defined as: the focused understanding of target audiences in support of a mission or task to create the desired planning effect.[119] MAA provides the depth and scope to support operational-level planning.

c. **Target audience analysis.** TAA enables commanders to identify the effects they want to create; it also helps them identify the risk of creating any unintended effects. TAA is defined as: the focused examination of targeted audiences to create desired effects.[120] TAA is an all-source process that uses psychological, anthropological and sociocultural methods to analyse state and non-state entities.[121]

5.9. **Human security.** A human security approach should consider a broad range of security and protection challenges that individuals and groups of people face in situations of conflict, instability and insecurity from their perspective, and how military operations may affect their security in the short, medium and long term. Any adverse impacts on the human security of local populations resulting from operations may have second or third order consequences that work counter to our objectives. Human security considerations include human security factors and cross-cutting themes that the intelligence staff will be required to make sure the commander understands.[122]

117 JTTP 3.81, *Integrated Action: An operational level guide to the audience-centric approach for commanders and staff*, Edition 3, pages 15–16.
118 JDP 0-01.1, *UK Terminology Supplement to NATOTerm*.
119 JDP 0-01.1, *UK Terminology Supplement to NATOTerm*.
120 NATOTerm.
121 JSP 900, *UK Full Spectrum Targeting Policy*, Edition 5.
122 Human security factors include: personal/physical, political, food, health, environment/climate, economy, cultural and information. Cross-cutting themes include: protection of civilians; women, peace and security (including conflict related sexual violence and, sexual exploitation and abuse); children and youth affected by armed conflict; modern slavery and human trafficking; building integrity (countering corruption); preventing and countering state and non-state adversaries; and cultural property protection.

> The biggest of the big ideas that guided strategy during the surge was explicit recognition that the most important terrain in the campaign in Iraq was the human terrain – the people – and our most important mission was to improve their security.
>
> General David H. Petraeus

5.10. **Enduring factors within the human environment.** Understanding the human environment 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. There are multiple possible approaches but some of the enduring factors that must be considered are as follows.[123]

a. **Culture.** This includes beliefs and values, ideology and psychology. Groups have shared beliefs and values that ensure the loyalty of members to the group. These may include formal ideologies or religions, informal or non-codified beliefs about the nature of the world and of society, honour and loyalty. Concepts of time and the significance of history also influence how individuals or groups may act. Ideology typically refers to common ideas, language, rituals and theories providing a common bond for communities such as tribes and religious and ethnic groups. Assessments of psychology involve analysing the mental and emotional state and behaviour of individuals or groups; it concerns their motivations, fears, attitudes and perceptions, and how these factors impact on their decision-making.

b. **Gender.** A gender perspective refers to assessment of gender-based differences between men and women as reflected in their social, economic and political roles and interactions, and in the distribution of power and access to resources. In many societies, power and decision-making bodies are dominated by a particular demographic and this is often male; this includes senior positions in academia, health care, media, the military and government. Therefore, a population analysis that does not disaggregate data by sex may be missing the female context and, for example, their leadership roles in communities. Understanding the gendered context provides insight into the movements, behaviours

123 See JDP 04, *Understanding and Decision-making* and AJP-10.1, *Allied Joint Doctrine for Information Operations* (with UK national elements).

and patterns of life for men, women, boys and girls and can highlight particular gendered vulnerabilities, drivers of conflict and gender-related early warning indicators. A gender perspective must be applied across the human terrain, such as understanding the differing gendered impact of religious and cultural practices and the social, economic and political organisation of society. Successful engagement with, and understanding of, men and women's roles and responsibilities in society allows a more detailed and complete picture of the population.

c. **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. Examples include family structures and kinship, language, history and religion. 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.

d. **Institutions and organisations.** Power, politics, religion and economies work in different ways in different societies. The political system within a population may include global, regional, national and provincial systems, but not all groups need or want the state to organise them. The role of the military within a society, its relationship with the political organisation and allegiances can also vary. Large-scale economic ideologies such as capitalism or socialism have economic institutions and approaches that influence how people earn a living and obtain the things they need; however, societies may also have alternative economic structures, such as the shadow economy or bartering, or networks of patronage. Understanding how economic structures work is necessary for any operations involving or supporting economic development. Furthermore, the significance of religion within a society and the relationship between religious bodies and political and judicial structures can vary.

e. **Technology and infrastructure.** Analysing the technology and infrastructure used in everyday life will assist in understanding how the environment is shaped by communities to suit their requirements. This includes physical items, such as communications equipment and infrastructure, utilities and transportation. Analysing technology must consider the level of scientific and technical development and supporting infrastructure.

A long-range reconnaissance patrol gathering information to help the United Nations better understand how to help the people of Mali

f. **Physical locations.** It is important to understand the physical locations where people live. Assessments should consider the terrain, climate, access to resources, employment structures and the collective impact those factors have on how people live and the importance of specific areas and locations or activities.

5.11. **Human factors analysis tools.** Analysis of the human factors of relevance to the operating environment is known as human factors analysis. Several frameworks exist to conduct this analysis, but one of the most commonly used approaches involves assessing political, military, economic, social, infrastructural and informational (PMESII) factors.[124] Consideration of additional elements may be desired, for example, PMESII and physical and time (PMESII-PT). Another approach, for example, looks at area, structures, capabilities, organisations, people and events (ASCOPE). PMESII is a baseline tool and it does not cover the full complexity of human activities, but it can be thought of as an initial stage of the analysis required to generate deep understanding of the human environment that will be necessary if we are planning for human effects and actions.[125]

124 AJP-10.1, *Allied Joint Doctrine for Information Operations* (with UK national elements), paragraph 4.11. See also Chapter 7, Section 3 of this publication for detail on PMESII as part of intelligence support to operations planning processes.

125 For example, PMESII/ASCOPE is included in the British Army's *Planning and Execution Handbook* as the precursor to the human terrain overlay during question one of the combat estimate.

5.12. **Virtual identity.** A 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; for example, an online gamer known online only by their cyber persona or where a group of gamers have a single virtual persona. Actors may operate in the virtual world creating online identities to hinder tracing or pursuit. Some adversaries may undertake subversion or terrorism in the real world in keeping with their online identities, effectively giving them the capacity to commit violent acts they would not normally have contemplated.

Information operations

5.13. **Information operations and the information environment.** The conduct of information operations is detailed in Allied Joint Publication (AJP)-10.1, *Allied Joint Doctrine for Information Operations* (with UK national elements). The information environment itself is segmented into three dimensions – cognitive, physical and virtual – as illustrated in Figure 5.2.[126]

- **Cognitive** – this dimension is where cognitive effects affect people's thinking, which influences their behaviour and decision-making.
- **Physical** – this dimension comprises the geographic areas where audiences live, including all physical objects and the infrastructure that supports them.
- **Virtual** – this dimension comprises the space in which audiences interact virtually; the most significant aspects within this dimension are virtual personas, the infrastructure, and information and data exchange.

126 AJP-10.1, *Allied Joint Doctrine for Information Operations* (with UK national elements), Chapter 4.

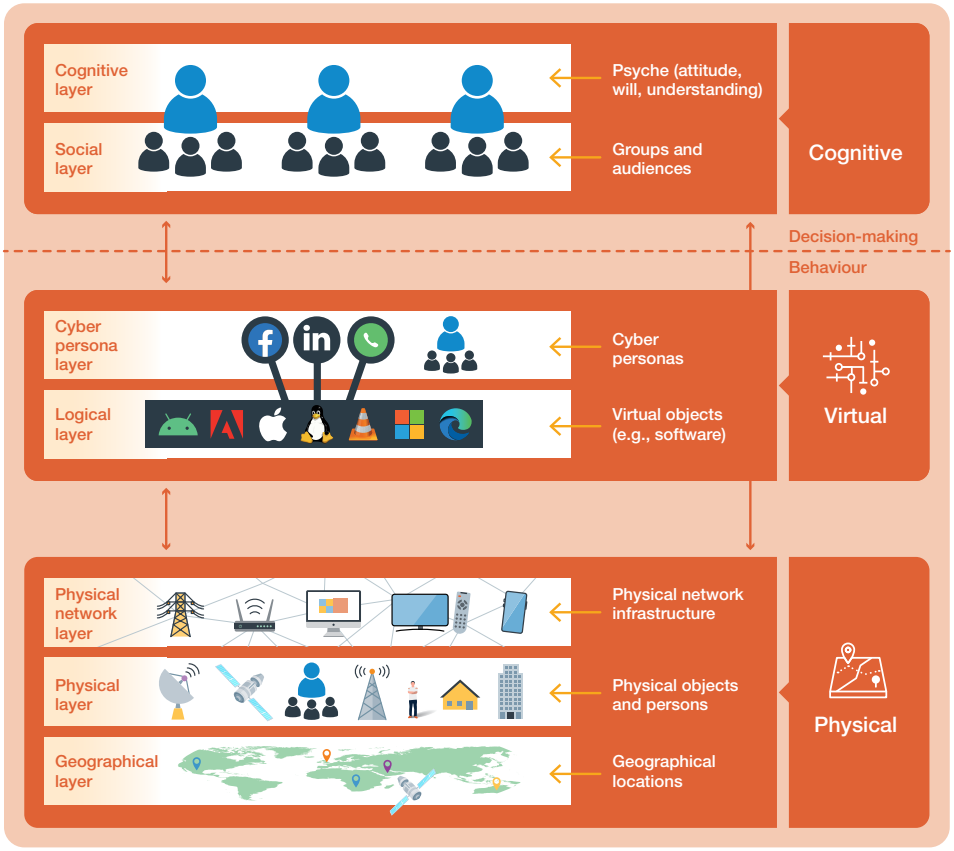


Figure 5.2 – The information environment[127]

5.14. **Intelligence support to information activities.** An information environment assessment (IEA) is conducted by information operations staff but they will use the intelligence baseline analysis, human factor and audience analyses in addition to the intelligence staff's JIPOE. This analysis and subsequent audience analysis product, such as an audience intelligence pack or target intelligence pack, informs the commander and bridges the gap between traditional J2 (intelligence) and actionable intelligence.

127 AJP-10.1, *Allied Joint Doctrine for Information Operations* (with UK national elements), Chapter 4.

Section 3 – Intelligence support to targeting

5.15. **Targeting.** Targeting is defined as: the process of selecting and prioritizing targets and matching the appropriate response to them, taking into account the operational requirements and capabilities.[128] Joint Service Publication (JSP) 900, *UK Full Spectrum Targeting Policy* is the policy document that must be followed. Targeting can be broadly divided into two types: deliberate and dynamic.

- **Deliberate targeting** – targeting conducted against targets identified and located during the planning phase of operations and intended to be prosecuted on either a scheduled or on-call basis.[129]

- **Dynamic targeting** – targeting conducted against targets known to exist, but which were not detected, located or selected for action in enough time to be included in the deliberate process.[130]

5.16. **Intelligence support to targeting and effects.** Intelligence is a critical enabler of the targeting process and is required throughout the whole targeting cycle to ensure that decisions are made considering the most up-to-date information and context.[131] A sound intelligence foundation is fundamental for the delivery of targeting; timely, accurate and relevant intelligence inputs are required throughout the targeting cycle across the physical, virtual and cognitive dimensions. All-source intelligence staff will request and coordinate inputs from across Defence, allies and others to provide appropriate prioritisation. They provide the understanding of the adversaries, identify criticalities in adversary systems through the target systems analysis and TAA processes, and also lead the validation of targets at target validation boards. They further support advanced target development and the application of full-spectrum effects. There is also significant intelligence work to support collateral damage effects and/or understand other collateral effects. Planning for targeting assessment, support to battle damage assessment and measuring effectiveness should be refined and appropriate collection and assessment plans completed for execution alongside the targeting activity.

128 NATOTerm.
129 JSP 900, *UK Full Spectrum Targeting Policy*, Edition 5, Part 1, paragraph 1.16.
130 JSP 900, *UK Full Spectrum Targeting Policy*, Edition 5, Part 1, paragraph 1.17.
131 JSP 900, *UK Full Spectrum Targeting Policy*, Edition 5, Part 2, page 1-1.

Section 4 – Intelligence support to operations evaluation

5.17. **Evaluation.** In the operational context, evaluation is the observation and interpretation of progress towards desired conditions against selected criteria. It draws on monitoring, which is essential to establish an initial baseline.[132] Evaluation allows commanders and their staff to develop insight on successes or failures so that they can make decisions on whether to continue on the same trajectory or to change course.

5.18. **Intelligence support to evaluation.** The evaluation of operations is activity usually led by J5 Plans staff, with J2 staff having a supporting role. From an intelligence perspective, the evaluation of operations typically comprises the following.[133]

a. **Assessments of effectiveness.** A measure of effectiveness is defined as: a criterion used to assess changes in system behaviour, capability, or operating environment, tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect.[134] Assessments of effectiveness examine whether the operation is achieving its purpose. They monitor and assesses progress, including setbacks, to support planning decisions.

b. **Assessments of performance.** A measure of performance is defined as: a criterion that is tied to measuring task accomplishment in order to assess friendly actions.[135] In partnership with other staff branches, intelligence staff at strategic and operational levels may be required to produce assessments that provide the commanders with agreed measures of performance. The focus for the intelligence staff will be the impact of joint operations. 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 over an adversary).

c. **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

132 See Chapter 3, Section 4.
133 Measurement of activity is also undertaken but should not require J2 support.
134 NATOTerm.
135 NATOTerm.

assessment of damage resulting from the application of lethal or non-lethal force against an entity.[136] Such assessment is supported by intelligence staff, but links into the targeting process. The production of battle damage assessments will generate a series of post-attack intelligence requirements.

d. **Measurements of combat power and combat effectiveness.** The evaluation of operations may also include measurements of combat power and combat effectiveness. Assessments of combat power are more objective than assessments of combat effectiveness, in which subjective elements such as leadership and morale are considered. Combat effectiveness can be challenging to assess in a timely manner due to the requirement for collection discipline access, especially, for example, when collection might most appropriately be undertaken using human or signals intelligence. Combat power and combat effectiveness are defined as follows.

- **Combat power:** the total means of destructive and/or disruptive force which a military unit/formation can apply against the opponent at a given time.[137]

- **Combat effectiveness:** the ability of a unit or formation, or equipment to perform assigned missions or functions.[138] Note: this should take into account leadership, personnel strength, the state of repair of the equipment, logistics, training and morale and may be expressed as a level or percentage.

e. **Intelligence assessments.** Intelligence assessments are critical to supporting decision-makers at all levels. In the context of intelligence support to operations evaluation, intelligence assessments have particular relevance in enabling the commander to measure progress towards mission accomplishment. They can 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 their assessments must be coherent across the joint task force. To ensure coherence, the commander and staff design and agree measurements and assessments during the operations planning process. Assessments

136 NATOTerm.
137 NATOTerm.
138 NATOTerm.

provide the information on campaign progress required before further higher-level and strategic decisions are made. Therefore, the joint task force commander must ensure that higher-level commanders understand the assessment system. Example measurement and assessment criteria may include: adversary capabilities, vulnerabilities and intentions; the impact of the results of elections or death of a key leader; economic progress; or the provision of basic services, such as medical care and utilities.

Section 5 – Approaches to intelligence development

5.19. Intelligence professionals are responsible for producing intelligence to assist policymakers and military commanders in making decisions in response to complex problems. A traditional approach is to use a linear and target-focused process, predominantly sequenced in the direction, collection, processing and dissemination (DCPD) order introduced in Chapter 3. An alternative approach described here is the problem-centric approach. This section provides an overview of both approaches, and they are explained in greater detail in Joint Doctrine Note 1/23, *Intelligence, Surveillance and Reconnaissance*.

Traditional and problem-centric approaches

5.20. **Linear approach.** Traditional approaches to intelligence collection and processing are largely target-centric, whether against physical locations, electromagnetic signatures, individuals or objects. Targets are typically well-defined, predictable adversaries with a known doctrine.[139] A predetermined collection plan is used to focus individual collection assets to collect on a part of an overall problem. The resultant information is then exploited by skilled analysts in a particular intelligence discipline. This exploited data is then disseminated in a report and often used by other analysts, usually all-source specialists, who combine several reports from different disciplines into a single understanding of a situation to satisfy the original intelligence requirement.

139 Patrick Biltgen and Stephen Ryan, *Activity-based intelligence – Principles and Applications*, 2016, pages 10–11.

5.21. **Problem-centric approach.** A problem-centric intelligence development takes a different approach. It task organises intelligence and intelligence, surveillance and reconnaissance (ISR) capabilities around specific problems, rather than disaggregating elements of the problem across numerous, often disconnected ISR and analytical capabilities and then attempting to re-aggregate individual outputs from these sources, sensors and agencies. The problem-centric approach is therefore fundamentally about the task organisation of the full range of intelligence and ISR capabilities necessary to deliver a required outcome. Problem-centric intelligence also differs from the linear approach in that the processing, exploitation and dissemination (PED) phases of the ISR process and the process phase of the intelligence cycle are merged. Rather than numerous, linear PED and analysis processes occurring independently within a hierarchical multi-stage approach, all data, information and intelligence is pooled for all analysts to work on concurrently and collaboratively. Most significantly, it creates a direct command relationship between those that are conducting exploitation and analysis, and those that are collecting and processing. Collection and processing is task-organised to deliver the information and data needs that the exploitation and analytical capability require to meet the outcome required.

Activity-based intelligence

5.22. An activity-based intelligence (ABI) methodology is a means of enabling a problem-centric approach. ABI promotes the exploitation and analysis of all data rather than the analysis and fusion of end product reporting derived from data. It is an analytical methodology that seeks to integrate data from multiple sources by identifying entities and activities to discover the relationship between entities and surface patterns in activity. It then characterises those patterns to drive further collection and create decision advantage. ABI is a series of analytic methods. It is an inherently source agnostic, data-driven approach to intelligence that relies on a shift to Information Age thinking where data is integrated and exploited in a fundamentally different way. ABI aims to take all the gathered data, process the full range of permitted collected data and analyse it with a deductive approach. Importantly, data fusion takes place at the stage of gathering the information, not in the assembling of analysis for the final product or output. An ABI approach is predicated on both answering directed questions but also discovering what is important, even if the wrong question, or no question, has been asked – often referred to as 'unknown-unknowns'.

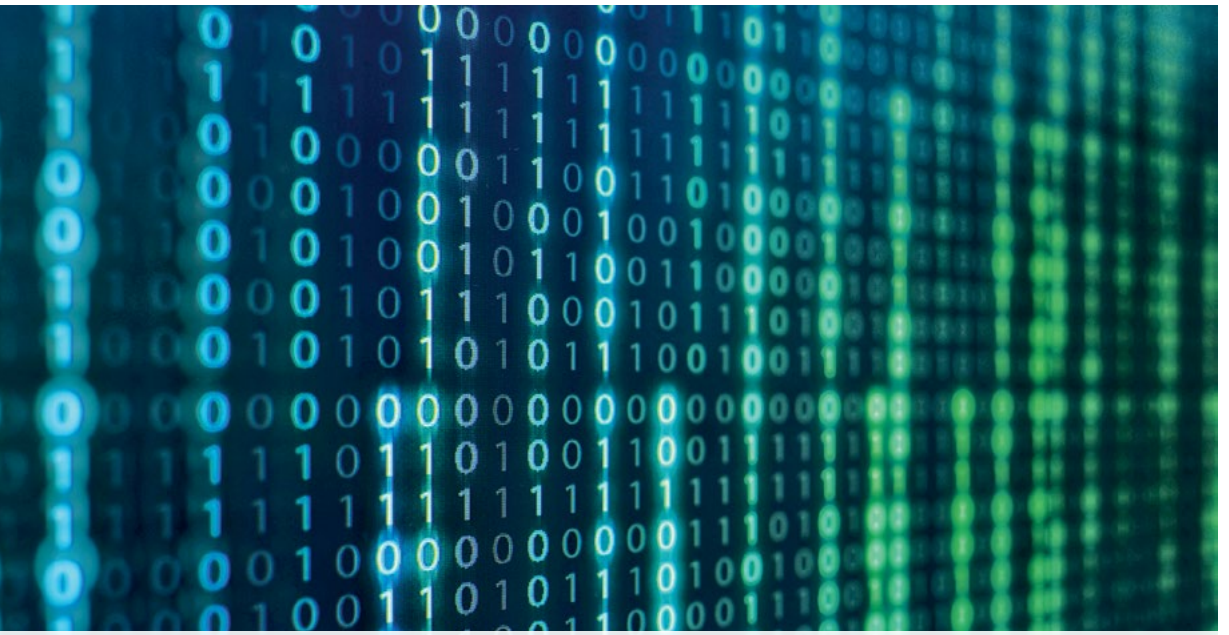
5.23. **ABI principles.** ABI is underpinned by four principles. These are:[140]

- **geo-reference to discover** – focusing on spatially and temporally correlating multi-intelligence data to discover key entities, transactions and patterns;
- **data neutrality** – regardless of the source, all data is valuable;
- **sequence neutrality** – data analysis is governed by correlation rather than causation – it is also the case that existing data often holds the answer to a question before it has been asked; and
- **integration before exploitation** – correlate data as early as possible because seemingly disparate, unimportant data points in a single intelligence may be important when integrated across multi-intelligence.

5.24. **Supporting analytical constructs.** There are two further essential processing developments supporting ABI: structured observation management (SOM) and object-based production (OBP). SOM and OBP are associated activities. SOM provides a common methodology and language for how objects and events are described and characterised. OBP uses these common descriptions and is the mechanism by which SOM observations are packaged and provided for analysis as individual data objects, for example, detected objects or events.

5.25. **ABI – applicability.** ABI as a methodology saw significant development during coalition counterterrorism and counter-insurgency operations in Iraq and Afghanistan.[141] It is a tradecraft focused on discovering the unknown, is well suited to advanced multi-intelligence analysis of non-traditional threats in a big data environment, and it can assist in undertaking an audience-centric approach. Whilst ABI has broad applicability across all intelligence problem sets, the traditional approach is limited to traditional problems. While an ABI-oriented system and processes can be quickly adapted to address traditional problems, traditional approaches are not as easily adapted or transformed.

140 Patrick Biltgen and Stephen Ryan, *Activity-based intelligence – Principles and Applications*, 2016, page 9.
141 Patrick Biltgen and Stephen Ryan, *Activity-based intelligence – Principles and Applications*, 2016, page 6.



Automation of processes within the processing, exploitation and dissemination of information and data is an ongoing area of intelligence capability development

Artificial intelligence, machine learning and human-machine teaming

5

5.26. Data science, machine learning and artificial intelligence are a series of technologies that support the ability of machines to undertake tasks normally requiring human involvement. In particular, PED is currently generally human-driven and the automation of some of this activity in conjunction with human-machine teaming and the use of algorithms will enable data to be processed more quickly. Additionally, with the right data and algorithms, artificial intelligence could enable 'prediction' ahead of events occurring. Machines can already either surpass or supplement human activity in some areas, for example, recognising objects in a photograph, translating foreign text into English, generation of text by large language models, intelligent search of vast numbers of documents and in transcribing audio information. Data science, machine learning and artificial intelligence approaches will continue to be developed through ongoing intelligence data exploitation programmes.

Key points

- Within audience analysis, it is important to analyse the audiences that will be impacted by an action, not just those we intend to target, to mitigate negative second and third order consequences that may impact on operational or strategic success.
- Analysis of the human and information environments must consider the human security issues that individuals and groups of people face, including across genders.
- Operations evaluation is led by J5 Plans staff but requires J2 support for measuring effectiveness, battle damage assessment and for providing intelligence reporting.
- As well as the traditional linear approach to intelligence development, problem-centric approaches provide an alternative model and approach.

Chapter 6

Chapter 6 explains the role and specific responsibilities of the joint commander and the intelligence staff. It also describes the joint operational and deployed intelligence architectures.

> To lack intelligence is to be in the ring blindfolded.
>
> General David M. Shoup,
> Former Commandant of the
> United States Marine Corps

Chapter 6

Underpinning joint intelligence: people, structures and training

Section 1 – The commander, intelligence and decision-making

6.1. **Commander's responsibilities.** The ultimate responsibility for intelligence rests with the commander. The commander should be familiar with the intelligence process and be able to articulate their critical information requirements to the intelligence staff. At all levels, the relationship between commanders and their staff is critically important for effective decision-making. Commanders provide the leadership, judgement and energy to focus the staff and the forces under their command towards the goal of accomplishing the mission. Commanders are the critical individuals in the planning and conduct of intelligence activities. They organise and assign their own staff, configuring them to meet their information, intelligence and operational requirements. It is the commander's responsibility to: provide direction and guidance; define priorities; resource intelligence collection and production effectively; demand the highest standard of products; and review the effects of their chosen actions to ensure they comply with the law with regard to intelligence activities.[142]

6.2. **Commanders and decision-making.** The commander provides direction and guidance to the staff to conduct their activities to generate the outputs required to support decision-making. Intelligence staff assist in making sure the commander understands the operating environment to enable intelligence-based decisions. Effective decision-making combines judgement with information; it requires knowing whether, when and what to decide. Mission analysis highlights gaps in information and intelligence, including that which is critical for the commander's subsequent decisions.

142 See Chapter 4, Section 5 and Allied Joint Publication (AJP)-2, *Allied Joint Doctrine for Intelligence, Counter-intelligence and Security*, Chapter 2, Section 2.7, for more detail on legal compliance requirements.

6.3. **Promoting access to intelligence.** A challenge for commanders is to focus the intelligence effort and achieve timely dissemination consistent with respective national disclosure policies. This includes ensuring the exchange of intelligence among all echelons and components. Access to intelligence capabilities to support mission requirements should be prioritised by need and established authorisation not restricted by organisations or command configurations. If a higher priority or competing tasks affect optimisation of intelligence activities, commanders should make alternative provision from within their assigned resources and/or request assistance from other agencies through their chain of command.

6.4. **Operations design.** Intelligence fits extensively into the operations design process. Operations design results in describing ends, ways, means and risks to take to create effects, achieve objectives and attain the end state.[143] Intelligence staff contribute to the development of operations design by providing intelligence, enabling the commander's understanding of the adversary, other audiences and the wider operating environment to answer the commander's critical information requirements.

6.5. **Support to contingency planning.** In the military context, contingency planning means developing plans for potential military operations.[144] The starting point for all contingency plans is to develop an understanding of the operational environment and the nature of the potential problem through the joint intelligence preparation of the operating environment (JIPOE). The intelligence staff will provide the commander with this understanding and identify gaps and associated intelligence requirements to drive the intelligence requirements management and collection management process. The JIPOE will provide the foundation data that is required when activating or revising contingency plans.

6.6. **Informing commanders.** To maintain the initiative, commanders will seek to make decisions quickly. This requires the ability to assess the adversary's decision-making cycle, identify opportunities for exploitation and to disseminate critical information. Intelligence directly supports commanders by producing assessments and reports that aid decision-making in the context of the likelihood of adversary courses of action.

143 AJP-5, *Allied Joint Doctrine for the Planning of Operations* (with UK national elements), Chapter 3, paragraph 3.1.

144 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. NATOTerm.

6.7. **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.

6.8. **Command–intelligence failures.** The relationship and trust developed between a commander and their intelligence staff is a critical component of operational success. There are numerous examples through history where the breakdown of this relationship has led to operational failure. Defining intelligence failure is difficult, with many theories trying to explain it, however, it remains that failure can happen at each core function of the intelligence cycle and at the interaction between the core functions. The actions and behaviours of commanders at all levels set the environment in which these core functions exist, so it is relevant to examine how the commander interacts with them.

a. **Direction.** When tasking intelligence, the start point is often one of a lack of understanding. The reason for tasking is that the command does not know something and seeks understanding; however, a lack of understanding may mean that the wrong question is initially asked. A perfect intelligence product answering the wrong question will not lead to operational success.

b. **Collection.** Despite the incredible advances of technology in intelligence, collection will only ever provide a glimpse of the totality of the information available and it is not possible to ensure that what is collected is valid and free from adversary deception. The processes and procedures within a headquarters and subordinate organisations may also prevent efficient flows of information both upwards and downwards, leading to delays. Commanders must be prepared to operate in uncertainty and understand that a perfect view of the adversary's capabilities and intent is impossible to achieve. More collection does not always lead to greater understanding or better decision-making; indeed, it can also hinder it.[145]

c. **Processing.** Analysis is an act of judgement under conditions of uncertainty and is subject to imperfect reasoning. Commanders will always develop their own analysis and conclusions about events, but they must resist the temptation to become 'their own chief analyst' at the expense of finished, all-source analysis. They should encourage

145 Min Zheng, et al., 'How Causal Information Affects Decisions', *Cognitive Research Principles and Implications*, 2020, Volume 5, Number 1.

sharing and cooperation amongst the teams within their headquarters to ensure intelligence production meets the demands of the staff. Analysts must in turn understand the commander's ways of thinking and other non-intelligence information flows to add value to decision-making.

d. **Dissemination.** Since perfect information too late is of no value, there must be structures and processes in place to ensure information flows up and down the chain of command. Intelligence must also be disseminated to the lowest levels acceptable to those with a need to know within the parameters of security.

6.9. **Command climate and reasonable challenge.** The commander should encourage an environment of independent thought and intellectual empowerment, respectful challenge and creative tension to optimise the intelligence staff's analysis. Commanders must be prepared to receive intelligence that contradicts their existing or preferred views. Situating the appreciation may result in commanders selecting a less favourable course of action based on their own heuristics and biases. The Ministry of Defence's (MOD's) *Reasonable Challenge: A Guide* fully supports the offering and receipt of reasonable challenge. Reasonable challenge is not about proving whether someone is right or wrong, but it helps to highlight and explore alternative options. Commanders and J2 staff must be prepared to challenge and be challenged when providing and reviewing intelligence assessments.

Section 2 – The joint headquarters and the intelligence staff

6.10. **The joint headquarters.** The primary function of a joint headquarters is to exercise control over assigned forces and to enable the commander to make effective decisions on their operational employment. Intelligence staff are an essential part of the headquarters and are involved in all its primary functions, especially support to decision-making.

6.11. **The intelligence staff.** Commanders and staff at every level require intelligence to plan, direct, conduct and assess campaigns and operations. Intelligence is crucial in baselining understanding, identifying and selecting specific objectives and targets, associating those objectives and targets with desired effects, and determining the means to accomplish the overall mission. The changing character of conflict emphasises the need to place intelligence

within the wider concept of understanding, where commanders must get a holistic view of the operating environment. There should be a particular emphasis on the human environment in which actors, audiences, adversaries and enemies will interact, compete with and confront each other. 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 staff who are responsive enough to react to new problems and have the professional skills required for their role.

6.12. **Intelligence staff functions.** An intelligence staff should deliver two broad functions: manage intelligence tasking, collection, processing and dissemination; and intelligence planning and support to operations. These are explained below.

a. **Manage intelligence tasking, collection, processing and dissemination.** The intelligence staff will align intelligence requirements to assigned collection assets or reachback to higher-level formations or to the single intelligence environment (SIntE). This is followed by conducting intelligence collation, evaluation, analysis and then disseminating a product that answers intelligence requirements and offers understanding to the commander and their staff. This should be achieved across the maritime, land, air, space, and cyber and electromagnetic operational domains. This will support the commander's decision-making and the staff's estimates, planning, control and coordination of operational activity.

b. **Intelligence planning and support to operations.** Intelligence staff will also conduct intelligence planning, enable intelligence operations and ensure the intelligence architecture can produce the information flows essential to the intelligence and intelligence, surveillance and reconnaissance (ISR) cycles. Intelligence planning should be supported by staff delivering functional capabilities such as ISR, J2X, cyber and electromagnetic warfare, geospatial analysis and imagery intelligence, counter-intelligence/security and exploitation. For example, the Permanent Joint Headquarters' (PJHQ's) J2 Division has two distinct parts. PJHQ J2 Operations provides the headquarters' analytical teams. The analytical teams set intelligence requirements, tasking both deployed forces and requesting support from UK-based elements of the SIntE, before collating, evaluating, analysing and disseminating assessments or outputs that inform Chief of Joint Operations and the staff. PJHQ J2 Plans provides the headquarters' intelligence planning

role, which determines the deployed J2 capability and architectures and has the functional teams that provide subject matter expertise in areas such as ISR, human intelligence and counter-intelligence/security.

6.13. **Structures.** There is a tendency to confine the intelligence staff within discipline channels or structures. The contemporary operating environment instead requires permeable boundaries between functional areas to obtain greater coordination. This coordination may be achieved by: integrating other members of the headquarters staff into some intelligence functions to broaden their expertise; integrating both J2 analysts and planners into headquarters planning teams and operational teams; and involving commanders in intelligence training to increase knowledge and to manage their expectations.

6.14. **Reachback.** Intelligence staff will invariably have limited resources and, furthermore, contested environments will drive headquarters to limit their footprint and prioritise manoeuvrability to help survivability. Therefore, intelligence planning should consider whether intelligence models based on reachback are applicable.[146] Joint headquarters can base much of their intelligence analysis and planning capability in rear areas. Only a small team of analysts, and possibly planners, may be required to deploy forward with the commander. A joint headquarters may also have a heavy reliance on intelligence planning and analytical production provided by the Defence SIntE. The Chief of Defence Intelligence's (CDI's) responsibility for the Defence's intelligence function has formalised CDI's responsibility for directing and cohering Defence's intelligence effort, focusing it towards better supporting operations and the warfighter.

6.15. **Intelligence staff support to the commander.** Operations should be intelligence-driven and provide the commander with timely and accurate intelligence that supports their particular needs. To maintain the initiative, the commander will seek to make good decisions quickly. This requires the intelligence staff to be able to: assess the enemy's or adversary's decision-making and intent within the area of operations; maintain situational awareness and understanding of the area of intelligence interest and area of intelligence responsibilities; understand actors and audiences; and identify domain-orientated mismatches and windows of opportunity. They must also disseminate critical information that supports the commander's understanding and decision-making and the staff's orchestration of activities and effects. Table 6.1 summarises these responsibilities.

146 Reachforward models may also be applicable where rear-based operational headquarters require the experience and insight of the operational environment that forward deployed analysts can deliver.

Intelligence staff responsibilities
• Maintain a thorough knowledge of understanding and intelligence doctrine, intelligence capabilities and their limitations. • Develop detailed intelligence plans and provide advice based on a sound intelligence estimate and intelligence collection plan, as well as providing support to campaign and other operational planning. • Participate in all joint inter-agency and military planning conducted by the combined joint task force headquarters. • Ensure all intelligence is set within the wider framework of understanding and 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, optimising reachback. • Synchronise J2 planning and 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 access to intelligence. • Continuously review all intelligence.

Table 6.1 – Intelligence staff responsibilities

The commander being briefed during Exercise Citadel Guibert 18, a British and French combined arms staff exercise

Section 3 – Joint operational intelligence architecture

6.16. Intelligence architecture is defined as: a structure that consists of the overall organization and hierarchy, processes and systems within which the NATO military intelligence structure interacts and operates with other national and international agencies and organizations to support decision-makers at all levels.[147] The architecture should be flexible, optimise reachback both within an operational theatre and to the UK, and be tailored to the demands and circumstances of the operation. In the broadest sense, the intelligence architecture will contribute to enhancing decision-making, multi-domain integration and creating effects, and effective movement and sustainment. This will require the integration and collaboration of a wide range of sensors and collection capabilities, connected to processing, exploitation and dissemination (PED) units ensuring the timely and accurate exploitation of collected information and dissemination to the joint headquarters' intelligence staff.

6.17. Intelligence procedures should support the planning and execution of all operations by providing timely, tailored and accurate intelligence. The intelligence process should also allow a rapid flow of intelligence from all available collection capabilities to, from and across the joint operations area.

147 NATOTerm.

The architecture must not only focus on the intelligence process, but must also allow intelligence sharing and 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 chain of command.

6.18. The intelligence architecture is a collaborative endeavour involving all members of the intelligence community. It aims to harmonise the intelligence process to achieve the optimal use of intelligence specialists, agencies, collection capabilities and activities to produce the best possible insight and foresight. The intelligence architecture is built on personal relationships just as much as physical capabilities. It is the overall space, conditions and surroundings through which the military intelligence structure interacts and operates with other national and international information and intelligence agencies to support decision-makers at all levels. Its success depends on:

- educating and training personnel and friendly forces, including Reserve Forces;
- making the best use of reachback, exploiting the Defence SIntE, UK intelligence community (UKIC), Five Eyes (FVEY) and North Atlantic Treaty Organization (NATO) PED and fusion (including their information systems);
- maintaining pan-Defence, SIntE, inter-Service, cross-government and multinational links;
- bridging boundaries between the maritime, land, air, space, and cyber and electromagnetic operational domains;
- removing historical distinctions between the strategic, operational and tactical levels of intelligence activity;
- driving fusion and integration at all levels; and
- networking systems to enable reachback and the effective operation of the diverse competencies within the intelligence architecture.

6.19. 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 their 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, the intelligence effort should be directed towards clearly defined intelligence requirements and commonly understood objectives, whilst fully embracing cooperation and coordination to maximise collective effort across the Defence SIntE and with UKIC, FVEY and NATO partners. It must also be enabled by an intelligence architecture, communication and information systems (CIS) network and intelligence processing systems that allows the rapid movement, storage and exploitation of data and intelligence products.

6.20. **Command, control and 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 reachback to the UK, effective CIS within the intelligence branch is critical to success.

6.21. **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.

6.22. **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.

6.23. **Intelligence resources and architecture.** Defence SIntE resources are only one part of a bigger equation. UKIC national intelligence is a multiple-source activity and all resources should be used, where applicable, to meet the operational intelligence requirement. Articulating the requirement and obtaining the resources are necessary parts of developing capability. When working in a coalition or NATO context, the UK should share assets and intelligence to the greatest extent, subject to the protection of sources and national capabilities.

6.24. **Continuity.** Continuity at the national level but, more specifically, in theatre, is necessary for the success of any intelligence endeavour. Once a force deploys overseas, it is vitally important to establish a long-term view and provide a properly constituted national contingent headquarters in the operational theatre that has an intelligence support element designed to achieve intelligence continuity.[148] The staff for this headquarters must be carefully selected and expect to deploy in a pattern that ensures continuity.

Section 4 – The deployed intelligence architecture

6.25. **Chief J2.** Chief J2 is the commander's principal intelligence officer. The relationship and trust between a commander and the Chief J2 is critical to the operation of a headquarters. Chief J2's responsibilities include the following.

a. Acting as a focal point for the passage of intelligence briefed to the commander. This is likely to include, as a minimum, the commander's critical information requirements, the joint intelligence estimate and the intelligence collection plan.

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

c. Maintaining effective and productive relationships with supporting partners within the Defence SIntE, UKIC and amongst allies. These must be relationships that are built on interpersonal skills rather than process. Chief J2 will therefore engage with the principal supporting partners within the Defence SIntE, UKIC and allies before deployment, and aim to draw the UKIC into the military planning process to enhance mutual understanding.

148 Examples include the theatre-level operational intelligence support groups deployed to Iraq and Afghanistan.

6.26. **J2 Plans.** J2 Plans staff are the primary operational planning interface with the headquarters' other J staffs. The J2 Plans staff will provide intelligence input into cross-J staff planning, refine the intelligence architecture and provide functional intelligence inputs. They will also contribute to a headquarters' campaign/operations management process.

6.27. **J2 Operations.** J2 Operations staffs are the primary interface between intelligence staff and the headquarters' other staff. The J2 Operations staff will undertake analysis and provide assessments. They use all-source intelligence to deliver understanding to the commander and staff.

6.28. **Intelligence requirements management and collection management and intelligence, surveillance and reconnaissance cells.** The intelligence requirements management and collection management (IRM&CM) are critical as they translate the commander's direction, planning requirements and intelligence-generated tasks into intelligence requirements. Intelligence gaps are then identified against existing understanding, requirements are prioritised and then passed to the ISR collection management staff for tasking against intelligence collection assets, which are both under command and control of the commander or are available within wider Defence, UKIC, FVEY or NATO. The IRM&CM staff should then manage the intelligence flow back into the headquarters so it can determine if and when intelligence requirements are serviced. ISR subject matter experts will: manage the headquarters' ISR overlay detailing named areas of interest and the ISR synchronisation matrix; monitor the execution of organic ISR collection; and advise the commander and staff on the tactical employment of collect and PED assets. Depending on the operational design, this cell might be task-organised as part of J3 Operations.

6.29. **J2 Targeting and effects.** Targeting requires collaboration between intelligence, operations and planning staffs. A headquarters may need to employ a 'J2 Targeting and effects' function which could sit within either the plans or operations areas. Within the multi-domain environment, sensitive intelligence collected by national intelligence and the UKIC provide the commander with unique opportunities to create a wide range of effects against opponents and to influence actors, audiences, adversaries and enemies within the joint operations area. These effects range from targeting of opponent networks to the coordination of hard and soft power to achieve influence over and between audiences.

Imagery gathered from operations over Libya

6.30. **J2 Analysis cells.** The intelligence staff are normally divided into a number of specialist cells. These may include the following.

a. **All-source analysis cell.** An all-source analysis cell comprises a task-orientated production section that processes information and provides all-source intelligence products. The all-source analysis cell is directed by the Chief J2 to ensure that intelligence products meet the commander's needs and that intelligence requirements and requests for information are addressed accordingly. The all-source analysis cell should have the ability to access intelligence at every classification, inclusive of any additional control markings; however, this is often not possible due to constraints imposed on intelligence of the highest classification and/or additional control marking. Where this is the case, a separate UK above secret working environment (ASWE) or national intelligence cell (NIC) should be established for the analysis of this intelligence and for briefing the commander.

b. **UK above secret working environment or national intelligence cell.** Each ASWE or NIC is structured to provide a mission-tailored all-source intelligence capability to meet the specific theatre and operational needs. Specifically, they provide the commander with access to national intelligence capabilities to enable tactical exploitation of their products, whilst also providing reachback to enriched

intelligence from across the spectrum of operations. Although working alongside the wider formation intelligence staff, the UK ASWE or NIC is compartmentalised to operate at the highest level of classification and can include elements from all J2 areas.

c. **Coalition partner national intelligence cells.** The UK has a requirement to access national intelligence at all levels of protective marking and so will our coalition partners. NICs are a national responsibility, but the requirement for their existence must be factored in during the planning process when the UK is the lead nation.

d. **Additional functional subject matter expert cells.** Other functional subject matter expert cells may also be required within the operational headquarters. These will advise which intelligence requirements their capability is most suited to service. They should advise how their capability can best be employed in both a collection operations and PED operations sense, including from technical, policy, permissions and legal perspectives. Additional functional subject matter expert cells could include: J2X, signals intelligence/electromagnetic warfare, cyber, geospatial intelligence, open-source intelligence, counter-intelligence, and materiel and personnel exploitation. The intelligence staff can also host academic subject matter experts and red teams.

The intelligence function is fundamentally a human activity with training at its foundation

Section 5 – Intelligence training

6.31. **Intelligence education and training progression.** The education and training of intelligence staff is an essential enabler of effective joint intelligence. Intelligence training should combine both professional training for individuals and, where possible, training with units or formations that intelligence personnel will deploy with in advance of deployed operations. Intelligence training includes not only training for individuals, units and headquarters staff, but also training for both generalists and specialists.

6.32. **Intelligence Professional Development Framework.** Intelligence training occurs across multiple providers within the MOD and across all three Services and partner organisations. The *Intelligence on Weapons of Mass Destruction Review* led by Lord Butler in 2004 led to the establishment of the Professional Head of Intelligence Assessment (PHIA) team. This is supported by a Professional Development Framework[149] that provides a framework for intelligence analyst technical skills and skill levels. There are four basic levels of intelligence education and training. They are: foundation, proficient, highly proficient and advanced.[150]

6.33. **Language capability.** The development of intelligence may require linguistic support. Military linguists require a high level of competence that must be developed and maintained; this requires deliberate capability planning within the intelligence community, for both intelligence development conducted in the home base and in the deployed environment. The cost of training may be high and therefore careful judgement is required regarding the volume and variety of a standing capability. It is possible that the intelligence function will need to draw on capability outside its own resources to meet linguistic demands. In a deployed environment, this capability may be obtainable from contractors and locally employed civilians; however, security considerations will require military linguists for some intelligence functions.

149 PHIA, *Professional Development Framework for all-source intelligence assessment*, January 2019.
150 Skill levels are described in detail in the PHIA, *Professional Development Framework for all-source intelligence assessment*, January 2019, page 9.

Key points

- The focus of operational intelligence is to assist the operational commander's decision-making by enhancing their understanding.
- Ultimate responsibility for intelligence remains with the commander, although Chief J2 is responsible to the commander for intelligence staff output.
- Commanders and staff at every level require intelligence to plan, direct, conduct and assess campaigns and operations.
- The intelligence staff should deliver two broad functions: first, they set the intelligence requirements to assigned collection assets, conduct information and data processing, and disseminate intelligence product; and second, they conduct intelligence planning, enabling intelligence operations and ensuring the intelligence architecture and information flows to the intelligence and ISR cycles.
- The deployed intelligence architecture will incorporate some or all of the following positions and teams: Chief J2; J2 Plans; J2 Operations; J2 Targeting and effects; specialist cells, including an all-source analysis cell, and IRM&CM cell, and ISR cell; and additional functional subject matter experts.
- Defence Intelligence personnel training is now underpinned by the PHIA Professional Development Framework, establishing four skill levels: foundation, proficient, highly proficient and advanced.

Notes

Chapter 7

Chapter 7 examines intelligence support to joint operational planning. This chapter outlines the role intelligence performs to support the operations planning process through the development of the joint intelligence preparation of the operating environment.

> “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.”

Rear Admiral Dave Buss, United States Navy (Commander CJ5, Headquarters Multinational Forces Iraq, June 2008 – May 2009)

Chapter 7

Intelligence support to joint operational planning

7.1. At the joint operational level, the intelligence process is one of the main activities that supports the operations planning process (OPP).[151] The intelligence process is a continuum and the constant flow and updating of information within the cycle may provide intelligence that fundamentally changes the development and implementation of a campaign plan at any stage during the planning process. The complexity of modern operations produces a greater need for all-encompassing intelligence, derived from a range of sources and agencies to develop understanding of the operating environment. This relies on all available intelligence disciplines and analytical specialisms (for example, signals intelligence, imagery intelligence, open-source intelligence, human intelligence, etc.) and intelligence, surveillance and reconnaissance for collection and the subsequent processing and dissemination of fused intelligence to satisfy intelligence requirements.

Section 1 – Preparation

7.2. It is important to maintain core intelligence capabilities 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, specialist language training, technical development or source recruitment).

7.3. **Initial planning.** Joint task force headquarters staff provide the intelligence production and dissemination focus for operational and deployed force activity beyond the UK.[152] These staff, in close cooperation with Defence Intelligence, are responsible for estimating an adversary's courses of action (COAs), centres of gravity and vulnerabilities. At the outset of a campaign, intensive planning ensures that appropriate intelligence is available to the joint task force commander and their assigned forces.

151 The full operations planning process is detailed in Allied Joint Publication (AJP)-5, *Allied Joint Doctrine for the Planning of Operations* (with UK national elements).
152 This includes not only the staff of the intelligence branch, but also the operations and planning staff.

7.4. **Intelligence support to operational staff work.** Intelligence supports development of all headquarters staff work outputs at the strategic, operational and tactical levels. Table 7.1 depicts the hierarchy of operational staff work.

Level	Output
Strategic	Chief of the Defence Staff (CDS) Directive
	Joint Commander's Directive
	CDS Planning Directive
Operational	Joint task force commander planning guidance
	Campaign directive
	Force instruction document
	Operation plans (OPLANs)
Operational and tactical	Contingency plans (CONPLANs)
	Operation orders (OPORDs)
	Fragmentary orders (FRAGOs)

Table 7.1 – The hierarchy of joint operational staff work

7.5. **The intelligence and security directive.** The intelligence staff should draft an intelligence and security directive for their formation's element of an operation. This short, succinct and clearly understandable directive must:

- articulate the role of intelligence in the operation;
- define the area of intelligence responsibility and area of intelligence interest for the operation;
- clarify the planned intelligence architecture, command arrangements and information exchange requirements;
- define the roles and responsibilities of the operational intelligence teams;
- detail collection assets available and their tasking arrangements;
- outline intelligence agencies and their liaison arrangements;
- confirm the operation battle rhythm and intelligence reporting requirements; and
- detail the counter-intelligence and security arrangements.

The completed intelligence and security directive requires approval by the commander and is included as an annex in the overall operation order. Figure 7.1 is an example of a Permanent Joint Headquarters (PJHQ) intelligence and security directive format.

Content

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/workforce

- Assigned and non-assigned military assets
- National and Defence Intelligence assets
- Multinational/coalition assets
- To include: intelligence, surveillance and reconnaissance, counter-intelligence and security, cyber, partners across government, and wider Defence intelligence enterprise.

Force preparation

Oversight and governance

- Collaboration protocols
- Arrangements for fusion
- Security risk management

Command and control

- Chain of command
- Joint operational architecture
- Communication and information systems

Figure 7.1 – An example of a PJHQ intelligence and security directive format

The Pathfinders are 16 Air Assault Brigade's advance reconnaissance force – training here on Exercise Swift Response

Section 2 – Joint intelligence preparation of the operating environment

7.6. The intelligence process supports all phases of the OPP, with one of the most significant J2 contributions termed the joint intelligence preparation of the operating environment (JIPOE).[153] The JIPOE process is a disciplined analytical methodology conducted by the intelligence staff that produces intelligence assessments, estimates and other intelligence products to support operations planning. JIPOE is a three-stage process that conducts operational area evaluation, threat identification and threat area evaluation.

a. JIPOE informs joint planning by providing planners and decision-makers with a comprehensive understanding of the operating environment (CUOE) and the actors within it. JIPOE enables the development of a comprehensive understanding of the entirety of the operating environment, covering all elements of the political, military, economic, social, infrastructure and information (PMESII) spectrum set against the backdrop of the human, information and physical

153 The JIPOE process is explained in detail in Allied Intelligence Publication (AIntP)-17, *Joint Intelligence Preparation of the Operating Environment*.

environments. This includes identifying associated opportunities, potential threats and risks in support of planning and the conduct of a campaign or operation. It develops an integrated understanding of the main characteristics of the operating environment, including its maritime, land, air, space, and cyber and electromagnetic operational domains and the PMESII factors of the main adversaries, friends and neutral actors that may influence joint operations.

b. The close alignment of the intelligence process and the J2 contribution to the OPP through the JIPOE means that intelligence produced at any level can be used seamlessly throughout the command chain. This ultimately contributes to operational success by providing better situational awareness to assist the commander's decision-making.

c. The outcome of the JIPOE process forms the basis of the joint intelligence estimate and is refined and updated as planning continues through the OPP, as outlined below. 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, the JIPOE underpins the OPP, execution and assessment of operations.

7.7. **Joint intelligence estimate.** The joint intelligence estimate is the end product of the JIPOE process but remains subject to continual review and development. Information received from all collection capabilities should be fused together by the intelligence staff to conduct a thorough JIPOE and will be articulated via the joint intelligence estimate. The joint intelligence estimate results in a forecast based on degrees of probability. It is a series of logical deductions drawn from the information available. The joint intelligence estimate enables commanders to decide how to accomplish their mission. As intelligence is collected, the joint intelligence estimate increases in detail and provides significant input to the operational-level planning process. The principal outputs of the joint intelligence estimate are:

- an understanding of the operational environment and actors;
- an assessment of the adversary's capabilities, intent and opportunities based on the available intelligence;
- identification of the adversary's probable COAs and the probability of their adoption;

- providing commanders with the intelligence required for the operational estimate;
- proving the start point for intelligence planning by identifying intelligence requirements; and
- highlighting the intelligence-sharing requirements between nations to support the operation.

Section 3 – Intelligence support to operational planning

7.8. The operational estimate is fundamental to campaign planning and to supporting operations. It aims to reduce a complex mass of information into potential COAs from which the commander will select their preference. It is by this means that the commander formulates a campaign plan.

a. Intelligence staff support the joint operational estimate by undertaking the JIPOE to enhance understanding and resultant decision-making through the joint intelligence estimate. Intelligence staff must remain cognisant of the commander's requirements as they evolve, so the commander must include the intelligence staff in all aspects of planning.

b. The intelligence process does not work in isolation from other OPPs within a headquarters. To create the optimum effect, all the planning processes must be synchronised.

The operations planning process

7.9. The OPP enables the synchronisation of planning; it is command led, but intelligence driven. The North Atlantic Treaty Organization's (NATO's) Allied Joint Publication (AJP)-5, *Allied Joint Doctrine for the Planning of Operations* (with UK national elements) describes the UK's approach to operational planning via the seven stages in the process that forms the joint operational estimate. Figure 7.2 summarises the OPP and the stages are then explained further.

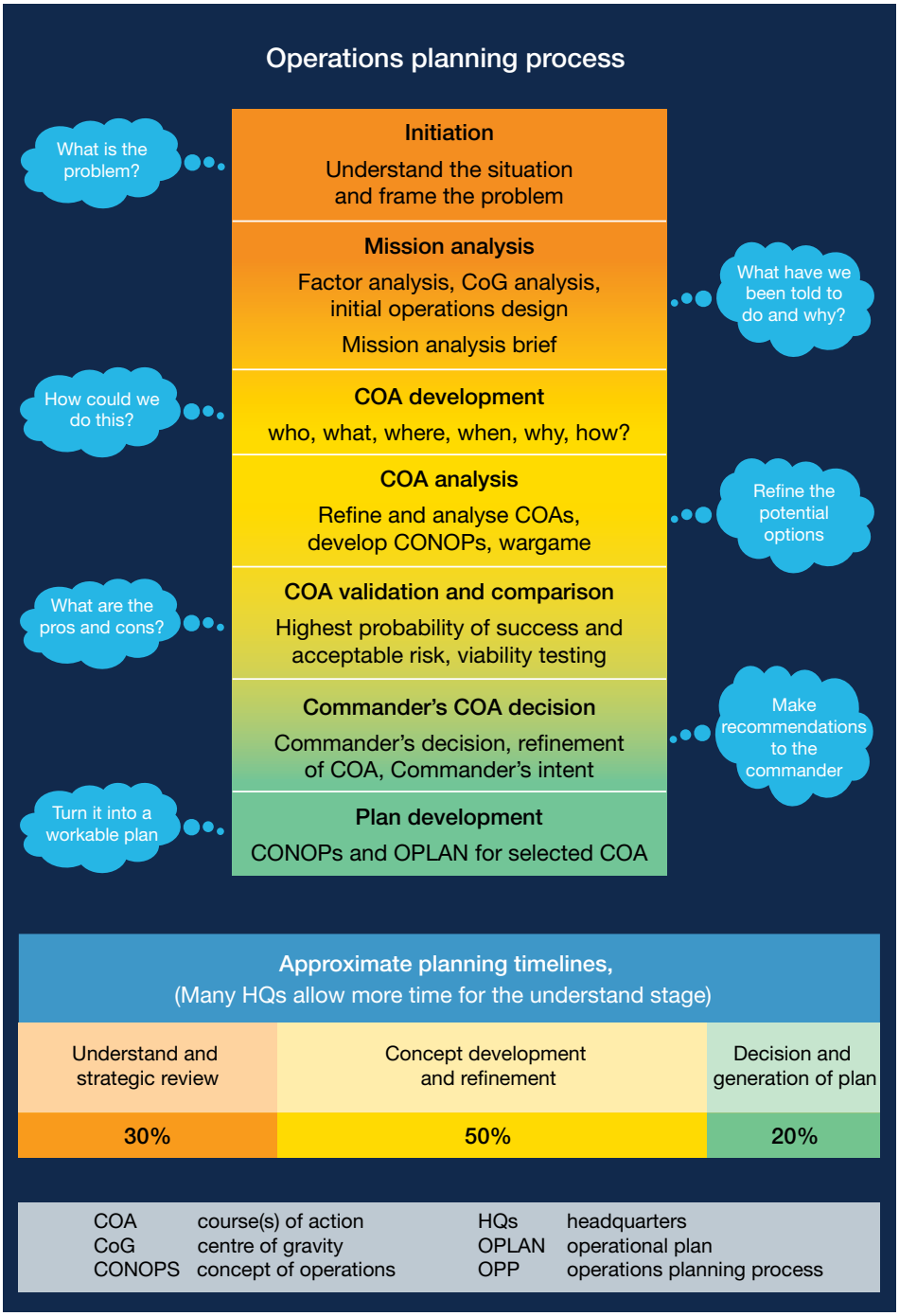
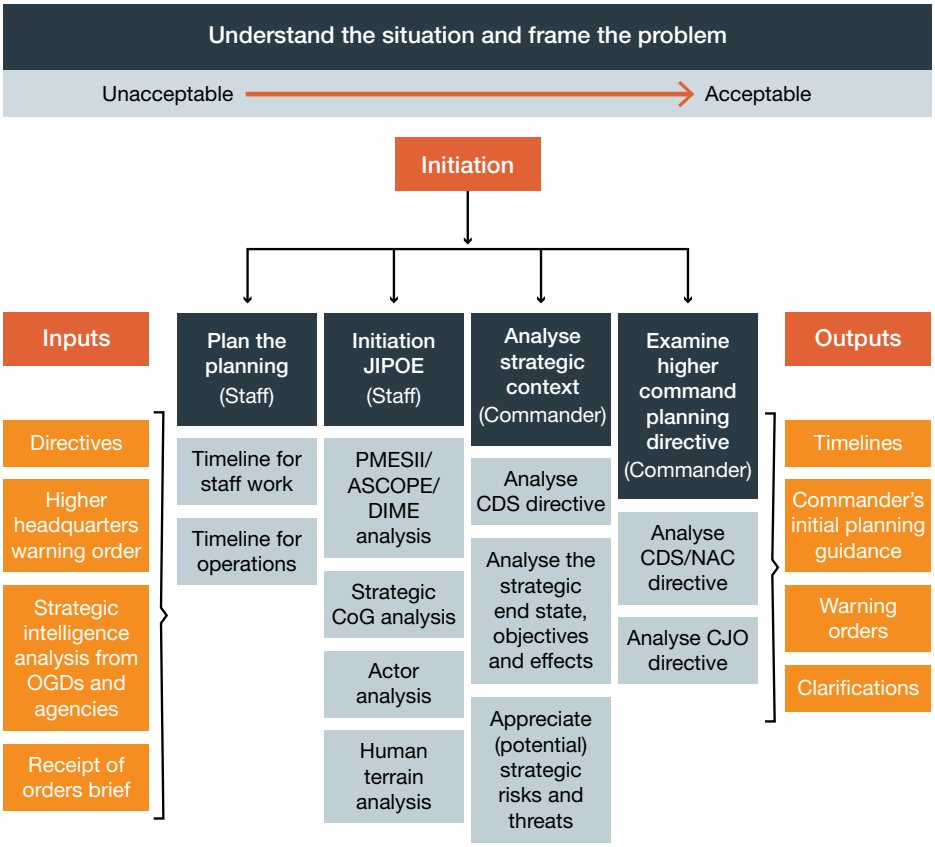


Figure 7.2 – The operations planning process[154]

154 AJP-5, *Allied Joint Doctrine for the Planning of Operations* (with UK national elements), UK Annex D, page D-1, UK Figure D1.

British and French staff officers working together during Exercise Rochambeau 2014, a 14-nation multinational exercise

7.10. **Stage 1 – initiation.** Initiation reviews the inputs from the strategic level, higher headquarters and within J2 it initiates the JIPOE. The primary aim of initiation is to achieve collective and common situational awareness with two main outcomes: why are we looking at this problem; and who is doing what and why in the operating environment. Figure 7.3 depicts the key inputs and outputs in this phase. Initiation focuses on conducting an operational area evaluation, threat identification and threat area evaluation, and will review the physical terrain and the information environment. Within the threat evaluation, the intelligence staff will seek to understand the adversary and conduct analysis of the span of actors within the operational environment. Threat integration will seek to identify adversary aims and objectives and will consider potential enemy COAs. Tools used by the J2 staff at this stage may include, but are not limited to: PMESII; area, structure, capabilities, organisation, people, events (ASCOPE) and/or diplomatic, information, military, economic (DIME) analysis; and strategic centre of gravity analysis.



ASCOPE	area, structure, capabilities, organisation, people, events
CDS	Chief of the Defence Staff
CJO	Chief of Joint Operations
CoG	centre of gravity
DIME	diplomatic, information, military, economic
OGDs	other government departments
JIPOE	joint intelligence preparation of the operating environment
NAC	North Atlantic Council
PMESII	political, military, economic, social, infrastructure, information

Figure 7.3 – Inputs, outputs and staff activity during initiation[155]

155 AJP-5, *Allied Joint Doctrine for the Planning of Operations* (with UK national elements), UK Annex D, page D-6, UK Figure D2.

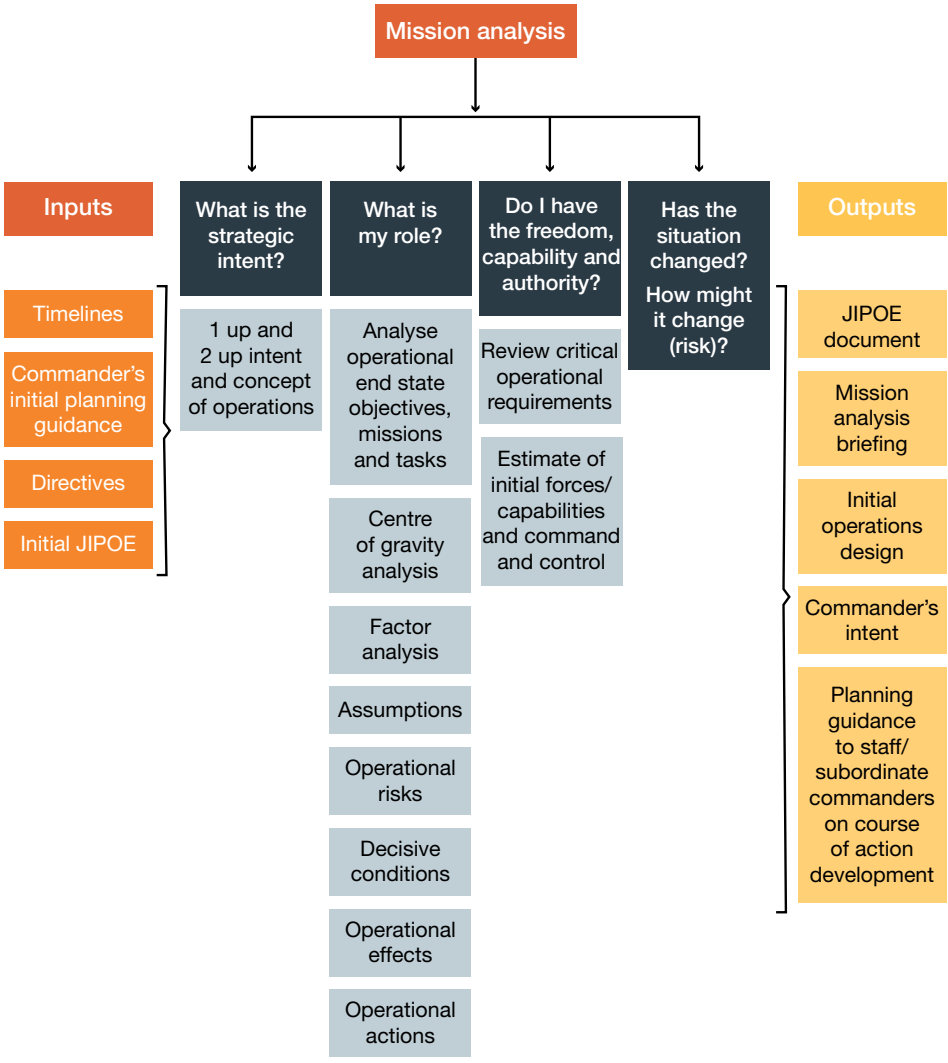
7.11. **Stage 2 – mission analysis.** The mission analysis stage takes the product from the initial JIPOE and develops it further. The commander's principal intelligence adviser and staff play a critical role in identifying and analysing the problem through the conduct of the joint intelligence estimate. The principal intelligence adviser also helps the commander to identify their critical information requirements. By understanding the mission and the commander's intent, the commander can direct the intelligence staff to begin detailed intelligence planning. Mission analysis will include: analysing the impact of the operational environment; 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 critical information requirements; determining the limitations of intelligence support; proposing acceptable risk guidelines; and conducting a thorough timeline estimate. Figure 7.4 illustrates the mission analysis process, which includes the following steps.

a. **Understanding role.** Conducted by the commander's command group, this analysis should include the principal intelligence adviser but this is dependent on the commander. Intelligence support to mission analysis outputs include the following: support to developing the initial campaign end state and objectives; support to centres of gravity analysis; and staffing of commander's critical information requirements (CCIR).

b. **Object and factor analysis.** The intelligence input during this stage is critical. It is here that intelligence staff begin to develop understanding for the commander. The JIPOE and other intelligence products form the basis of object and factor analysis.

c. **Commander's confirmation.** Intelligence staff can help to provide final confirmation of issues identified throughout the mission analysis step through the CCIR process.

d. **Key outputs.** Outputs from this stage include: JIPOE document; J2 support to mission analysis briefing; and J2 support to planning guidance for staff and subordinate commanders on COA development.



JIPOE joint intelligence preparation of the operating environment

Figure 7.4 – Inputs, outputs and staff activity during mission analysis[156]

7.12. **Stage 3 – course of action development.** The purpose of COA development is to develop a set of draft COAs in accordance with the commander's intent. Outline COAs are developed by the staff for the commander's review before being developed and further refined. The headquarters will be reconfigured into cross-function COA development

156 AJP-5, *Allied Joint Doctrine for the Planning of Operations* (with UK national elements), UK Annex D, page D-6, UK Figure D3.

teams, while the J2 staff also develop the primary actors' most likely and most dangerous COAs for the staff to plan against.

7.13. **Stage 4 – course of action analysis.** Intelligence input to COA development and evaluation includes the following.

a. Conducting a review of the situation and environmental characteristics, concentrating on those aspects that have changed since the initial COAs were developed.

b. A detailed description, in priority order, of the threats for each COA from most likely to least likely and from most dangerous to least dangerous.

c. Intelligence staff support to any wargaming the commander requires.

d. Updating understanding through responses to the CCIR and other information requirements.

7.14. **Stage 5 – course of action validation and comparison.** The purpose of the fifth stage of the OPP is to validate and compare the COAs and develop a proposal for the COA to be recommended (and selected). COAs are assessed independently of each other against criteria established by the staff and/or commander. The COA recommended by the staff should be the one with the highest probability of success with an acceptable level of risk.[157]

7.15. **Stage 6 – commander's course of action decision.** During this stage, the commander is briefed on the COAs before making their final decision. The commander identifies what they consider the optimum COA is for the staff to develop in detail. The principal intelligence adviser has an important role in helping the commander decide which to choose. Subsequently, a final intelligence assessment is required for the joint force commander's directive.

7.16. **Stage 7 – plan development.** The purpose here is to produce a concept of operations and operation plan. The concept of operations will express what the commander intends to accomplish and how it will be done. The operation plan will be in the same structure and format as the concept

157 See AJP-5, *Allied Joint Doctrine for the Planning of Operations* (with UK national elements), UK Annex D, page D-23, for further detail on the sub-elements of COA validation and comparison.

of operations but will be developed to include greater detail, including force capability statements of requirements. This phase also allows for finalising the initial version of the joint intelligence estimate.

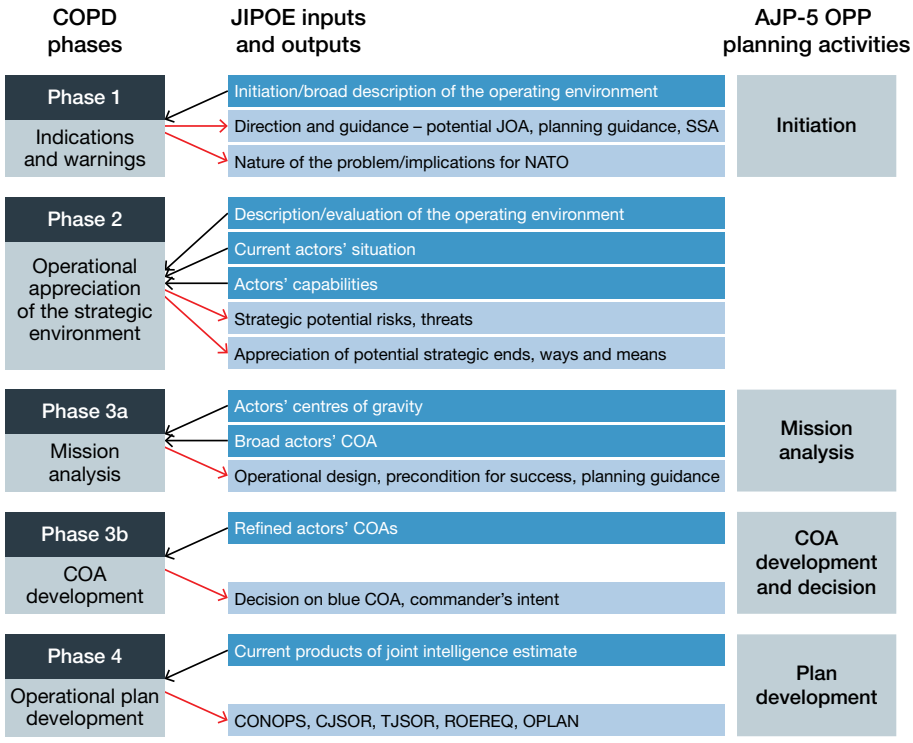
Additional considerations

7.17. **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 operation plan will require at least three iterative warning orders to be issued. The first warning order provides a basic intelligence summary at the start of the planning process outlining the operational environment and the audiences within it. Warning order two refines the intelligence assessment based on analysis of the joint intelligence estimate and the more holistic JIPOE. Warning order three refines this information further and provides sufficient understanding to allow the commander to make effective decisions.

7.18. **The intelligence staff, wargaming and red teaming.** Wargaming and red teaming normally occurs during the COA analysis stage. The intelligence staff play an important role by 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.[158]

7.19. **J2 joint intelligence preparation of the operating environment and alignment of UK and NATO planning processes.** AJP-5, *Allied Joint Doctrine for the Planning of Operations* (with UK national elements), UK Annex D details the UK OPP, including the J2 contribution. Operations in a NATO-led operation may require the use of the NATO OPP and use of the Allied Command Operations' *Comprehensive Operations Planning Directive* (COPD), which differs slightly from the UK OPP. The JIPOE inputs and outputs and synchronisation with AJP-5 are detailed in Allied Intelligence Publication (AIntP)-17, *Joint Intelligence Preparation of the Operating Environment*. Figure 7.5 outlines the COPD, JIPOE and AJP-5 OPP phases.

158 See the Development, Concepts and Doctrine Centre's *Red Teaming Handbook*, 3rd Edition.



AJP	Allied joint publication
CJSOR	combined joint statement of requirements
COA	course of action
CONOPS	concept of operations
COPD	Comprehensive Operations Planning Directive
JIPOE	joint intelligence preparation of the operating environment
JOA	joint operations area
OPLAN	operations plan
OPP	operations planning process
ROEREQ	rule-of-engagement request
SSA	Supreme Allied Commander Europe's (SACEUR's) strategic assessment
TCSOR	theatre capability statement of requirements

Figure 7.5 – Synchronisation of joint intelligence preparation of the operating environment with the *Comprehensive Operations Planning Directive* and operations planning process[159]

7.20. **NATO and the comprehensive understanding of the operating environment.** The CUOE is the combination of the information environment assessment (described in Chapter 5), the JIPOE described above and other stakeholder analysis (including external organisations). Within the NATO OPP, the development and application of the CUOE links to supporting the commander's decision-making process and direction. Figure 7.6 illustrates the development of the CUOE.

159 AIntP-17, *Joint Intelligence Preparation of the Operating Environment*, page 1-10.

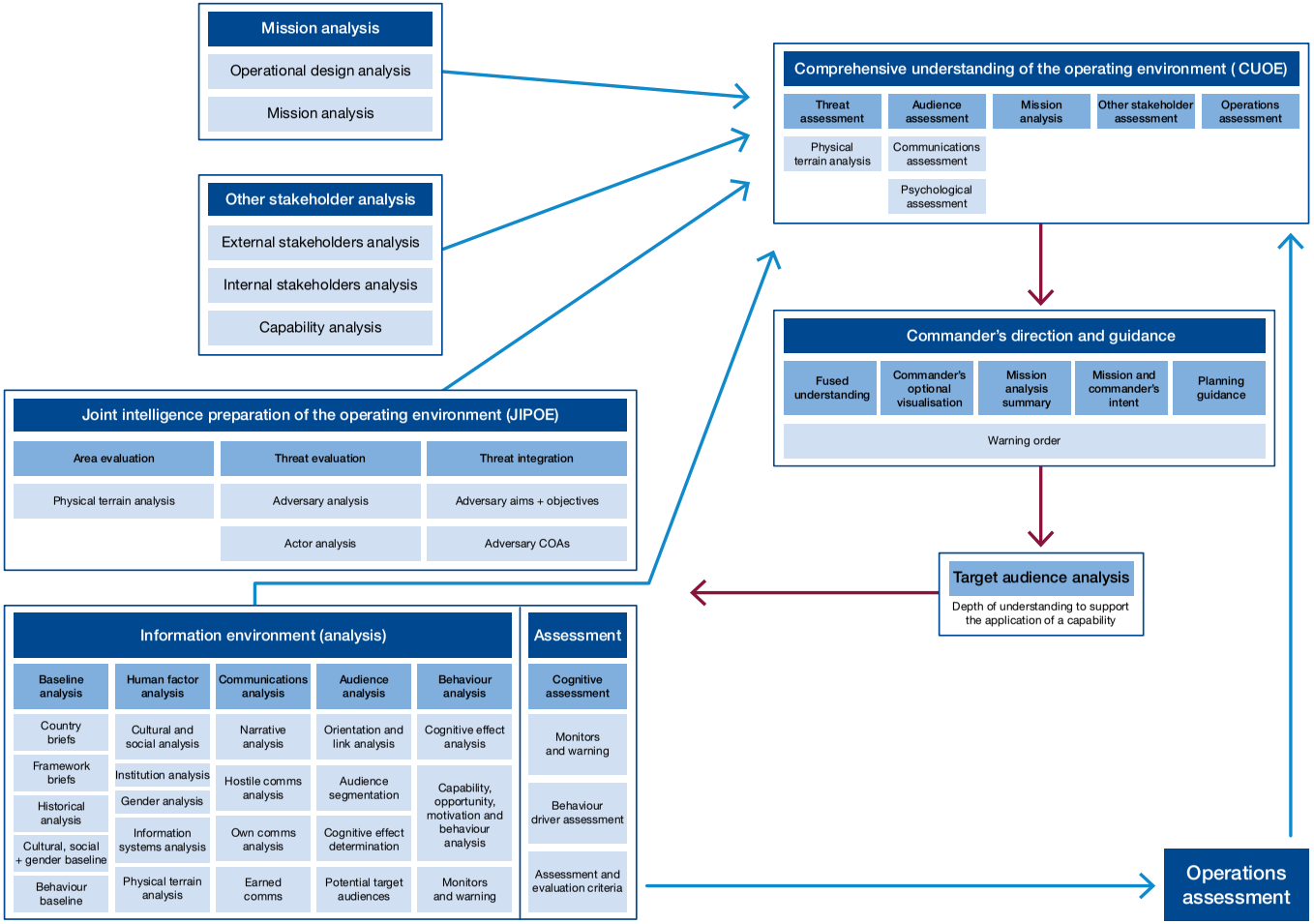


Figure 7.6 – Comprehensive understanding of the operating environment[160]

160 AJP-10.1, *Allied Joint Doctrine for Information Operations* (with UK national elements), Figure 4.8. The development of the CUOE is described in greater detail in AJP-10.1, *Allied Joint Doctrine for Information Operations* (with UK national elements).

Key points

- It is important to prepare for future operations through maintaining core intelligence capabilities and skill sets in anticipation of future requirements.
- Intelligence supports the development of all headquarters staff work outputs at the strategic, operational and tactical levels.
- The intelligence staff should draft an intelligence and security directive for their formation's element of an operation.
- The intelligence process supports all phases of the OPP; one of the most significant intelligence contributions is the JIPOE.
- The end product of the JIPOE is the joint intelligence estimate.
- The first main intelligence contribution to the seven-stage joint operational estimate is during stage one – initiation – which focuses on conducting an operational area evaluation, threat identification and threat area evaluation.
- The second contribution to the joint operational estimate is in stage two – mission analysis. Principal intelligence outputs are the JIPOE document, J2 support to the mission analysis briefing, and J2 support to planning guidance for staff and subordinate commanders on subsequent COA development.
- Operations in a NATO environment may require J2 staff to use the Allied Command Operations' COPD planning process rather than UK OPP; although similar, there are differences. Additional references are AJP-5, *Allied Joint Doctrine for the Planning of Operations* (with UK national elements), and AIntP-17, *Joint Intelligence Preparation of the Operating Environment*.
- A further NATO process is the development of the CUOE. The CUOE is a combination of the information environment assessment, the JIPOE and other stakeholder analysis/engagement.

Lexicon

Section 1 – Acronyms and abbreviations

ABI	activity-based intelligence
ACINT	acoustic intelligence
AIntP	Allied intelligence publication
AJP	Allied joint publication
ASCOPE	area, structures, capabilities, organisations, people and events
ASWE	above secret working environment
BAA	baseline audience analysis
CBRN	chemical, biological, radiological and nuclear
CCIR	commander's critical information requirement
CDI	Chief of Defence Intelligence
CDPA	Copyright, Designs and Patents Act
CHINT	cultural heritage intelligence
CI	counter-intelligence
CI-INTREP	counter-intelligence intelligence report
CI-INTSUM	counter-intelligence intelligence summary
CI-SUPINTREP	counter-intelligence supplementary intelligence report
CICA	Counter-Intelligence Coordinating Authority
CIG	Current Intelligence Group
CIS	communication and information systems
CJO	Chief of Joint Operations
COA	course of action
COAS	Cabinet Office Assessments Staff
Comd UKStratCom	Commander Strategic Command
COMINT	communications intelligence
COPD	Comprehensive Operations Planning Directive
CPERS	captured persons
CRL	collection requirements list
CUOE	comprehensive understanding of the operating environment

DCDC	Development, Concepts and Doctrine Centre
DCPD	direction, collection, processing and dissemination
DIME	diplomatic, information, military, economic
EAU	Extremism Analysis Unit
ECHR	European Convention on Human Rights
EEI	essential elements of information
ELINT	electromagnetic intelligence
FCDO	Foreign, Commonwealth and Development Office
FVEY	Five Eyes
GCHQ	Government Communications Headquarters
GEOINT	geospatial intelligence
HUMINT	human intelligence
IAC	international armed conflict
IEA	information environment assessment
IHRL	international human rights law
IMINT	imagery intelligence
INTREP	intelligence report
INTSUM	intelligence summary
IPA	Investigatory Powers Act
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
JIC	Joint Intelligence Committee
JIO	Joint Intelligence Organisation
JIPOE	joint intelligence preparation of the operating environment
JISR	joint intelligence, surveillance and reconnaissance
JOA	joint operations area
JSP	joint Service publication
JSTAT	Joint State Threats Assessment Team
JTAC	Joint Terrorism Analysis Centre
JTTP	joint tactics, techniques and procedures

LOAC	law of armed conflict
MAA	mission audience analysis
MASINT	measurement and signature intelligence
MDI	multi-domain integration
MOD	Ministry of Defence
MPE	materiel and personnel exploitation
NATO	North Atlantic Treaty Organization
NCA	National Crime Agency
NCSC	National Cyber Security Centre
NIAC	non-international armed conflict
NIC	national intelligence cell
NSA	National Security Adviser
NSC	National Security Council
OBP	object-based production
OPP	operations planning process
OSINT	open-source intelligence
PAI	publicly available information
PED	processing, exploitation and dissemination
PHIA	Professional Head of Intelligence Assessment
PIR	priority information requirement
PJHQ	Permanent Joint Headquarters
PMESII	political, military, economic, social, infrastructure and information
PMESII-PT	political, military, economic, social, infrastructure and information and physical and time
RFI	request for information
RIPA	Regulation of Investigatory Powers Act
ROE	rules of engagement
SATs	structured analytical techniques
SIGINT	signals intelligence
SIntE	single intelligence environment
SIR	specific intelligence requirement
SIS	Secret Intelligence Service
SOM	structured observation management
SUPINTREP	supplementary intelligence report

TAA	target audience analysis
TCPED	task, collect, process, exploit and disseminate
TESSOC	terrorism, espionage, subversion, sabotage and organised crime
UKIC	UK intelligence community
UN	United Nations

Section 2 – Terms and definitions

This section is divided into three parts. First, we list definitions modified by this publication which will be updated in JDP 0-01.1, *UK Terminology Supplement to NATOTerm*. Second, we list endorsed terms and definitions.

Modified definitions

multiple-source intelligence
The deliberate application of two or more discrete but supporting intelligence disciplines, seeking to improve the quality of the intelligence product.
Note: Supporting intelligence disciplines include, for example, geospatial intelligence, human intelligence and signals intelligence. (JDP 2-00, 4th Edition)

Endorsed definitions

acoustic intelligence
Intelligence derived from acoustic signals or emissions. (NATOTerm)

actor
An individual, group or entity whose actions are affecting the attainment of the end state. (NATOTerm)

agency
In intelligence usage, an organization or individual engaged in collecting and/or processing information. (NATOTerm)

all-source intelligence
Intelligence produced using all available sources and agencies. (NATOTerm)

analysis
In intelligence usage, an activity in the processing phase of the intelligence cycle in which information is subjected to review in order to identify significant facts for subsequent interpretation.
Note: The analysis identifies and extracts the pieces of information relevant to the intelligence requirement. (NATOTerm)

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

area of intelligence interest
A geographical area for which commanders require intelligence on the factors and developments that may affect the outcome of operations. (NATOTerm)

area of intelligence responsibility
A geographical area allocated to a commander, in which the commander is responsible for the provision of intelligence. (NATOTerm)

audience
An individual, group or entity whose interpretation of events and subsequent behaviour may affect the attainment of the end state.
Note: The audience may consist of publics, stakeholders and actors. (NATOTerm)

audience analysis
The understanding and segmentation of audiences in support of the achievement of objectives. (NATOTerm)

baseline audience analysis
The foundational level of audience analysis to support planning and inform mission and target audience analysis. (JDP 0-01.1)

basic intelligence
Intelligence derived from any source, that may be used as reference material for planning and as a basis for processing subsequent information or intelligence.
Note: Basic intelligence is fused from all available data, information, joint intelligence, surveillance and reconnaissance results, single-source intelligence and all-source intelligence and it is fundamental to current intelligence. (NATOTerm)

battle damage assessment
The timely and accurate assessment of damage resulting from the application of lethal or non-lethal force against an entity. (NATOTerm)

chemical exploitation
Provides chemical intelligence on, improvised weapons and unknown substances by processing, examining and analysing samples of materials. (JDP 0-01.1)

collation
In intelligence usage, an activity 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. (NATOTerm)

collection
The gathering and exploitation of data and information by specialists and agencies and the delivery of the results obtained to the appropriate processing unit for use in the production of intelligence. (Awaiting approval by the MCJSB)

collection management
In intelligence usage, the process of satisfying collection requirements by tasking, requesting or coordinating with appropriate collection sources or agencies, monitoring results and re-tasking, as required. (NATOTerm)

combat effectiveness
The ability of a unit or formation, or equipment to perform assigned missions or functions.
Note: This should take into account leadership, personnel strength, the state of repair of the equipment, logistics, training and morale and may be expressed as a level or percentage. (NATOTerm)

combat power
The total means of destructive and/or disruptive force which a military unit / formation can apply against the opponent at a given time. (NATOTerm)

communications intelligence
Intelligence derived from electromagnetic communications and communication systems by other than intended recipients or users.
Note: Communications intelligence is a subset of signals intelligence. (NATOTerm)

contingency plan
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. (NATOTerm)

counter-intelligence
Those activities concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organizations or by individuals engaged in espionage, sabotage, subversion or terrorism. (NATOTerm)

current intelligence
Intelligence that reflects the current situation at strategic, operational and/or tactical levels. (NATOTerm)

data
A reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.
Note: Data can be processed by humans or by automatic means. (NATOTerm)

direction
The determination of intelligence requirements, planning of collection effort, issuance of orders and requests to agencies and continuous monitoring on the productivity of such agencies.
Note: Direction describes the first phase of the intelligence cycle. (NATOTerm)

dissemination
The timely conveyance of intelligence, in appropriate forms and means, to those who need it.
Note: Dissemination describes the fourth phase of the intelligence cycle. (NATOTerm)

electromagnetic intelligence
Intelligence derived from electromagnetic non-communications transmissions by other than intended recipients or users.
Notes: Electromagnetic intelligence is a subset of signals intelligence. (NATOTerm)

environment
The surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans and their interrelations. (NATOTerm)

espionage
In intelligence usage, an activity directed towards the acquisition of information through clandestine means and forbidden by the law of the country against which it is committed. (NATOTerm)

evaluation
In intelligence usage, an activity in the processing phase of the intelligence cycle consisting in an appraisal of the quality of the reported information, which is key to determining the reliability of the originator or source and the credibility of the information. (NATOTerm)

fusion
In intelligence usage, the blending of intelligence, information and data from multiple sources or agencies into a coherent picture in such a manner that the origin of the initial individual items is no longer apparent. (NATOTerm)

geospatial information
Facts about the earth referenced by geographic position and arranged in a coherent structure.
Notes: Geospatial information includes products, data, publications and materials based on topographic, aeronautical, hydrographic, planimetric, relief, thematic, geodetic, and geophysical information, including geo-referenced imagery and may be available in either analogue or digital formats. (NATOTerm)

geospatial intelligence
Intelligence derived from the exploitation and analysis of geospatial information, imagery and other data to describe, assess or visually depict geographically referenced activities and features.
Note: Geospatial intelligence includes imagery intelligence and the production or analysis of geospatial information; it underpins understanding, planning, navigation and targeting. (JDP 0-01.1)

horizon scanning
The systematic search across the global environment for potential threats, hazards and opportunities. (JDP 0-01.1)

human intelligence
Intelligence derived from information collected by human operators and primarily provided by human sources. (NATOTerm)

imagery intelligence
Intelligence derived from imagery acquired from sensors that can be ground-based, seaborne or carried by air or space platforms. (NATOTerm)

indicators and warnings
Intelligence activities to detect and report time-sensitive information on developments that could threaten the multinational force, including forewarning of adversaries' intentions or actions, insurgency, terrorism and other similar events. (JDP 0-01.1)

information
Data arranged to convey meaning. (NATOTerm)

information requirement
In intelligence usage, information regarding an adversary or potentially hostile actors and other relevant aspects of the operational environment that needs to be collected and processed to meet the intelligence requirements of a commander. (NATOTerm)

integration
An activity in 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. (NATOTerm)

intelligence
The product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers. (NATOTerm)

intelligence architecture
A structure that consists of the overall organization and hierarchy, processes and systems within which the NATO military intelligence structure interacts and operates with other national and international agencies and organizations to support decision-makers at all levels. (NATOTerm)

intelligence cycle
The sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users. (NATOTerm)

intelligence requirement
A statement that provides the rationale and priority for an intelligence activity, as well as the detail to allow the intelligence staff to satisfy the requirement in the most effective manner.
Notes:
1. Intelligence requirements should cover the broad scope of information on the political, military, economic, social, infrastructural and informational spectrum.
2. The military spectrum will be covered by the commander's critical information requirement.
3. Military types of intelligence requirements are: priority information requirements, specific intelligence requirement and essential elements of information. (NATOTerm)

intelligence requirements management
The management function that develops, validates and prioritizes intelligence requirements, forwards validated intelligence requirements to the collection management function, and oversees dissemination of the intelligence products. (NATOTerm)

intelligence requirements management and collection management
A set of integrated processes and services to manage and satisfy the intelligence requirements by making best use of the available collection, processing, exploitation and dissemination capabilities. (NATOTerm)

interpretation
In intelligence usage, an activity in the processing phase of the intelligence cycle during which the significance of information or intelligence is judged in relation to the current body of knowledge. (NATOTerm)

joint intelligence preparation of the operating environment
The analytical process used to produce intelligence estimates and other intelligence products in support of the commanders' decision-making and operations planning. (NATOTerm)

joint intelligence, surveillance and reconnaissance
An integrated intelligence and operations set of capabilities, which synchronises and integrates the planning and operations of all collection capabilities with the processing, exploitation, and dissemination of the resulting information in direct support of the planning, preparation, and execution of operations. (NATOTerm)

joint operations area
A temporary area within a theatre of operations defined by the Supreme Allied Commander Europe, in which a designated joint force commander plans and executes a specific mission at the operational level. (NATOTerm)

materiel and personnel exploitation
Exploiting material and personnel by scientific, technical and specialist intelligence activities. (JDP 0-01.1)

measurement and signature intelligence
Intelligence derived from the scientific and technical 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. (NATOTerm)

measure of effectiveness
A criterion used to assess changes in system behaviour, capability, or operating environment, tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. (NATOTerm)

measure of performance
A criterion that is tied to measuring task accomplishment in order to assess friendly actions. (NATOTerm)

mission audience analysis
The focused understanding of target audiences in support of a mission or task to create the desired planning effect. (JDP 0-01.1)

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

operational intelligence
Intelligence required for the planning and conduct of campaigns at the operational level. (NATOTerm)

organized crime
Sustained illegal activities by an enterprise or group of persons, irrespective of national borders, and that have as their primary purpose the generation of profits. (NATOterm)

priority intelligence requirement
An intelligence requirement for which the commander has an anticipated and stated priority in their task of planning and decision-making. (NATOTerm)

processing
In joint intelligence, surveillance and reconnaissance usage, the conversion of collected data and information into appropriate readable or useable formats that enable further exploitation, storage or dissemination.
Note: Processing is the third step in the joint intelligence, surveillance and reconnaissance process that consists in the following five steps: task, collect, process, exploit and disseminate. (NATOTerm)

public
An individual, group or entity who is aware of activities that may affect the attainment of the end state. (NATOTerm)

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

sabotage
In intelligence usage, acts intended to injure, interfere with, or cause physical damage in order to assist an adversary or to further a subversive political objective. (NATOTerm)

scientific and technical intelligence
Intelligence derived from foreign developments in basic and applied scientific and technical research and development, including engineering and production techniques, new technology, weapons systems and their capabilities. (NATOTerm)

security
The condition achieved when designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion, terrorism and damage, as well as against loss or unauthorized disclosure. (NATOTerm)

security intelligence
Intelligence on the identity, capabilities and intentions of hostile organizations or individuals who are or may be engaged in espionage, sabotage, subversion, terrorism and organized crime. (NATOTerm)

signals intelligence
Intelligence derived from electromagnetic signals or emissions.
Note: the main subcategories of signals intelligence are communications intelligence and electromagnetic intelligence. (NATOTerm)

situational awareness
The knowledge of the elements in the battlespace necessary to make well-informed decisions. (NATOTerm)

source
In intelligence usage, a person from whom or thing from which information can be obtained. (NATOTerm)

specific intelligence requirement
An intelligence requirement that supports and complements each priority intelligence requirement and provides a more detailed description of the requirement. (NATOTerm)

stakeholder
An individual, group or entity who can affect or is affected by the attainment of the end state. (NATOTerm)

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. (NATOTerm)

subversion
Action or a coordinated set of actions of any nature intended to weaken the military, economic or political strength of an established authority by undermining the morale, loyalty or reliability of its members. (NATOTerm)

surveillance
The systematic observation across all domains, places, persons or objects by visual, electronic, photographic or other means. (NATOTerm)

tactical intelligence
Intelligence required for the planning and execution of operations at the tactical level. (NATOTerm)

target
1. In intelligence usage, a country, area, installation agency or person against which intelligence activities are directed. (NATOTerm)
2. An area, infrastructure, object, audience or organization against which activities can be directed to create desired effects. (NATOTerm)

target audience analysis
The focused examination of targeted audiences to create desired effects. (NATOTerm)

targeting
The process of selecting and prioritizing targets and matching the appropriate response to them, taking into account operational requirements and capabilities. (NATOTerm)

technical intelligence
Intelligence concerning foreign technological developments, and the performance and operational capabilities of foreign materiel, which have or may eventually have a practical application for military purposes.
Notes: Technical intelligence is a subset of scientific and technical intelligence. (NATOTerm)

terrorism
The unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives. (NATOTerm)

Designed by the Development, Concepts and Doctrine Centre

Published by the Ministry of Defence
This publication is also available at www.gov.uk/mod/dcdc

The material in this publication is certified as an FSC mixed resourced product, fully recyclable and biodegradable.