Ministry of Defence

Joint Doctrine Note 1/23

Intelligence, Surveillance and Reconnaissance

Joint Doctrine Note 1/23

Intelligence, Surveillance and Reconnaissance

Joint Doctrine Note 1/23 (JDN 1/23),
dated January 2023, is promulgated as directed
by the Chiefs of Staff

Head Doctrine

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. UK policy is to adopt North Atlantic Treaty Organization (NATO) doctrine wherever possible. Allied Joint Publication (AJP)-2.7, *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance* details the NATO joint intelligence, surveillance and reconnaissance (ISR) process. The decision to proceed with a national ISR doctrine publication reflects the desire to provide significant additional detail on the UK's approach to ISR following the publication of the *Defence ISR Strategy*.[1] Joint Doctrine Note (JDN) 1/23, *Intelligence, Surveillance and Reconnaissance* therefore attempts to capture concepts of current and future developments in ISR and draws together elements of existing doctrine and best practice. This JDN is also intended to be exploratory in nature and includes principles and concepts that are not yet wholly agreed.

Context

2. The conduct of military operations has always been shaped by the requirement to fully understand the range of audiences. ISR supports the development of this understanding. It is fundamentally about data, information and intelligence, but the transition from an Industrial to an Information Age has presented ISR with the challenge of how best to leverage the burgeoning information environment in support of military operations.

Audience

3. JDN 1/23 is written with the following audiences in mind. Primarily, it informs senior commanders about how ISR staff can support their operations. Secondly, it provides the opportunity for commanders at all levels to understand the value of ISR. Thirdly, it provides a reference point alongside Allied joint doctrine for Defence ISR and intelligence specialists. Finally, it provides external readers with an explanation of Defence ISR functions.

1 Ministry of Defence, *Defence Intelligence, Surveillance and Reconnaissance (ISR) Strategy*. Referred to as the *Defence ISR Strategy* throughout.

Structure

4. JDN 1/23 is divided into six chapters and a supporting lexicon. An outline of the contents is described below.

a. Chapter 1 introduces several fundamental ISR concepts, including task, collect, process, exploit and disseminate (TCPED).

b. Chapter 2 describes the core elements of tasking, detailing the key roles within the tasking process.

c. Chapter 3 covers collection within the TCPED process, including collection characteristics and methods. It also includes planning and conducting collection activity.

d. Chapter 4 describes processing, exploitation and dissemination and how these processes may be undertaken.

e. Chapter 5 introduces problem-centric ISR supported by activity-based intelligence, which reflects the *Defence ISR Strategy* that identifies this approach as its preferred future means of conducting ISR. It also examines automation, artificial intelligence and machine learning.

f. Chapter 6 covers applying the ISR process within the wider operations planning process.

Linkages

5. JDN 1/23 is intended to be read in conjunction with other Allied and national joint doctrine publications to provide wider context. These include:

- Joint Doctrine Publication 2-00, *Intelligence, Counter-intelligence and Security Support to Joint Operations*, 4th Edition;[2]
- AJP-2, A*llied Joint Doctrine for Intelligence, Counter-Intelligence and Security*;
- AJP-2.7, *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*;

2 The 4th Edition is due to publish in 2023.

- Allied Intelligence Publication (AIntP)-14, *Joint Intelligence, Surveillance and Reconnaissance Procedures in Support of NATO Operations*; and

- AIntP-16, *Intelligence Requirement Management and Collection Management*.

Contents

Chapter 1

Chapter 1 describes a number of intelligence, surveillance and reconnaissance (ISR) fundamental concepts. It introduces the task, collect, process, exploit and disseminate process and details the main principles and capabilities underpinning ISR as well as outlining some limitations that planners should be aware of.

1

> The biggest change in warfare at the operational level since the first Gulf War in 1990-1 has been what are often called joint enablers… Armed forces have a greater capacity to conduct reconnaissance, to use the intelligence that they so acquire to identify targets (and to do so correctly), and then to kill or destroy them with relatively little collateral damage.

Sir Hew Strachan, *The Direction of War*, 2013

Chapter 1

Intelligence, surveillance and reconnaissance fundamentals

Section 1 – Introduction

1.1. **Purpose.** Intelligence, surveillance and reconnaissance (ISR) is an integrated activity that 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, effectors and intelligence analysts. The ISR process delivers three primary outputs: support to operations; support to intelligence; and support to targeting.[1]

1.2. **Joint ISR definition.** Within Allied joint doctrine, the term joint intelligence, surveillance and reconnaissance (JISR) is defined as: 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.[2] Allied joint doctrine further explains JISR and the constituent elements, which are outlined below.[3]

a. **Intelligence.** The intelligence component of JISR refers to all intelligence collection disciplines, including their collection, processing, exploitation and dissemination capabilities/assets and the results they can deliver to the commander and staff elements. Intelligence may also be referred to as the resulting outcome of analysed information when used to support decision-making.

b. **Surveillance.** Surveillance refers to the systematic observation across all operational domains, the information environment and across the cognitive, physical and virtual dimensions of places, persons or objects by visual, electronic, photographic or other means. Surveillance

1 *Defence ISR Strategy*, page 11.
2 NATOTerm.
3 See Allied Joint Publication (AJP)-2.7, *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*.

may occur over a wide area or can focus upon a particular location, object or actor.

c. **Reconnaissance.** Reconnaissance is 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. Reconnaissance is directed observation in time, space and across the electromagnetic spectrum to obtain specific data or information required for a specific purpose. Reconnaissance particularly supports audience analysis through obtaining information or relevant characteristics of particular audiences.

Section 2 – The intelligence, surveillance and reconnaissance process

1.3. **Overview.** The ISR process is the means through which ISR capabilities are tasked and ISR operations are planned and executed to deliver the outcome desired by a commander. The ISR process consists of five subordinate processes: task, collect, process, exploit and disseminate (TCPED). These processes are neither linear nor circular in their conduct but are dynamically employed depending on the required outcome. The subordinate ISR processes can be employed sequentially, concurrently or independently, as shown in Figure 1.1.

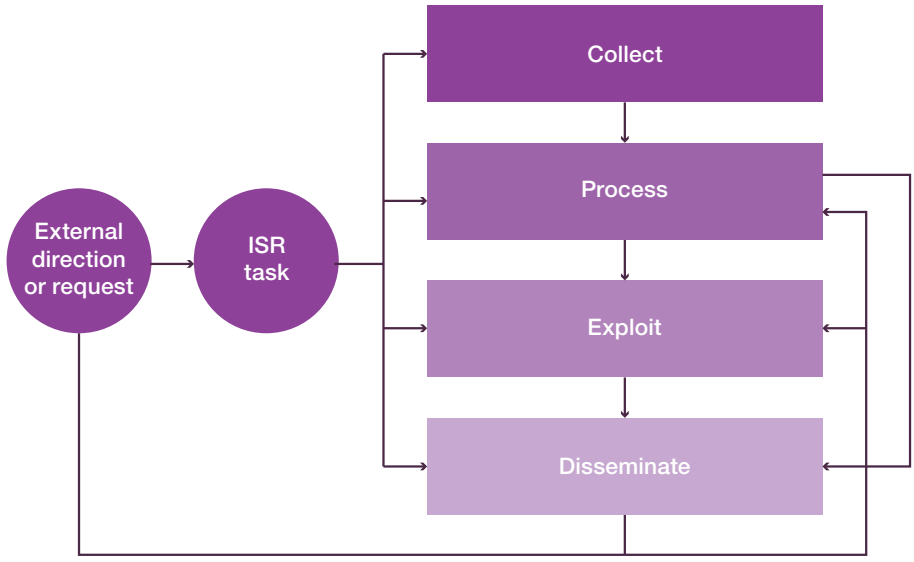


Figure 1.1 – The intelligence, surveillance and reconnaissance process

1.4. **Task, collect, process, exploit and disseminate.** The constituent elements of the ISR process are summarised below. They are described in detail in Chapters 2, 3 and 4.

a. **Task** – receiving external direction, and internal planning, resourcing, management and allocation of ISR capabilities (including processing, exploitation and dissemination (PED) capabilities), against the outcomes required.

b. **Collect –** gathering information by ISR capabilities. These can include technical and human sensors to deliver raw data.

c. **Process –** translating 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 –** exploiting data or information to derive value and attribute value from and to it. This process may also identify the requirement for additional data or information.

e. **Disseminate –** providing access to data, information and intelligence resulting from collect, process and exploit processes. Access may be in near real time or sequentially following more rigorous processing and exploitation.

Section 3 – Roles and missions

1.5. **ISR outputs.** The ISR process collates and prioritises requirements from intelligence, operations and targeting staff. This is carried out in line with command priorities and direction, before planning, optimising and executing ISR missions, employing surveillance and reconnaissance activity to generate data. This data may be the final product or it may be further refined into information and intelligence during processing and exploitation phases before dissemination to an end user. ISR exists to provide the right data to the right user at the right time to support decision-making, creation of effects and conducting operations.

1.6. **ISR and support to operations.** All ISR activity supports operations and must be driven by operational priorities. This activity can directly support operations and planning staff or be conducted indirectly through support to

wider intelligence and target development activities. Direct support takes the form of providing data, information and intelligence that flows from the ISR process into the operation and plans processes without passing through other staff processes first. In supporting operations, examples include providing real time monitoring and direct passage of situational awareness and force protection information to a commander or other force elements, or providing data and information that is used to employ effects in a combat engagement. Support to planning includes providing data and information that enables decisions on manoeuvre, for example, topographical or environmental information.

1.7. **ISR and intelligence development.** ISR supports intelligence development by providing general situational awareness on which the intelligence staff rely to contextualise reporting and on which to base their assessments. This creates the foundation for undertaking the joint intelligence preparation of the operating environment process. Through formal tasking processes, ISR supports the intelligence development process by providing collected data and information to assist in satisfying intelligence requirements.

1.8. **ISR and targeting.** ISR support to targeting may also be both direct and indirect. Indirect support is the provision of data, information and intelligence which is then used in the intelligence cycle for supporting targeting and the creation of effects, or for enhancing situational awareness. This can include providing data and information required for creating effects, for example, target acquisition, the near real time provision of coordinates, or target designation to a sufficient fidelity for employing a given effector. ISR also supports timely and accurate measures of effect, including battle damage assessment.

1.9. **Relationship between the intelligence and operations cycles and task, collect, process, exploit and disseminate.** The ISR process is synchronised with the intelligence and operations decision cycles. Although TCPED 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 1.2 illustrates the alignment of the ISR process and the intelligence and operations decision cycles.[4]

4 AJP-2.7, *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*, Edition A, Version 2, page 6, Figure 1.2.

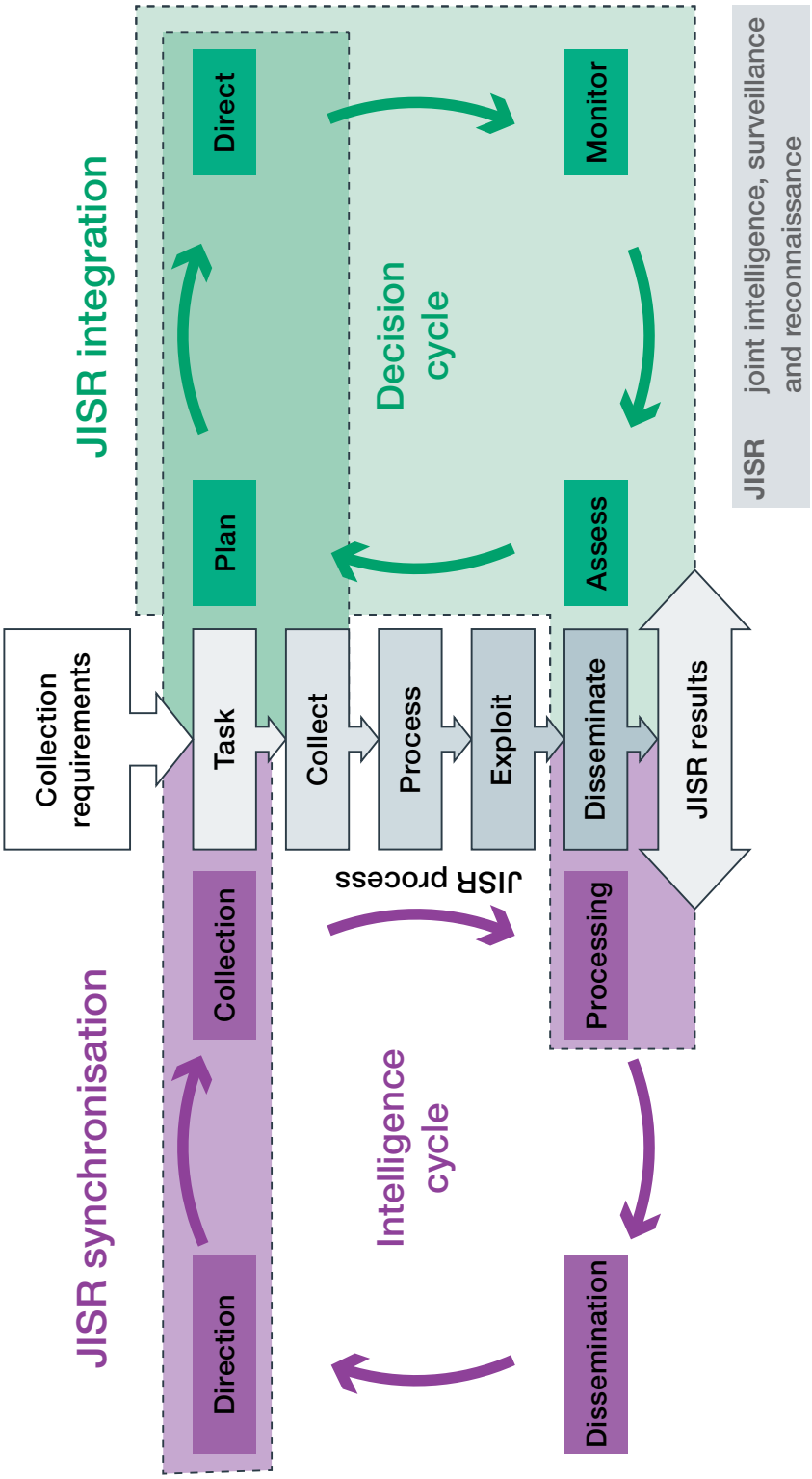


Figure 1.2 – Intelligence, surveillance and reconnaissance synchronisation and integration

1.10. **ISR mission sets.** ISR undertakes several missions sets. Examples of these mission sets that support the three broad ISR roles are listed in Table 1.1.

Representative intelligence, surveillance and reconnaissance mission sets	
Direct support to operations	Support to dynamic targeting
	Force protection and overwatch
	Support to fixed-point security
	Support to high-value target targeting
	Support to measures of effectiveness
Support to intelligence development	Provision of indicators and warnings
	Support to joint intelligence preparation of the operating environment
Support to targeting[5]	Target discovery and development
	Target acquisition
	Support to battle damage assessment

Table 1.1 – Intelligence, surveillance and reconnaissance mission sets

1.11. **ISR and non-ISR activities.** ISR activities are all activities undertaken within the missions included in Table 1.1. ISR capabilities can be used for other operationally relevant purposes than these missions, for example, reinforcing posture, presence or profile, or for messaging. However, their use for purposes other than ISR missions does not constitute an ISR activity, but the use of an ISR asset for a non-ISR activity.

Section 4 – Intelligence, surveillance and reconnaissance as a single enterprise

1.12. **The *Defence ISR Strategy* and the single intelligence environment.** The *Defence ISR Strategy* and the UK single intelligence environment seek to harmonise all elements of the ISR operations and intelligence process. The aim is to achieve the optimal use of intelligence specialists, agencies, sources and activities to produce the best possible support to decision-makers.

5 See also Joint Service Publication 900, *UK Full Spectrum Targeting Policy*.

1.13. **Past approaches.** In previous eras ISR was divided across strategic, operational and tactical levels of command, across operational domains and across numerous intelligence disciplines, based on the type and complexity of sensors and platforms. Similarly, the conduct of ISR previously varied significantly depending on the threat, adversary or character of an operation; for instance, ISR for counterinsurgency was conducted differently to the strategic surveillance of state-based competitors, and often with different capabilities.

1.14. **ISR support across operational domains and levels of command.** The changing nature of the data environment, ISR technologies and the character of military operations means that divisions between operational domains now lead to suboptimal operational outcomes. Maritime, land, air, space, and cyber and electromagnetic domain-based ISR capabilities may also have significant efficacy in simultaneously supporting all other operational domains. Technological developments in collection capabilities also now mean that one collection task can collect information or data relevant to all three levels of command. However, what may differentiate intelligence as being strategic, operational and tactical is whether a decision that is made using that intelligence is made at the strategic, operational or tactical level. ISR capabilities and processes are therefore best used entirely agnostic of operational domain or level of command.

1.15. **ISR as a single enterprise.** The realisation of the *Defence ISR Strategy* and the single intelligence environment will see ISR operate as a single enterprise that uses the right capabilities, at the right time, to deliver the most economical and effective support of the outcomes required. This requires the dynamic and flexible employment of ISR and integration across all levels and operational domains. The applicability of different means of ISR collection across differing conflict types and command levels is represented at Figure 1.3. Traditional ISR approaches to state-based threats held many sensors at the strategic level and many of the information requirements were viewed as being strategic and operational. Access to information was greatest at the higher levels and there was a reliance on pushing information and intelligence downwards. This model was reversed for operations to counter violent extremist organisations, counterterrorism and stabilisation operations with control of many sensors pushed to the tactical level and much of the relevant information being collectible and accessible at the tactical edge. This resulted in an upwards pull of information and data for decision-makers at higher levels. The current and future operational environment will be characterised by data and information being ubiquitous. Capability and operational domain-agnostic sensing will be pervasive at all levels and information flows will be access-based, rather than hierarchical.

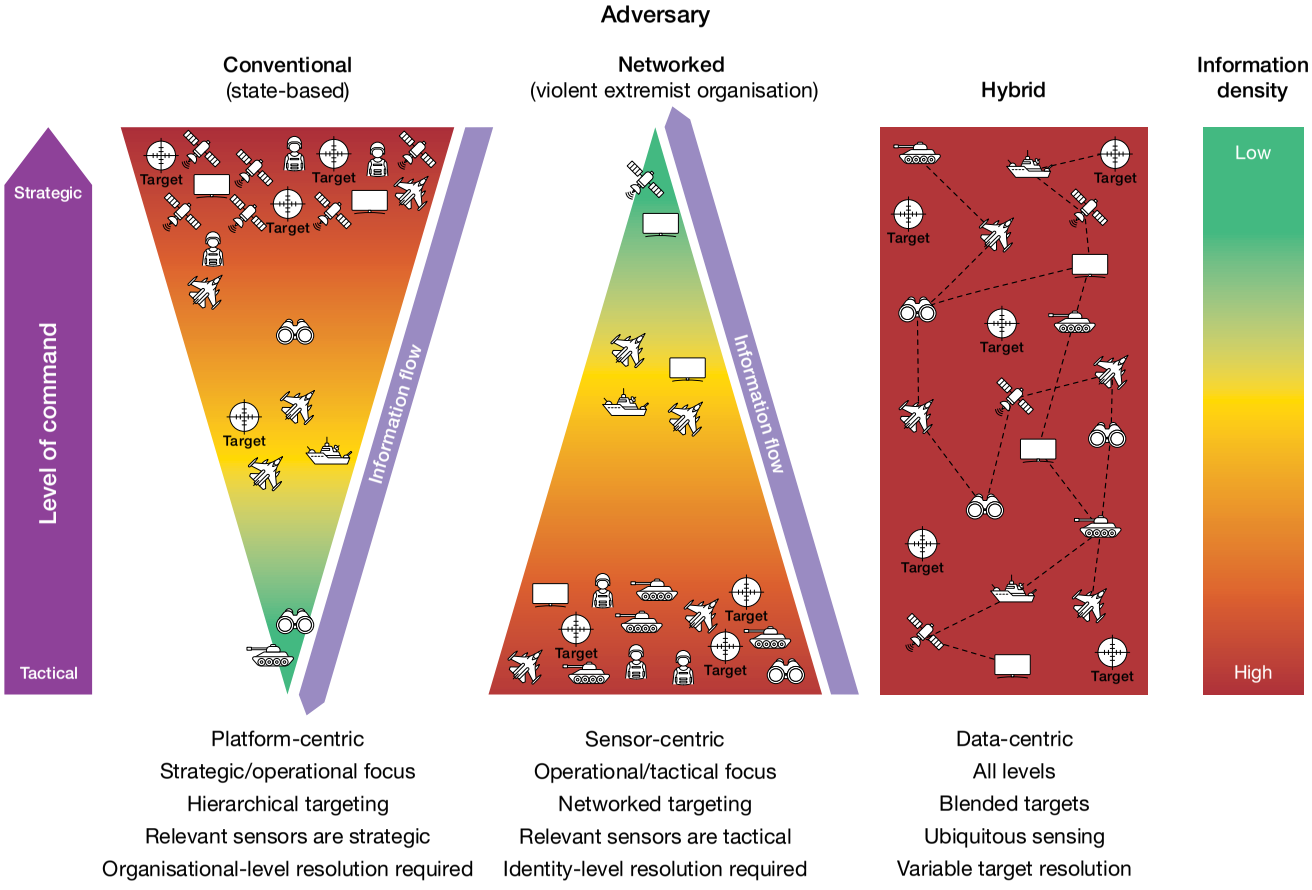


Figure 1.3 – Examples of variable intelligence, surveillance and reconnaissance collection approaches[6]

6 Figure developed from National Research Council of the National Academies, *Capability Planning and Analysis to Optimize Air Force Intelligence, Surveillance, and Reconnaissance Investments*, 2012, page 49, Figure 3.2.

1.16. **ISR capability composition.** ISR capabilities may be provided as complete force elements, but will more likely be composite, drawing on multiple units, sensors, platforms and PED capabilities to deliver an ISR capability. ISR capabilities are not limited to platforms with technical sensors such as ships, vehicles, satellites and aircraft. A human intelligence source handling capability, foot patrol or use of publicly available information data from social media are all equally valid ISR capabilities.

a. **ISR platforms, assets and lines of effort.** An ISR platform is a physical or virtual object, organisation or unit with a specific and designated ISR role. An ISR asset is the lowest level of ISR resource that can be tasked; for some capabilities such as human intelligence, open-source intelligence or PED units, the asset could be a single line of effort generated by a unit.

b. **Composite approaches.** The ability to task organise differing platforms or assets to generate an ISR capability increases the complexity of the command, control mechanisms and communications architectures required. However, composite approaches may increase flexibility, resilience and achieve greater outcomes as force elements can be organised for best effect. For example, a PED unit may be able to support multiple sensors or collectors, thus maximising outputs by aligning to different collectors as they conduct missions.

c. **ISR task lines.** A task line is typically a 24-hour block of a given capability. For example, if an uncrewed aircraft system has an on-mission time of 12 hours, two sequential missions would be required to provide a single task line.

Section 5 – Principles

1.17. ISR follows eight key principles. These principles are appropriate at all levels or command, across all operational domains and across the full range of operations.

a. **Integrated.** ISR activities must be integrated, command-led and centrally coordinated to set the conditions for mission success, while enabling mission command by permitting delegation of ISR planning and execution. Commanders set an intent, priorities and direct the ISR effort to meet operational requirements.

b. **Responsive.** ISR must be responsive and flexible to satisfy the needs of the supported activity. The ISR process must dynamically respond to evolving situations, new information and revised requirements. ISR capabilities are employed flexibly using massing, layering, cross-cueing and fusion of all capabilities as a single enterprise, across levels of command, operational domains and components.

c. **Discoverable and accessible.** ISR is available for tasking and ISR outputs are accessible. Enterprise architecture should be integrated and interoperable to allow timely and seamless access to ISR-derived data, information and intelligence at the point of need.

d. **Data-centric.** All data must be fully used. To enable this, data must be fully contextualised, available and discoverable across boundaries. Data-centricity requires interoperable data systems and common data standards. It also requires systems that enable faster, wider and deeper access to intelligence, information and data sources via means that are both intuitive and user friendly.

e. **Sustainable.** ISR capabilities need to be sustainable to meet mission requirements. Persistent and survivable ISR capabilities are required to satisfy the information requirements of commanders and their staff in planning and executing operations. In the event that an asset is destroyed, disabled or becomes unavailable, commanders need to consider how to compensate for the loss of ISR capabilities. In addition, commanders need to consider how to resource and sustain continuous PED operations.

f. **Reliable.** Measures of reliability are established for ISR capabilities to give commanders and their staff confidence in ISR results. Measures of probability also need to be established to determine to what extent an ISR capability can collect the data and information required. PED elements will need to provide timely results to contribute to maintaining accurate situational awareness and understanding, therefore allowing commanders to maintain decision advantage.

g. **Resilient.** The ISR enterprise should have the capability to operate within contested, constrained and degraded environments. It should be able to operate with the loss of some capabilities while still providing mission critical outputs. Resilience is achieved through creating an

appropriate ISR operational design, using appropriate tactics, building redundancy into planning, and through the appropriate and economical employment of ISR resources.

h. **Accurate.** ISR results must answer information requirements in the most accurate way possible. Accuracy must be maintained continuously throughout every step of the ISR process, from tasking through collection, processing, exploitation and dissemination. Objective, clear, unbiased and undistorted ISR outputs are critical to support subsequent multi-source and all-source intelligence analysis, as well as to prevent reliance on single source confirmation or circular reporting.

Section 6 – Limitations and contemporary challenges

1.18. **Limitations.** ISR is subject to four main limitations. The applicability of these limitations varies according to the operational situation.

a. **Mass.** There may not be sufficient ISR resource available to meet all requirements. Some collection capabilities are low in density but in consistently high demand. PED also has a finite capacity.

b. **Technical capability.** Despite the rapid and continuous evolution in sensor capabilities, some environments and types of target present challenges that technology cannot yet provide assured solutions for. Overcoming these challenges often requires a blended approach, using numerous sensors and sensor types which consumes limited resources. The ability to process, exploit and disseminate the results of collection is also limited by technical constraints such as computational power and communications bandwidth.

c. **Adversary action.** Adversaries may limit our ability to conduct ISR activity by targeting collection and PED capabilities using kinetic effects, electromagnetic attack and information operations. Such operations may also include camouflage, concealment and deception efforts aimed at hiding from observation (across all areas of the electromagnetic spectrum), deceiving sensors and attempting to lead analysts to false conclusions through misinformation.

d. **Access.** The ability to conduct ISR activities may be limited through the lack of physical, cognitive and virtual access or due to legal constraints, policy or permissions. Threats may deny access for sensors or platforms, or access to the data they generate through targeting communications. Legal, policy and profile, posture and presence considerations may also determine access to collection capabilities and to relevant data, particularly during operations other than international armed conflict.

1.19. **ISR and the information environment.** The transition to an Information Age and the characteristics and dynamics of the information environment have presented fundamental change and challenge for how ISR is conducted. The new information environment and the growth in data in the contemporary environment provides specific challenges for ISR based on the variety, volume, velocity and veracity of data. These challenges are listed below.

a. **Variety.** The increasingly numerous and disparate forms and sources of data.

b. **Volume.** The scale of data in its entirety and the relative size of individual pieces of data.

c. **Velocity.** The rate at which data is created, mutated and erased, and the resulting latency between point of collection and point of receipt.

d. **Veracity.** The increasing ambiguity of data and difficulty in determining its accuracy and validity due to its variety, volume and velocity.

1.20. **Problem-centric ISR and activity-based intelligence.** The *Defence ISR Strategy* expands the use of problem-centric ISR supported by activity-based intelligence in response to the challenges posed by increased data. This is explained in Chapter 5.

Key points

- ISR is an activity that supports operations by sensing objects and events and it provides data and information to support decision-making.
- The ISR process comprises: tasking, collection, processing, exploitation and dissemination.
- ISR has three core outputs: support to operations, support to intelligence development, and support to targeting.
- ISR in the contemporary environment should be viewed as a single enterprise, not artificially divided between levels of operation or operational domains.
- The growth of big data in the contemporary operating environment presents specific challenges for ISR relating to the variety, volume, velocity and veracity of data.

Chapter 2

Chapter 2 describes the core elements and roles within the intelligence, surveillance and reconnaissance tasking process.

2

> All the business of war, and indeed all the business of life, is to endeavour to find out what you don't know from what you do; that's what I called "guessing what was at the other side of the hill".

Arthur Wellesley, 1st Duke of Wellington, 1852

Chapter 2

Tasking

Section 1 – Introduction

2.1. **Overview.** The intelligence, surveillance and reconnaissance (ISR) process starts with the receipt of validated, prioritised tasking and requests. These will likely be from multiple users, including the operational and intelligence staff within the headquarters, subordinate, lateral and higher units and formations. This initiates the collection management process. The collection management process comprises two subordinate functions – collection requirements management (CRM) and collection operations management (COM).

2.2. **Key requirements.** The collection management process is dependent on the commander communicating a clear intent, plan and prioritisation for ISR. There is rarely sufficient ISR resource to satisfy all requirements, therefore prioritisation is critical. Equally important is a constructive and close relationship with the operations, joint effects and intelligence staffs that submit requirements, and especially with the intelligence requirements management staff. Poor requirements slow down the ISR process, lead to inefficient use of limited resources and can result in suboptimal outcomes. Close and constructive coordination between the staffs ensures that appropriate advice can shape requirements prior to submission. Intelligence requirements management and operations staff have a responsibility to apply due diligence when submitting requirements to avoid unrealistic, duplicative and uncollectable requirements.

Section 2 – Collection requirements management

2.3. **Receipt of ISR tasking requests.** All tasking and requests for ISR are initially subject to CRM. CRM staff must be trained ISR practitioners and understand the operations, planning and intelligence functions. They require specialist knowledge to identify credible from unrealistic requirements. The

CRM staff will undertake a series of actions upon receipt of a tasking request; these are described below.

a. **Task validation.** CRM staff will validate the tasking or requirement and ensure it is complete and from a valid source. Where tasking and requests are invalid, unworkable or where there is no authority to task or request, the CRM staff return the tasking back to the originator. Feedback, guidance and assistance are provided to assist in a resubmission where appropriate.

b. **Tasking check.** CRM staff will check the requirement against existing previous taskings and planned ISR activity to ensure that the requirement is not duplicative, has not already been met and cannot be answered without new activity. If the CRM staff believe the requirement can be met from the results of previous or planned activity they liaise with the originator to ensure they are aware and close the requirement. Where two originators have the same requirement the task remains valid but is attributed against both originators and is merged into a single requirement.

c. **Request validation.** CRM staff will ensure the requirement contains the level of detail necessary and is realistic and achievable. Where insufficient detail is provided or where requirements are unrealistic, the CRM staff return the tasking to the originator. Feedback, guidance and assistance are provided to assist in a resubmission where appropriate. Requirements must be tightly bound in time, space and on the electromagnetic spectrum, and have a clear outcome.

d. **Prioritise the task.** ISR tasks will be prioritised by the CRM staff. CRM prioritisation will be in line with the commander's intent, current plans and stated priorities.

e. **Translate the request into collection requirements.** CRM staff translate an ISR request or essential elements of information (EEI) request into one or more collection requirements. The relationship between tasking and requests is not linear. One EEI request received might generate many ISR requirements for numerous capabilities. Alternatively, one collection requirement might be able to service several EEI requests.

f. **Compile the collection requirements list.** CRM staff compile collection requirements for their own, subordinate and higher headquarters directed ISR requests into a collection requirements list. Where any other issues are found with received tasks and requests, they are returned to the originator and feedback, guidance and assistance are provided to assist in resubmission.

2.4. **Capability to requirement matching.** On completion of a collection requirements list the CRM staff then match capabilities against requirements in the most efficient manner possible. This is a highly technical process that requires considerable expertise and a broad and deep understanding of both organically held ISR capabilities and those held by subordinate, lateral and higher units, formations and headquarters.

2.5. **Generating collection tasks.** To generate tasks, collection management staff require validated requirements derived from a collection requirements manager, and the authority to task organic capability and request external capability. They also require current information on the numbers and availability of ISR capabilities from ISR-owning units, formations and headquarters. Additionally, a collection manager requires an understanding of the range of likely ISR targets, potential and existing threats to ISR capability and an understanding of ISR tactics.

2.6. **Capability to requirement matching process.** There are various approaches to resourcing tasks but all involve breaking down a requirement into constituent planning considerations to understand what capabilities are best suited to meet the requirement. The start point for this process is understanding the outcome or end state required in terms of data, information or intelligence arriving with the requester at the right time and in a manner that meets their needs. Collection management is therefore about more than collection, but also planning and the end-to-end employment of capabilities and platforms, including subsequent processing, exploitation and dissemination (PED) and the supporting communications architecture.

2.7. **Assigning capabilities – collection requirements management considerations.** A structured analysis of requirements allows the collection manager to identify the ISR capability for servicing the requirement. This might be as broad as airborne imagery intelligence or maritime electromagnetic intelligence, or as detailed as a specific sensor on a specific platform. The collection manager will work through the collection requirement list in priority order and attribute capability against requirements until all ISR resource has

been exhausted. The factors a collection manager will assess when assigning a capability to a requirement are detailed in Table 2.1.

Collection manager considerations	
Requirement	What does the requester want, in what format and when?
Communications	What means has the customer got of receiving data, information and intelligence and at what classification?
Task	What is the task? Surveillance or reconnaissance?
Target	What is the target? Object or event? What are its observable characteristics in time, space and spectrum?
Sensor	What type of sensors can observe this target?
Constraints	What constraints are there on meeting requirement? Are there environmental, meteorological, threat or policy and legal factors which restrict how the requirement is met?
Periodicity and frequency	What is the frequency of the request? Once, multiple or enduring?

Table 2.1 – Collection requirements management considerations

2.8. **Outstanding requirements.** Invariably there will be insufficient capability to satisfy all requirements; collection managers will have to apply an initial threshold below which requirements will not be met. The collection manager will then look at opportunities which arise to satisfy more requirements from within the resource available. For instance, a collector might be assigned against a high priority target but could pass several low priority targets as it moves to the area of its primary task (known as collect in transit). These targets could therefore be satisfied by the same capability. The collection manager looks at how capability can be manoeuvred and sequenced to deliver against the greatest number of requirements.

2.9. **Use of non-traditional ISR and non-dedicated ISR.** ISR capability is a precious and often scarce resource so must be carefully managed and used in line with the commander's operational design and priorities. This will invariably result in many requirements going unfulfilled due to a lack of capacity or capability being allocated elsewhere. Collection managers will therefore consider all means of resourcing requirements, including non-traditional ISR and non-dedicated ISR. Non-traditional and non-dedicated ISR are explained in greater detail in Chapter 3.

2.10. **Non-interference based collection.** While there is rarely enough capability to satisfy all requirements, the specific tasking of a given platform or asset may result in it having spare capacity. Non-interference based (NIB) collection refers to the deliberate tasking of a capability beyond the primary tasking specified in its orders. The asset is given the task to service on an opportunity basis and on the basis that it does not interfere with its primary tasking. As such, there is no assurance that the task will be undertaken and NIB collection should therefore never be used on tasks that require assured output.

2.11. **Unresourced requirements.** Following rationalisation, some requirements will remain unresourced or under-resourced due to lack of priority, capacity or capability. If the requirement can only partially be met the collection manager liaises with the relevant staff to see if partial fulfilment remains worthwhile and should be taken forward as a task.

2.12. **Failed requirements.** A requirement may remain unresourced for two reasons: firstly, because it has not met the priority threshold for resourcing; or secondly, because the collection manager does not have the right capability available to meet the requirement. In the case of failing to achieve priority, the requester is informed and the requirement is carried forward into the next collection management planning cycle if the requirement remains extant.

2.13. **Requirement escalation.** Where a requirement cannot be resourced due to capacity or capability considerations the collection management staff can escalate the requirement to a higher headquarters or request support laterally using an ISR request. As the CRM and collection management process is carried out at every level and for every operational domain this creates a system of interlinked headquarters which can pass requirements in the form of ISR requests upwards, downwards and laterally.

2.14. **Requirement transparency and situational awareness.** Even where requirements are being internally resourced, it is appropriate for all levels of command to have good situational awareness of higher, subordinate and lateral headquarters' requirements, plans and ISR activities. This awareness should ideally be to at least two levels above and below. This allows all headquarters to coordinate and optimise the use of all available ISR assets and ensure that any unintentionally redundant collection requirements are deconflicted. For example, a higher headquarters might employ a wide area collection platform for their own needs, thus mitigating the requirement for subordinate tactical headquarters to employ numerous, less capable platforms at the same time and in the same area. This process is often conducted using a formalised battle rhythm, culminating in a joint collection management board (JCMB).

2.15. **Variations in collection management by level.** The role of the collection manager can vary considerably by level. At the operational theatre level, collection managers may be mostly involved in broad apportionment of resource to components, formations and units. At lower tactical levels the collection manager may effectively take on the responsibility for COM. Collection tasks may therefore be developed either for specific collection disciplines (such as imagery intelligence, human intelligence, measurement and signature intelligence, open-source intelligence and signals intelligence) or for specified collection capabilities or assets.

2.16. **Task agreement and the collection task list.** When requirements have been resourced and optimised the collection management staff compile all the resulting collection tasks into a collection task list (CTL). The relationship between collection requirements and collection tasks is not linear. A single requirement might require multiple tasks across multiple operational domains and sensing types to satisfy it. Conversely, following rationalisation, one collection task might be able to satisfy multiple collection requirements. The CRM process ends with the formal handover of an agreed set of prioritised and resourced ISR tasks in the form of a CTL. The CTL is then handed to the appropriate headquarters, formations and units for refinement and execution. The CTL is the authoritative collection management document for the theatre or operation. The CTL is consistent with the commander's overall mission priorities and the theatre collection priorities. The CTL provides a list of approved and prioritised collection tasks, ISR tasks and, as required, dynamic retasking priorities. The CTL is passed to COM staff for mission planning and execution.

2.17. **Joint collection management board.** On large and complex operations the requirement for rigorous prioritisation and decisions on capability attribution may require establishing a formalised JCMB. This may be supported by a joint collection management working group (JCMWG). The JCMB or JCMWG are responsible for formalising the coordination between different Service components and intelligence and operations staffs. The JCMB issues priority guidance across the Service components to ensure that the overall ISR effort is coordinated, prioritised, appropriately balanced and focused on the commander's objectives.

2.18. **Joint collection management working group.** A JCMWG is often used as a deconfliction and discussion mechanism prior to a formalised JCMB. The JCMWG aims to collegiately manage conflicts prior to a JCMB and, where these cannot be resolved, to produce options and recommendations for endorsement by the JCMB chair. The use of a JCMWG is useful in resolving many issues at desk level and preserving the commander's time and decision space. The JCMB can then be used as a decision brief rather than a problem-solving forum. A JCMWG will normally draft the CTL or mission-type order (MTO) for endorsement at a later JCMB.

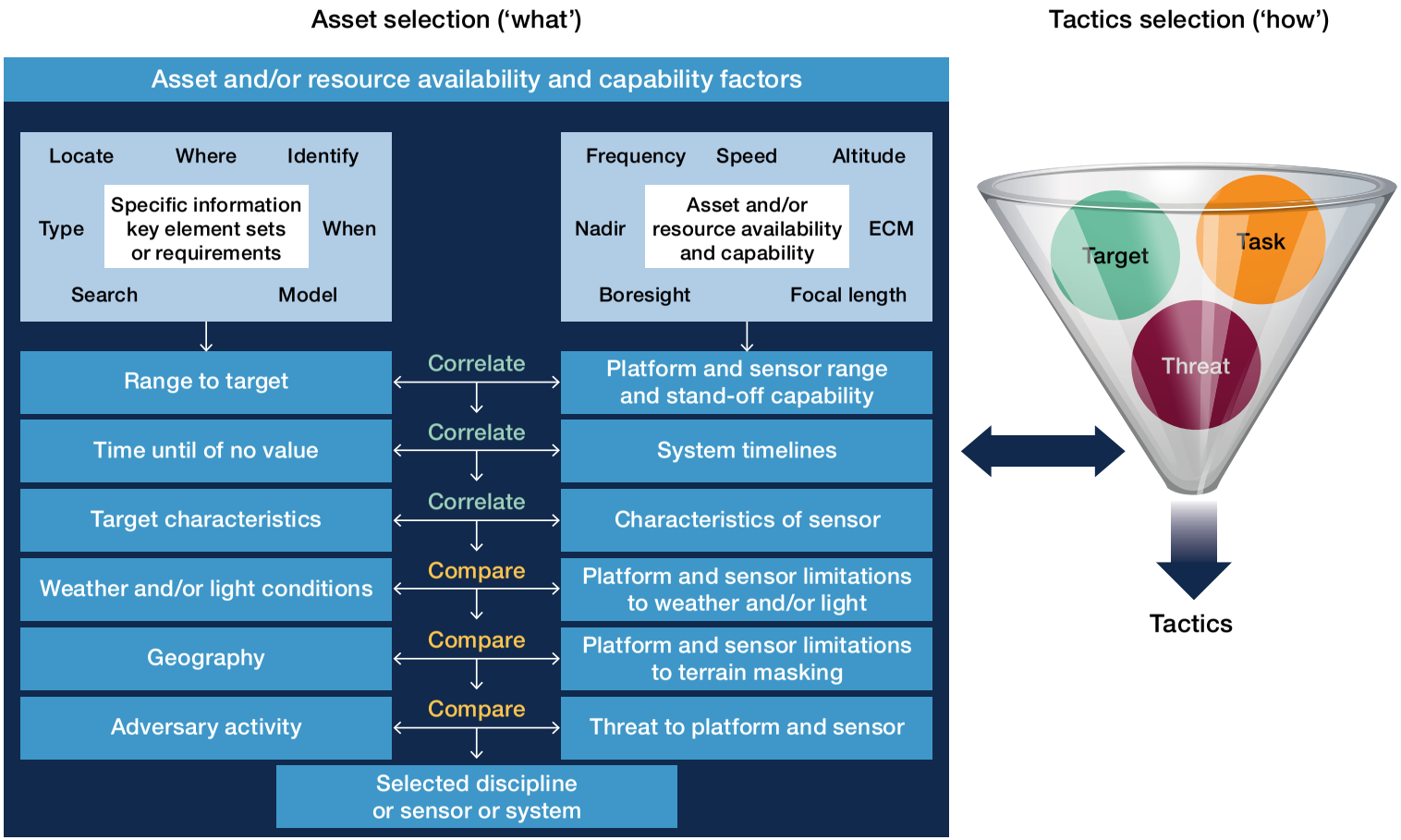
2.19. **Theatre collection and exploitation management.** In addition to the functional staff elements, a commander may choose to allocate responsibility for running the ISR process to specific roles. These are most often called the theatre collection manager (TCM) and theatre exploitation manager (TEM). They hold responsibilities for all aspects of collection and PED activity respectively. The TCM and TEM will often be responsible for organising the ISR battle rhythm culminating in the JCMWG/JCMB.

Section 3 – Collection operations management

2.20. **Overview.** COM is the process of planning and executing ISR activities. It is a combined J2 and J3 activity conducted in components, formations and units that have command and control of tasked ISR capabilities, platforms and assets. The CTL, MTO or other appropriate orders bound the commander's intent, mission and tasks in time and space. In line with the ISR principle of mission command, they instruct the recipient as to what is to be achieved, but not how it is to be done. Collection operations managers are the final authority for coordination, mission integration and issuing orders for execution. COM ensures that ISR is fully integrated into wider mission planning, with due consideration to other tactical activities such as engagement space management, force protection and logistics. This includes mission planning (future plans), mission tasking (future operations and orders) and preparing the mission at the unit level.

2.21. **Staff responsibilities.** COM staff analyse the: task, mission and intent; target of the activity; and threat and environmental factors which might influence the mission. This analysis enables credible capability employment and tactics for mission success; it requires expert knowledge of the capabilities being employed. Where tasks are being undertaken as an ISR package, using multiple platforms and capabilities, collective planning should be undertaken to ensure the optimal use of all allocated capabilities and to achieve common understanding of the mission and plan. COM staff then disseminate orders. The asset and tactics selection factors the collection operations manager and staff will consider are illustrated at Figure 2.1.[7]

7 Figure derived from United States Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations*, 5 July 2017, page 23.



ECM electromagnetic countermeasures

Figure 2.1 – Asset and tactics selection

2.22. **Planning considerations.** In addition to asset and tactic selection, there are a further range of key planning considerations that must be assessed during COM. These are detailed in Table 2.2.

Collection operations management planning considerations	
Operational priority	Common understanding by all parties of what is to be achieved. This must include the intent of the mission and the effect and/or end state desired.
Sequencing and force flows	When and where capabilities will be operating in time and space, including handover arrangements.
Detailed capability tasking	What each capability is to achieve, when and where.
Contingencies	Specific actions to take in the event of unforeseen events, such as the loss of a capability.
Command, control and communications	How command and control will occur, what communications will be used and how, including reversionary and tertiary means to ensure resilience.
Contracts/actions on	Agreed, pre-planned actions or activities which will be taken when an event, activity or object is detected. These will be in addition to those captured in standard operating procedures or where these procedures need to be adjusted.

Table 2.2 – Collections operations management planning considerations

2.23. **Communicating tasking.** The efficient and timely transmission of orders is critical in enabling ISR activities. The actual format of orders will vary according to the operational domain, command level and the ISR management architecture. A land component may use a decision support overlay and matrix, and a surveillance and target acquisition plan. An air component may, for example, use several order sets including the air tasking order, collection emphasis messages and signals intelligence emphasis messages, and the reconnaissance, surveillance and targeting annex. At the most basic level, a

tasking constitutes a validated CTL from an authorised collection manager, with a formalised command relationship over the resources to be employed. This can be further refined by using an operational order or tasking order. Commonly used orders include collection task order, PED task order and MTO.

a. **Collection task order.** A collection task order normally directs a single capability against one or more tasks on the CTL.

b. **PED task order.** A PED task order is normally used to direct a single PED capability against one or more tasks on the CTL.

c. **Mission-type order.** MTOs are used to coordinate and synchronise multiple capabilities employed against one or more tasks from a CTL. MTOs communicate the commander's intent to all ISR units and detail the relevant coordinating instructions. This is often accompanied by a coordination card as a 'carry on' document that all those participating in the activity can refer to and provides all relevant detail on how the mission will be executed.

2.24. **The end-to-end collection management process.** The collection management process outlined in Chapter 2 originating with the commander's direction and comprising CRM and COM is represented at Figure 2.2. The CRM process concludes with the issuing of orders prior to mission execution.

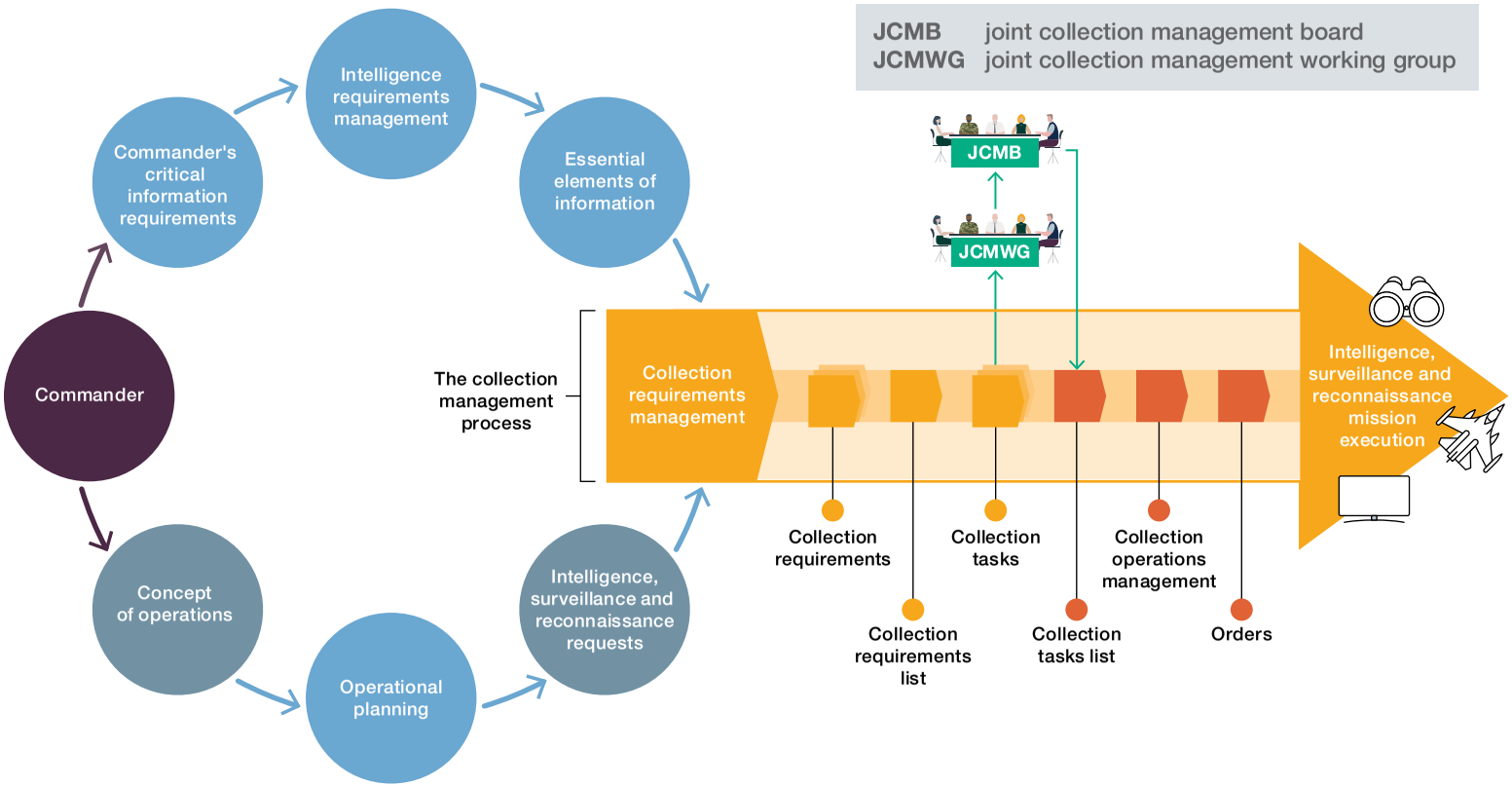


Figure 2.2 – The collection management process

Section 4 – Deliberate, ad hoc and dynamic tasking

2.25. **Deliberate, ad-hoc and dynamic tasking.** Planning can occur at various phases in an operation and is largely characterised as deliberate, ad hoc or dynamic. These terms are defined relative to the planning and mission timelines. Deliberate, ad hoc or dynamic tasking are described below and time frames differentiating them are shown at Figure 2.3.[8]

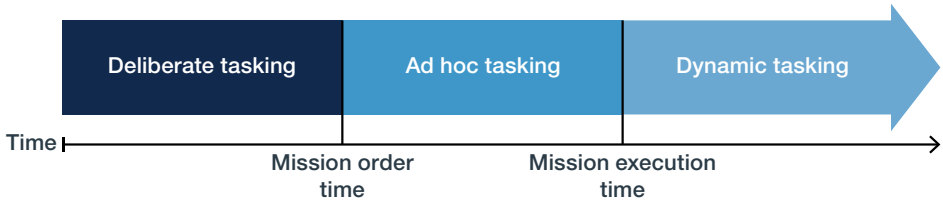


Figure 2.3 – Time frames for deliberate, ad hoc and dynamic tasking

a. **Deliberate tasking.** Deliberate ISR tasking is the typical mechanism to develop, coordinate and assign ISR tasks to ISR assets using the processes described above. It guarantees sufficient time for mission integration, mission planning, mission tasking and mission preparation. Deliberate tasking occurs during the standard mission planning process and is concluded with an approved CTL and an approved MTO by the operations staff.

b. **Ad hoc tasking.** This is the process for integrating emerging and urgent ISR requests into an already released CTL and prior to mission execution. The closer to the start of the mission execution for any given planning cycle that the ISR request is received, the higher in priority it must be deemed to be to justify the disruption to the ongoing operations planning process.

c. **Dynamic tasking.** Dynamic tasking occurs during mission execution when the importance and urgency of an emerging ISR requirement demands immediate attention and redirection and/or reallocation of a capability already on task. Dynamic tasking

8 Figure derived from Allied Joint Publication-2.7, *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance*, Edition A, Version 2, page 25, Figure 3.2.

for immediate execution is typically developed by operations staff. It requires rapid decision-making by an empowered collection operations manager who will balance the importance of the task against the commander's priorities, the current plan and capability characteristics to validate, prioritise and resource the new task.

2.26. **Ad hoc and dynamic request process.** Where timelines allow, requests inside a deliberate planning cycle should be made using existing request mechanisms. The CRM and COM staff will then conduct a rapid process to review, authorise or reject the request as appropriate. Where time does not allow for formal requests, or during mission execution, ISR can be requested dynamically by submitting an 8-liner format. Such requests are normally the result of a high priority change to the execution of a plan or the discovery of a fleeting target of opportunity. It is most common for dynamic changes to be initiated and fulfilled through secure chat communication capability between those staff requesting the change, the ISR platform controllers and COM personnel. The 8-liner request can be submitted in any agreed medium. Standard operating procedures and the guidance for collection operations managers must explicitly detail their level of authority, and detail in what circumstances decision-making must be escalated and to whom. Decisions must be captured and where possible more detail of the task captured retrospectively to inform ISR assessments.

Key points

- Tasking takes the receipt of external direction and internal planning and converts that into ISR operations. It does this through the collection management process.
- Collection management consists of two subordinate processes:
    - collection requirements management – receiving and prioritising requests and requirements and apportioning resources against these tasks; and
    - collection operations management – planning and executing ISR activities.

Chapter 3

Chapter 3 describes collection within the overall task, collect, process, exploit and disseminate process, covering the key characteristics of collection and how collection is undertaken.

3

> In the classic Boyd cycle, or 'OODA loop', high-tech sensors can help us observe, but they can only superficially help us to orientate.

Captain Paul Bethnell, 'Accidental Counterinsurgents: Nad E Ali, Hybrid War And The Future Of The British Army', *British Army Review*, 2010

Chapter 3

Collection

Section 1 – Collection characteristics

3.1. **Overview.** Collection uses sensing of all types to detect objects and events geospatially, temporally and on the electromagnetic spectrum. Collection delivers raw data, which is then subject to processing, exploitation and dissemination (PED) to generate information and intelligence. There are two general means of collecting information – human and technical sensors – conducted across all operational domains and using many means. Effective collection uses the right blend of sensing capability to deliver the required result, in the most economical manner possible.

3.2. **The characteristics of collection.** All sensors, be they human or technical have various attributes, strengths and weaknesses. However, all collection can be defined in terms of the characteristics below.

a. **Type.** The type of sensing used and how objects and events are detected. The type of sensor will vary significantly according to the collection disciplines.

b. **Range.** The distance at which a sensor can reliably detect the required object or event at the fidelity, accuracy and latency required.

c. **Persistence.** The amount of time a sensor can be employed before it needs to be removed from task. Interruptions might be caused by the requirement to refuel, for maintenance or to download data.

d. **Ubiquity.** The ability to detect over the desired geographic, temporal and spectral area to be covered, influenced by the field of view and field of regard of the sensor. Sensors can either stare at a location or can be slewed to cover greater areas at the expense of ubiquity and persistence.

e. **Fidelity.** The ability of the sensor to detect objects or events of a given characteristic, for example, the ability to differentiate between a man, woman and child or different types of vehicles. Fidelity can be

affected by range and persistence. Increasing fidelity increases the ability to detect, recognise, classify or identify a person or object.

- **Detect.** The ability to determine whether something is present or not present.
- **Recognise.** The ability to make broad observations as to the type of object or event, for example, a motor vehicle.
- **Classify.** The ability to make a more refined judgement as to the type of object or event, for example, a car.
- **Identify.** The ability to determine with a higher degree of confidence the exact type of object or event, for example, a specific make and model of car.

f. **Accuracy.** The spatial, temporal or spectral resolution of the sensor. For instance, if it can geolocate the observed object or event to within 1 metre or 1,000 metres of its actual location. Accuracy may be affected by range and persistence.

g. **Latency.** The speed from the point of collect at which the detection can be relayed for use. For example, a wet film camera requires developing which delays the image's availability compared with digital cameras.

Section 2 – Collection methods

3.3. **Mission and incidental collection.** Mission collection is the detection of objects and events specifically requested or required by mission tasking. Many collection capabilities, especially those with high persistence and ubiquity, will also collect on significantly more than just those objects and events against which they have been specifically tasked. These additional detections are known as incidental collection. On most platforms the volume of incidental collection surpasses mission collection. While some incidental collection will clearly be of interest and be appropriately dealt with, significant volumes will have no immediate or apparent value and there is an inherent danger that such collection is discarded. It is imperative that all collection is treated as of equal value at point of collection to fully leverage PED capabilities. This is further explored in the consideration of activity-based intelligence in Chapter 4.

3.4. **Dedicated ISR.** Dedicated intelligence, surveillance and reconnaissance (ISR) is the term for capabilities, assets and platforms that have been specifically designed and task organised to conduct ISR activity. Both technical and human sensors constitute dedicated ISR. Dedicated ISR is enormously broad in scope; capabilities sense across physical, virtual and electromagnetic space and across operational domains. While some sensors may be optimised against specific targets or particular target signatures, many will have far broader application. Given the specialised nature of many ISR capabilities, it is imperative that subject matter experts are integrated into ISR planning and mission execution and provide suitable advice to broader operational planning.

3.5. **Non-dedicated ISR and non-traditional ISR.** Collection will be primarily accomplished by dedicated ISR capabilities, platforms and assets. Additionally, collection can be undertaken by non-dedicated and non-traditional sources. In some cases non-dedicated ISR (NDISR) and non-traditional ISR (NTISR) may offer particular advantages over dedicated ISR; for example, combat capabilities may be able to generate information in threat environments that preclude the use of dedicated ISR capabilities.

a. **Non-dedicated ISR.** There are many NDISR capabilities that can be used to gather data and information and fulfil requirements, even though their primary role is not ISR related. NDISR is an asset, platform or capability that could be used to deliver ISR activity, but that is not specifically designed for ISR. Many platforms have sensors used for internal or external targeting or force protection purposes that can equally be used for ISR requirements. Radar warning receivers, targeting pods and electromagnetic support measures equipment carried by platforms may support ISR through the collection of signals, imagery or electronic signature data. A key consideration for NDISR is that it often constitutes an asset or platform, rather than a capability, and may require significant planning and support to meet ISR requirements – for instance, the ability to off-board data and information and ensuring the availability of PED. There must be a demonstrable urgency or limited opportunity cost to using NDISR and it must be agreed with the asset owner as part of collection management planning.

b. **Non-traditional ISR.** NTISR differs from NDISR in that the asset employed has no specific ISR capability. It recognises that every person or platform is a potential sensor. NTISR may present unique opportunities for collection as the asset may have specific freedoms to operate where a dedicated ISR capability would not be able to.

NTISR is normally employed as a capability on low priority tasks to free up dedicated resources for other tasks, or where the deployment or activity of the NTISR asset provides specific opportunities for achieving tasks. NTISR will also not normally be able to be directly tasked by the collection management staff and will require negotiation and agreement by the asset owner.

3.6. **Publicly available information.** Publicly available information can be described as any information where there is a reasonable basis to believe that it is lawfully made available to the general public. It comprises both human and machine created data and can take the form of human-to-human, machine-to-human, human-to-machine or machine-to-machine communications.

Publicly available information as a 'game changer'

ISR has traditionally been reliant on 'exquisite' military platforms and sensors for its data. The transition from the Industrial to the Information Age has resulted in publicly available information vastly exceeding Defence sources in both the volume and variety of data and information available from public sources. Publicly available information includes social media, smart devices, the Internet, smart city sensors and machine-to-machine communications. It will fundamentally change the paradigm of ISR as it becomes more valuable, accessible and available. This will generate challenges due to the huge volume, variety and velocity of the data.

3.7. **Commercial ISR.** Commercial ISR are capabilities, assets and platforms that are either government owned but contractor operated or both contractor owned and contractor operated. Commercial ISR may take the form of an integrated ISR capability, collection or PED operating in or from any operational domain. The capabilities of commercial ISR can exceed those of both the military and government, and the use of commercial ISR is likely to continue to grow, especially collection from space and the PED of publicly available information. In many cases commercial ISR capabilities may be equivalent to or exceed those of Defence. Commercial ISR should be treated no differently for planning purposes and is subject to the same tasking mechanisms; however, the use of commercial ISR may be bound by specific factors that affect its employment. These factors might be contractual, such as the hours, locations and missions it can be employed on. Policy and legal requirements may also impose constraints, for instance, operating within particular threat environments, or involvement and contribution to certain targeting activities only. These will likely be unique to each commercial ISR provider, capability and operation.

Section 3 – Collection planning and execution

3.8. **Collection planning considerations.** Collection activity is planned and executed in the same manner as other military tasks. There are three key areas for consideration when planning collection – task, target and threat.

3.9. **Task.** This is the requirement to be achieved by undertaking the collection. This activity will be bounded by the commander's intent and the wider scheme of manoeuvre and may include both specified and implied tasks. For instance, a task may require collection in a particular location at a particular time. It may require persistence for a given period or the ability to detect a particular type of object or event. Policy, legal or other control measures such as engagement space management will also be factored into the task. Common ISR tasks and actions are shown in Table 3.1.

Task/action	Description
Find	Detect, recognise, identify and/or locate a unit, object, activity, situation, event or individual or groups.
Collect	Systematically seek and acquire (items of a particular kind).
Confirm	Provide current information on previous reporting within a specified degree of certainty and/or accuracy
Cross-cue	Pre-planned collaborative detection, recognition, identification, location or tracking; the deliberate handover of a collection/find task to a nominated unit, system or person.
Detect	Discover the presence or absence of a unit, object, activity, situation, event or persons of significance.
Expose	Make (something) visible by uncovering it.

Task/action	Description
Identify	Determine the status (including friendly or hostile nature) of the detected unit, object, activity, situation, event or persons.
Intercept	Search for and listen to and/or record communications and/or electronic data.
Locate	To determine the geographical position of a specified entity or object.
Monitor	Develop or maintain situational awareness, pattern of life or atmospherics of a geographical area, activity or situation.
Recognise	Classify the capability of the unit, persons, object, event, situation or activity of potential military significance.
Search	Locate specific targets using intelligence assessments, systematic procedures and appropriate detection techniques.
Track	Maintain identification and location of a unit, activity, situation or persons.
Warn	Pre-planned provision of information to provide warning of a specified situation, event or activity.

Table 3.1 – Common intelligence, surveillance and reconnaissance tasks and actions[9]

3.10. **Target.** This refers to the objects, events or engagement space to be observed. Planning requires consideration of the likely observable signatures to enable optimal sensor to target matching. For example, an adversary tank can be observed visually, has a heat signature that can be detected by infrared sensors and may have associated radios that can be detected by signals intelligence sensors. When moving it can be observed by moving target indication radar. When static it can be imaged by synthetic aperture radar. As the target is likely to try and hide from detection through camouflage,

9 The descriptions reflect commonly understood meanings for ISR tasking but are not formal definitions.

concealment, deception and emission control measures, a range of sensing types should be employed to enable the best chance of detection.

3.11. **Threat.** This refers to the risks and issues from collecting against the target, other adversarial threats, political and environmental factors. Collection occurs within a risk envelope set by the commander. The threat influences what collection can be undertaken. For example, in a high threat environment it will be preferable to use long range systems which can collect whilst beyond the range of the threat. Alternatively, the use of some collection capabilities might incur risks such as escalation or counter-detection.

3.12. **Tactics.** The task, target and threat for a given collection activity will determine the best tactics to be used to achieve mission success, and collection operations will be tailored to the specific needs of a given mission. Detailed below are the general principles used.

a. **Massing.** ISR is most effective when massed, particularly against low-resolution targets. Massing encompasses both time and space by operating ISR in the same engagement space at decisive moments and key decision points. Massing requires focus and prioritising; commanders should avoid sharing ISR equitably across multiple commands and lines of effort. Massing increases the likelihood of detection through saturation, creates redundancy and is more resilient to both adversary counter-ISR efforts and camouflage, concealment, deception and emission control measures. Massing must be carefully balanced against the requirement for persistence.

b. **Layering.** Layering is the application of multiple different sensing types across all operational domains. No sensor guarantees successful collection, particularly when an adversary or target is taking deliberate steps to avoid detection, observation, classification and identification. Layering of collection greatly increases the chances of successful collection. An example of layering would be the detection of possible adversary radio activity in an area. Long range imaging can be used to identify if the area is occupied. Wide area airborne ground moving target indication can be used to track movement from the area and finally cue a full motion video carrying platform to positively identify what is moving.

c. **Sequencing.** Sequencing is the engineering of ISR assets or capability force flows for best collection effect. For instance, this might be ensuring several assets of the same type or capability arrive over a target with overlap to conduct a handover of the target and maintain a constant presence for a protracted period. Alternatively, it might be ensuring that numerous complementary capabilities are massed in time and space at a decisive point for an operation such as a strike.

d. **Tipping.** Tipping is the broadcast from an ISR capability to all relevant ISR capabilities to inform them of a target detection. A tip is not time bound or a directive and there is no expectation by the tipper that another capability will act on it. Tipping requires planning to ensure all interested parties can broadcast and receive tips. Setting tipping criteria ensures all salient detections are passed while minimising superfluous traffic that risks overwhelming the communication system.

e. **Cueing.** Cueing uses one sensor to guide the collection of another. Unlike tipping, cueing or cross-cueing is usually time bound and directive as the result of an agreed 'contract' established in mission planning.

f. **Contracts.** Contracts are mission-specific requirements for sensor, platform and capability interactions that exist outside normal standard operating procedures and tactics, techniques and procedures. They are based on specific mission outcomes, such as the warning of threats or requirement to detect fleeting targets quickly. An example contract might be a ground moving target indication platform notifying a protected target of anything approaching within 5 kilometres and then for a full motion video platform to investigate the movement.

3.13. **Headquarters support to ISR collection.** ISR collection activity requires significant support from a headquarters. Logistics are critical to deploying and sustaining collection, particularly for limited endurance platforms. Similarly, the wider operations community will be engaged to ensure the force protection of valuable capabilities. This might range from close escort to deliberate operations to remove or mitigate threats. In some circumstances successful collection may require deliberate activity and manoeuvre by other forces, for instance, by presenting a target to initiate an enemy reaction that can then be observed. Contracts, tipping and cueing therefore extends beyond ISR capabilities and contracts may exist between ISR capabilities and other force elements.

Key points

- The two general means of collecting information are by human or technical sensor.
- Collection uses sensing of all types to detect objects and events in time, space and on the electromagnetic spectrum, and operates across all operational domains.
- Dedicated ISR collection may also be supplemented through non-traditional and non-dedicated collection means.
- Collection must be integrated into the wider operational plan and may require supporting non-ISR assets to support it.

Chapter 4

Chapter 4 describes processing, exploitation and dissemination and how these processes may be undertaken.

> We're going to find ourselves in the not too distant future swimming in sensors and drowning in data.

Lieutenant General David A. Deptula, United States Air Force Deputy Chief of Staff for intelligence, surveillance and reconnaissance, 2009

Chapter 4

Processing, exploitation and dissemination

Section 1 – Core elements

4.1. The utility of collection is dependent upon the subsequent processing, exploitation and dissemination (PED) of the data and information from sensors. PED interprets the data and ensures it gets to the right place, at the right time and in the right format so that the required decision or action can be taken. PED should be regarded as one function, not three separate functions. PED can be applied individually, sequentially or concurrently and under various models, dependent on requirements. It should not be regarded as a rigid, linear process. PED is a vital and distinct function and is not subordinate to collection in terms of importance.

4.2. **Processing.** Processing can be described as the translation of sensor-derived data, by machine or human, into a format where it is exploitable or useable by subsequent processes or capabilities. Processing occurs repeatedly, in multiple different guises and can take place sequentially or concurrently. It can be human or automated, and can occur between machines, between humans or between humans and machines.

4.3. **Processing outputs.** Processing generates three outputs. These are raw data, processed data and information.

a. **Raw data** is data which may have been subject to some form of initial machine or human processing, but which cannot be further consumed by other machines or humans without additional processing.

b. **Processed data** is data that has been processed so that it can be consumed, although this may still require specialised training and systems.

c. **Information** is data that has been sufficiently processed to be easily intelligible without further processing. Confidence in the observation has been attributed and contextualisation, and insight and foresight may have been added. However, its value and accuracy cannot be judged in isolation.

4.4. **Exploitation.** Exploitation is the examination of data or information to derive and attribute value from and to it. As with processing, exploitation can be a machine or human activity and can occur sequentially or concurrently with processing. Exploitation has the two primary functions of entity extraction and contextual analysis, whilst it also supports the development of insight and foresight.

a. **Entity extraction.** This detects, recognises, classifies and identifies observations (objects and events), and attributes confidence to the observation. For instance, this may be factually describing what a sensor shows and attributing a confidence level on what has been seen.

b. **Contextual analysis.** This contextualises observations by applying skills, knowledge and experience to the observations to add further value through attribution of intent and identification of anomalies and patterns. For instance, an operator observes a tank moving south, they contextualise this by knowing that friendly forces are 1 kilometre south of the tank's position and recognise that the tank is therefore advancing on friendly forces, is within weapons range and is a threat.

c. **Insight and foresight.** Providing assessment of intent and prediction of future activity. For example, the adversary has held an exercise, an adversary formation likely deployed for the exercise and is now likely to return to its barracks.

4.5. **Exploitation outputs.** Exploitation generates three main outputs. These are described below.

a. **Processed data.** Data that has gone through additional processing so it can be consumed, although this may still require specialised training and systems.

b. **Information.** In common with processing outputs at paragraph 4.3c, information is also an exploitation output and still relates to data that has been sufficiently processed so that it is easily intelligible without further processing.

c. **Intelligence.** Information that has been further processed, contextualised and where there is a high degree of confidence in the known level of accuracy of the information. Exploitation, insight and foresight indicates that the information is of importance to one or more users.

4.6. **Dissemination.** Dissemination is making raw data or processed data, information and intelligence resulting from processing and/or exploitation available for others to use. As with processing and exploitation, dissemination occurs throughout PED. It takes place sequentially and/or concurrently, is performed by both humans and machines, and occurs between humans, between machines and between humans and machines. Dissemination may be in near real time or sequentially following more rigorous processing and exploitation.

4.7. **Dissemination media.** Dissemination can be achieved by one of the following three methods, dependent on requirements. These are manual, digital and automated dissemination.

a. **Manual.** Verbal or written communication between humans.

b. **Digital.** Using computer systems and networks such as data links, chat services, email, databases and radio. These systems still require human input.

c. **Automated.** The use of computer systems and networks to transmit, publish and alert without human interaction.

4.8. **Dissemination models.** Dissemination media describes how data, information and intelligence is shared. Dissemination models describe how a user can access it. Dissemination models are described below, although they are often blended depending on operational requirements.

a. **Targeted.** Data, information and intelligence will be sent only to specific users. This will likely be specified in orders, as the result of a contract established in planning or due to an established relationship between the originator and receiver.

b. **Broadcast.** Data, information and intelligence will be sent to all potential users irrespective of likely benefit or interest. The user group might be defined by the network or communications system the originator operates on, interest group, or command and control structure.

c. **Push.** The originator sends the data, information and intelligence to the user.

d. **Pull.** The originator hosts the data, information and intelligence. It is the responsibility of the user to monitor the area where outputs are hosted. Pull dissemination best operates when aligned to a push alert system.

e. **Subscription.** The user subscribes to a feed, service or repository hosted by the originator. All content is either pushed to them or alerts are pushed allowing them to pull the outputs.

f. **Smart.** Smart dissemination uses modern data methods and analytics to dynamically match users to data, information and intelligence based on their needs. Computer systems monitor what users use and interact with to suggest outputs which they might wish to pull, alert or actively push this content to them.

4.9. **Dissemination best practice.** Wherever possible dissemination should aim to meet the following criteria.

a. **Data-centric.** Data should be formatted as common data objects, to agreed standards, to maximise the utility of processed and exploited data and information and resultant intelligence. The use of static end-product reporting such as written documents, images, diagrams and storyboards should be limited unless there is a specific requirement to use these outputs for mission success.

b. **Value agnostic.** All data, from all sources, from both mission and incidental collection must be treated as of equal potential value and be handled and treated in the same manner. A rigorous triage process must be put in place where limitations such as bandwidth preclude this.

c. **Discoverable.** All outputs should be discoverable by everyone with the necessary security clearances. Dissemination should not assume interest or lack of interest by a given consumer.

d. **Reflect ground truth.** Disseminated data, information and intelligence must reflect the reality and truth of what was observed. Contextualisation, analysis and assessment must not obfuscate the actual objects and events as they were observed.

e. **Traceable.** Disseminated data, information and intelligence must be traceable back to source, even where there is a requirement to obfuscate the source.

Section 2 – Processing, exploitation and dissemination structures

4.10. **PED nodes.** A PED node is a physical or virtual location where PED is conducted. Given the potential concurrency and ubiquity of processing, exploitation and dissemination throughout a PED workflow it is likely that multiple PED nodes will be formed into a network to achieve the desired outputs. There are three primary types of PED node.

a. **Edge.** The PED, or elements of it, is conducted within the sensor or platform. Edge PED is normally an automated function and its capabilities depend on the computational power, PED algorithms, bandwidth and dissemination means available.

b. **On-board.** PED, or elements of it, are conducted on the sensing platform, using either on-board machines or the platform might host dedicated PED personnel. On-board PED often benefits from being near real time as the crew has immediate access to data at point of collection. On-board PED is often limited by the means of disseminating from the platform.

c. **Off-board.** PED is conducted off the platform. Off-board PED might be directly connected to the sensor or platform by data link, such as an uncrewed air vehicle ground control station. Alternatively, an air gap might exist, for example, a platform may capture data before returning to a base location where it can be exported into a PED system. Off-board PED is normally conducted within the operational theatre; it is desirable for it to be in the closest proximity possible to the collector to reduce latency. Off-board PED can be in near real time or post collection depending on the architecture available.

4.11. **Reachback or reach forward and virtual crews.** There are two further node approaches where PED is conducted at distance from the collection. These approaches use variations of reachback or reach forward constructs or could use a disaggregated approach.

a. **Reachback or reach forward PED.** PED is conducted outside the operational theatre with the collector able to send outputs back to the PED provider, or the PED provider able to reach forward to pull the data. Reachback PED can be conducted in near real time with streaming data links, or post mission with a degree of delay as raw or processed data is transmitted and received.

b. **Virtual crews.** PED is conducted by analysts located at disaggregated nodes using a common network. This could incorporate a blend of on-board, off-board and reachback analysts.

4.12. **Specialised PED applications.** Some PED capabilities provide unique insight separate from the means of collection. They generate specific data, information and intelligence based on the raw material collected and provide unique outputs that do not fit within the traditional collection disciplines. An example is materiel and personnel exploitation, which is not reliant on a specific, technical mechanism of collection, although this may occur, for instance, the recovery of improvised explosive devices by explosive ordnance disposal personnel. Materiel and personnel exploitation can be viewed as a PED application that includes tactical questioning, document, electronic device and financial exploitation, together with a range of tactical measurement and signature intelligence activities, undertaken by scientific, technical and specialist intelligence personnel.

4.13. **Traditional PED models.** PED can be conducted in several ways. The different models are suited to particular tasks and outcomes as outlined below.

a. **Direct support.** PED is directly attributed to a collection platform or sensor based on the likely missions, tasks and outputs required of that platform or sensor. PED is supporting and the platform or sensor is supported. The PED units' size, skills and capabilities are determined by the requirements of the platform or sensor. Examples would be analysts on-board an aircraft, ship or land platform. Direct platform support benefits from an intimate relationship and knowledge of the platform and sensors, which breeds deep expertise and understanding of the system, data and capability. However, PED capacity may be

underused if the collector is inactive. This can lead to PED inefficiency if large volumes of specialist personnel are required for each platform or sensor. This approach also creates duplication, which leads to further inefficiency and PED being conducted within platform channels which hinders an enterprise approach to intelligence, surveillance and reconnaissance (ISR).

b. **Platform-agnostic PED.** Platform-agnostic PED is a progression from direct platform support. Under this model a PED capability can support several platforms or sensors of the same collection type or discipline. Rather than being aligned to the platform's unit, the PED element will typically form a separate unit and will be dynamically assigned against the collector for a specified time period. Platform-agnostic PED is far more economical than direct support as PED can be burden-shared, with analysts allocated at the point of need. As one PED unit can support multiple sensors they can still be fully used if some platforms are not collecting. However, platform-agnostic PED requires more sophisticated command and control and is reliant on adopting common standards for data, training and outputs. Platform-agnostic PED also requires robust and resilient network architecture, unless time-consuming manual dissemination methods are used between the various platforms and sensors and the PED capability.

c. **Federated PED.** Federated PED is a further progression on platform-agnostic PED with multiple PED units supporting multiple collection capabilities. PED units form a network with collection being linked to the most suitable PED capability to meet the requirement. Federated PED can be scaled across one operational domain, across multiple domains and across allies and partners. Federated PED increases the advantages of platform-agnostic PED in terms of economy, flexibility and commonality but is more complex given the technical requirements to enable it and the command and control necessary for efficient operation.

d. **Problem-centric PED.** PED has previously been viewed as a supporting function, aligned to collection as the supported function. Intelligence, operational and targeting problem sets are fragmented across multiple operational domains, units, disciplines and sensors through the collection management process. Problem-centric PED deviates from other PED models by task organising multiple staff

functions against a specific problem. This includes information requirements management and collection management functionality, mission management and command and control, analytical and exploitation capabilities and data management. This creates multidisciplinary teams with the ability to task, process, exploit and disseminate to and from any sensor, or mix of sensors that are required to meet the mission objectives. Collection is therefore task organised to the problem-centric PED capability with the PED becoming the supported activity and the collection the supporting. There are several ways of conducting problem-centric ISR, however, the *Defence ISR Strategy* introduces problem-centric ISR aligned with activity-based intelligence as Defence's preferred future means of conducting problem-centric ISR; this is described in detail in Chapter 5.

4.14. **PED timelines.** PED timelines have previously been divided into levels, or phases, but this approach has been replaced by the single aim of delivering data, information and intelligence within the time that achieves the mission. This could range from seconds to months. Some missions, such as force protection overwatch, target acquisition and threat warning, may require near real time reporting of individual observations in the form of processed data or information. Where the task is in support of intelligence functions, more rigorous longer-term observations made over hours, weeks or months may be more applicable.

4.15. **Traditional PED, correlation and fusion.** Direct support, platform-agnostic and federated PED models are also platform, sensor and discipline-centric models. This means that analysts are aligned to the sensing type of the platforms, sensors or PED network, for instance, to focus on imagery, communications or electromagnetic intelligence. It is likely on a given operation that all the above models will be used concurrently by different capabilities and across different sensing disciplines. This creates a high degree of fragmentation both within specific disciplines and between different disciplines. This creates significant challenges for command and control, operational employment and deriving the best possible outcomes from the capabilities available. Correlation and fusion are therefore critical to ISR. No sensing type provides a single solution and individual observations from sensors constitute data pieces which only reveal their true value when collated, correlated and analysed together.

4.16. **Correlation.** Correlation is the use of multiple different collectors to increase the confidence in detection from individual sensors and is largely

used as a multi-source entity extraction technique. It is normally conducted at the tactical edge and in compressed time frames. The exact criteria for correlation will be mission specific and linked to the rules of engagement. During mission execution, correlation will normally be vested as an authority to a headquarters or command and control node controlling all ISR, and with access to all observations, from all sensors. The authority can escalate and de-escalate the level of confidence based on the totality of collect occurring.

4.17. **Fusion.** Fusion moves beyond correlation and seeks to use multiple sources to add context, insight and foresight to detections. This has traditionally been enabled through the sensing disciplines, their associated discipline-aligned PED teams and the production of single source or single discipline end-product reporting. This methodology then requires disciplinary specialists to translate sensor-derived data into a format where it can be consumed by all-source analysts in the intelligence cycle. The linear, fusion approach to developing intelligence is shown at Figure 4.1.

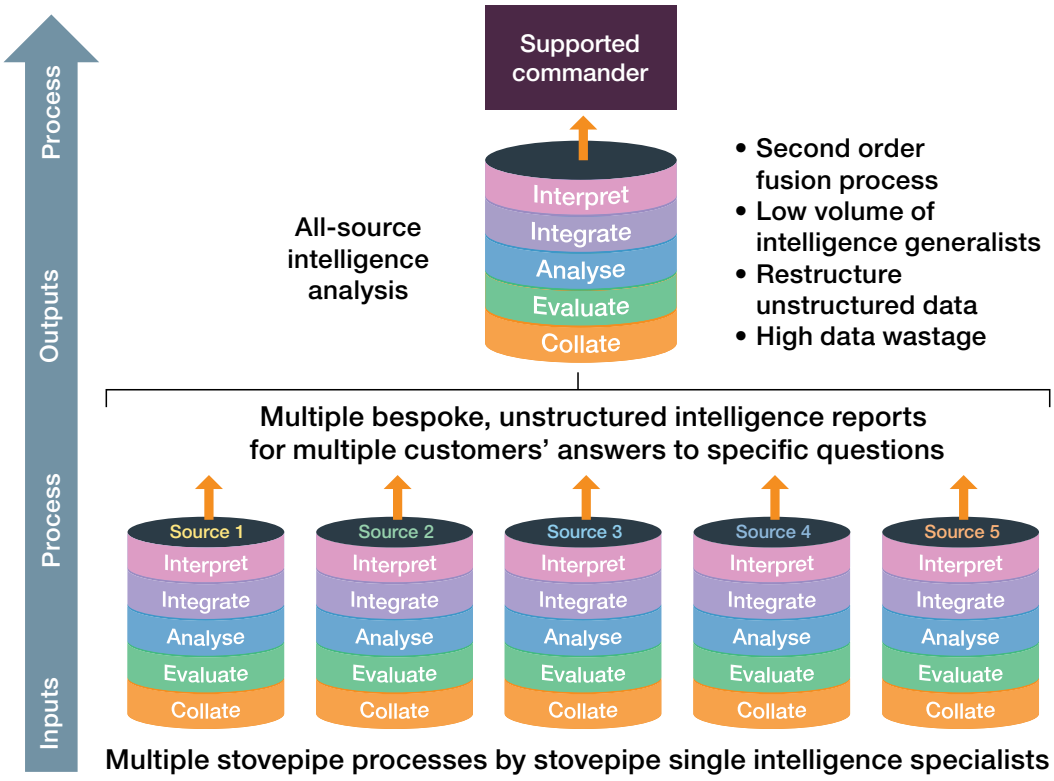


Figure 4.1 – Linear intelligence development and fusion

4.18. **The ISR limitations of the intelligence fusion model.** The intelligence fusion approach is suited to small-scale tactical activity with tightly bounded tasks, limited collection capability and PED, but it becomes limiting as size, resourcing and complexity grows. Conversely, intelligence fusion remains highly suitable for strategic assessment given that there is no linear relationship between ISR observations and assessments at that level. At the operational and higher tactical levels, the intelligence fusion model can experience several limitations. These challenges can vary according to the complexity and the scale of an operation. The main challenges are outlined below.

a. There is limited capability within sensor, platform and discipline stovepipes to exploit collection against fleeting, complex and signature-suppressed targets. It is unlikely that any single sensor or discipline will generate enough information of sufficient fidelity to meet mission or task requirements.

b. The model is linear, transactional and orientated on known gaps and targets of interest or 'known unknowns'. It is not optimised to address 'unknown unknowns' where specific questions have not been asked.

c. It is built upon tight control of produced data and information, which renders much of what is collected opaque or invisible to commanders and intelligence staffs. Data, information and intelligence remains within discipline channels unless it crosses the threshold for reporting in the form of end-product reporting. Most data, particularly incidental collection, is deleted or unused as it is either not related to a formal requirement and/or is exploited in isolation. Links between data which generate compound value are never achieved as the data remains within system, sensor, discipline and organisational specific architectures.

d. The focus around sensors and discipline channels across all operational domains and levels of command means that staff are often unaware of what is being collected while collectors are unaware of requirements.

e. The growth in sensor diversity and complexity, and the continued use of static end-product reporting, overburdens staff due to the volume and multiple formats of reporting available.

4.19. **Mitigating intelligence fusion issues.** A significant reason for fusion model limitations is the way in which PED and intelligence analysis have historically been divided. This division existed due to the functional requirement for sensor data to be processed and exploited by disciplinary experts and translated into a format where it is easily digestible by all-source analysts. However, PED and the processing phase of the intelligence cycle can be far more closely aligned and modern technology enables alternative approaches to the traditional linear and procedural ISR PED process. It is now possible for an analyst at any level to receive data of all types, derived from all sensing types and at machine speed. The combination of new operational challenges and new technologies has generated new models, techniques and organisational constructs. These combine in a modular fashion to create a new PED model orientated around data fusion, rather than intelligence fusion.

Key points

- A PED node is a physical or virtual location where PED is conducted; this may be edge, on-board or off-board.
- Traditional PED models include direct support, platform-agnostic PED and federated PED.
- Problem-centric PED task organises multiple staff functions against a specific problem. This creates multi-disciplinary teams with the ability to task, process, exploit and disseminate to and from any sensor, or mix of sensors that are required to meet the mission objectives.
- PED timelines have previously been divided into levels, or phases, but this approach has been replaced by the single aim of delivering data, information and intelligence within the time that achieves the mission.


mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True
#selection at the end -add back the deselected mirror modifi
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active
#mirror_ob.select = 0

Chapter 5

Chapter 5 introduces the application of problem-centric intelligence, surveillance and reconnaissance (ISR) using activity-based intelligence. The *Defence ISR Strategy* has identified activity-based intelligence as Defence's preferred future means of undertaking problem-centric ISR. This chapter also outlines the potential application of automation, artificial intelligence and machine learning.

> “In the last 10 years, numerous reports have highlighted obstacles to the integration of intelligence, surveillance, and reconnaissance into military campaigns and major operations. The root cause of many of these difficulties is adherence to a centralized Cold War collection management doctrine focused on production rather than goals and objectives.”

Jason M. Brown,
‘Strategy for Intelligence, Surveillance, and Reconnaissance’,
Joint Force Quarterly, Issue 72, 2014

5

Chapter 5

Problem-centric approaches, activity-based intelligence and automation

Section 1 – Problem-centric intelligence, surveillance and reconnaissance and activity-based intelligence

5.1. The traditional linear intelligence, surveillance and reconnaissance (ISR) process creates a clear division between the intelligence and ISR functions. Additionally, the ISR process has typically been aligned with the collection phase of the intelligence cycle, with the results of ISR collection incorporated within the processing stage of the intelligence cycle, whilst also supporting the decision cycle.[10]

5.2. The traditional ISR approach breaks large, complex operational and intelligence problem sets into much smaller ISR problems through the intelligence requirements management and collection management process and attributes these tasks across multiple ISR capabilities. These ISR tasks are carried out in isolation, with the intent that the output from each can be reaggregated by the intelligence staff to meet the commander's requirements. The linear approach to ISR is shown at Figure 5.1.

10 As shown in Chapter 1, Figure 1.2.

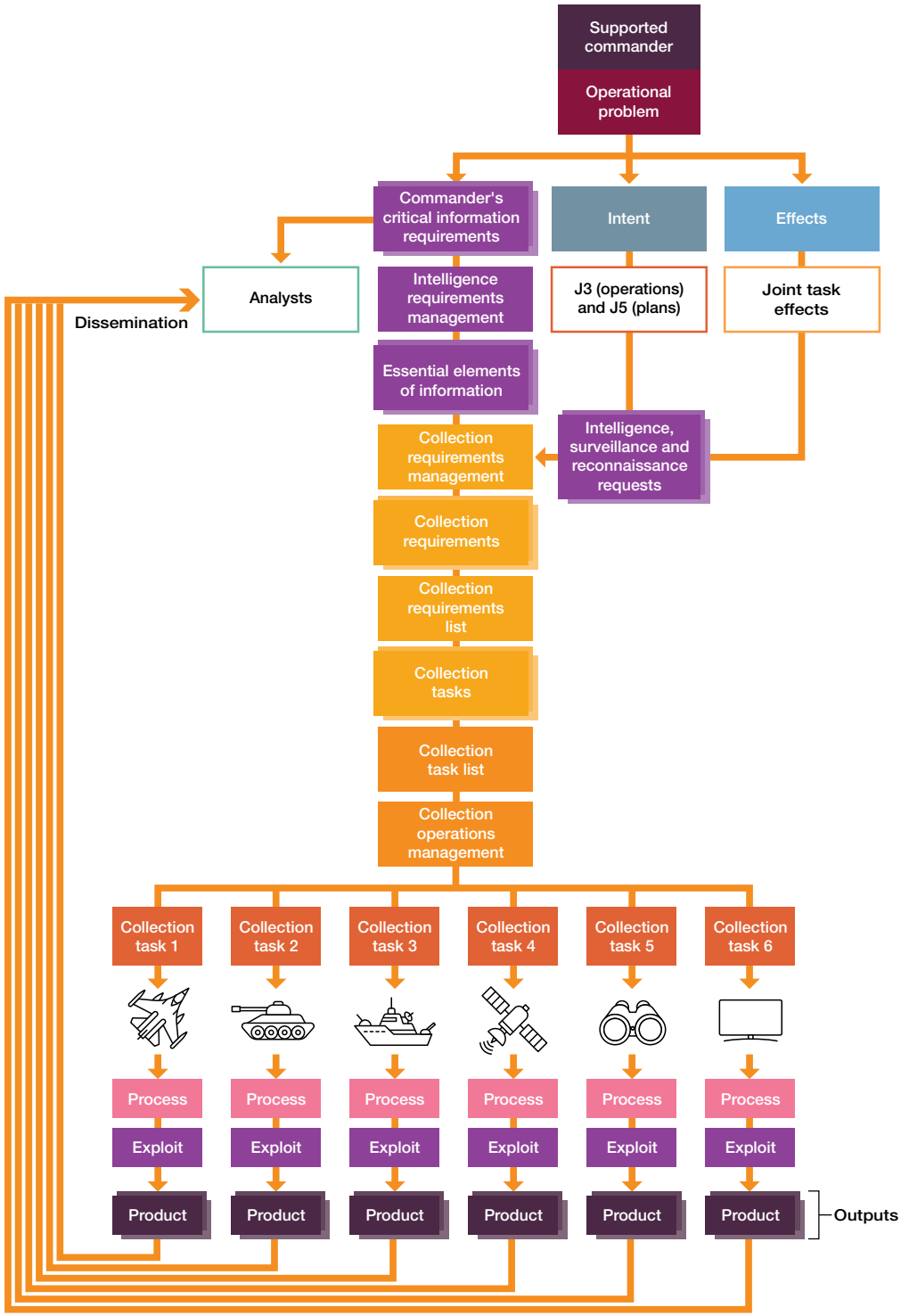
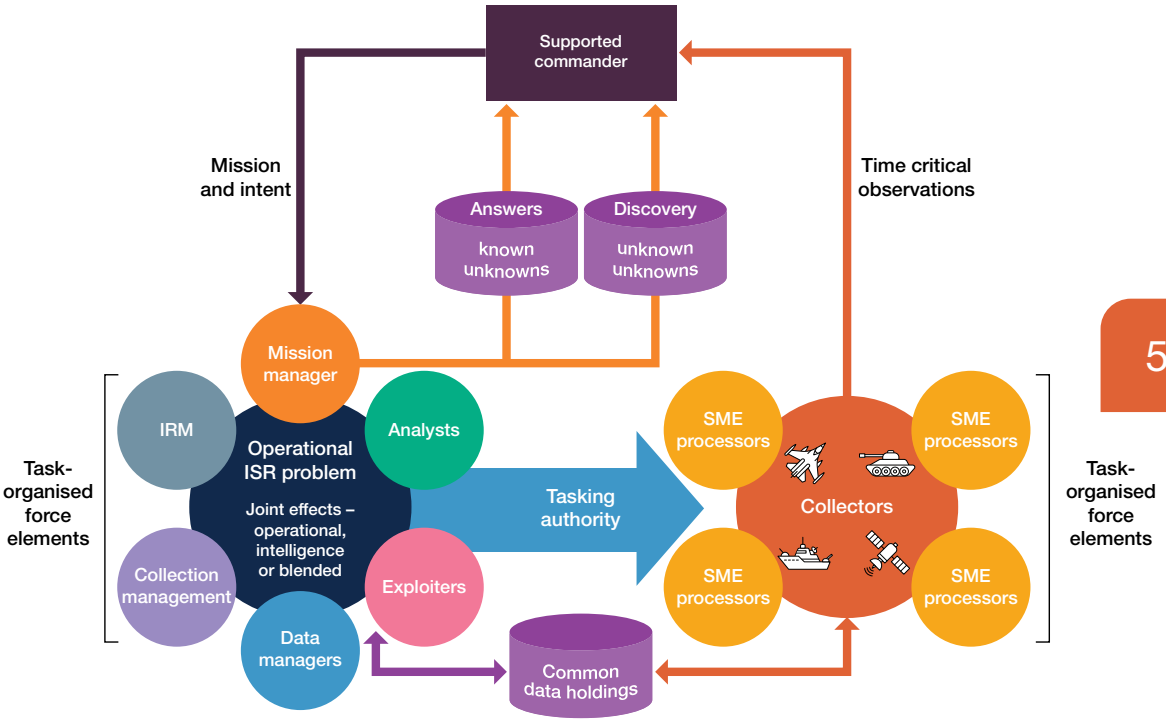


Figure 5.1 – Traditional linear intelligence, surveillance and reconnaissance process

5.3. **Problem-centric ISR.** Problem-centric ISR changes linear intelligence processes and the practice of undertaking processing, exploitation and dissemination (PED) within disciplinary channels by adopting greater mission command within the ISR enterprise. It addresses the current procedural breaks in information flows between all-source analysis and single-source PED through dynamic task organisation that combines analysis, PED and collection against specific operational problems. Most importantly, it draws a direct link between mission and intent rather than creating numerous and disparate tasks which are often disconnected to the original requirement. Rather than fragmenting responsibility for small elements of complex problems across numerous analytical, PED and collection capabilities, problem-centric ISR task organises resources around the operational outcome required. A problem-centric ISR approach is illustrated at Figure 5.2.



IRM	intelligence requirements management
ISR	intelligence, surveillance and reconnaissance
SME	subject matter expert

Figure 5.2 – Problem-centric intelligence, surveillance and reconnaissance

5.4. **Activity-based intelligence.** The *Defence ISR Strategy* has identified activity-based intelligence (ABI) as a key enabler for conducting a problem-centric approach to ISR. ABI is an analytical methodology which provides significant benefits when used alongside a problem-centric approach. ABI can be described as 'an analysis methodology which rapidly integrates data from multiple INTs [intelligence disciplines] and sources around the interactions of people, events and activities, in order to discover relevant patterns, determine and identify change, and characterise those patterns to drive collection and create decision advantage'.[11]

5.5. **Activity-based intelligence characteristics.** ABI is characterised by ceasing to operate ISR and intelligence processes within disciplinary channels and instead providing all processed data to analysts so it can be exploited as a whole. All sensing types, capabilities, disciplines and platforms process their data so that it can be integrated, analysed, interpreted and evaluated as one coherent body of data and information, including all non-dedicated ISR, non-traditional ISR and friendly or allied force data. This effectively ends the separation between intelligence analysis and PED. PED no longer deals solely with single sensors, platforms and disciplines and intelligence analysts no longer solely analyse end-product reporting originating from PED. All data, information and intelligence becomes available and exploitable by everyone. An analyst might simultaneously have available to them streaming full motion video, social media feeds and historic intelligence of all classifications. A representation of a problem-centric approach visualising the early integration of platform data using ABI is at Figure 5.3.

11 Chandler P Atwood, 'Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis', *Joint Force Quarterly*, Issue 77, 2015, page 26.

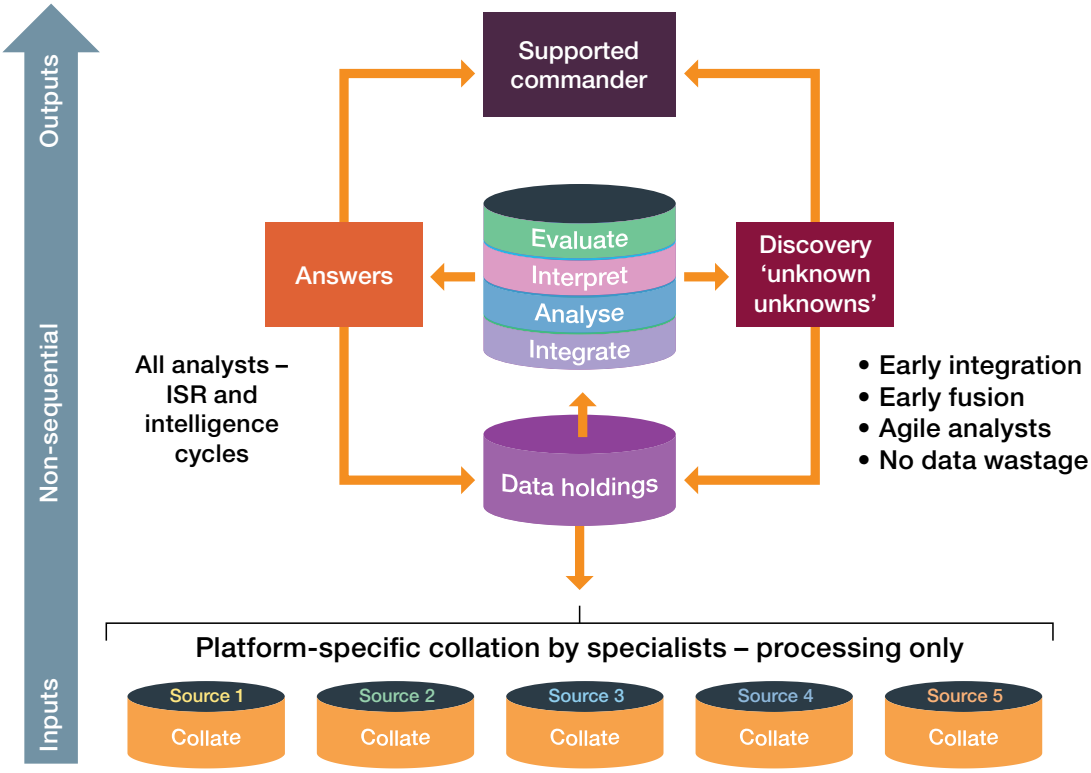


Figure 5.3 – Activity-based intelligence process

5.6. **Activity-based intelligence principles.** ABI has four key principles: geo-reference to discover; integration before exploitation; data (sensor) neutrality; and sequence neutrality.

a. **Geo-reference to discover.** All data sources should be spatially and temporally indexed at the time of, or as close as possible to, the point of collection. This allows data to be easily discoverable.

b. **Integration before exploitation.** All data, from all sources, is integrated prior to attempting to exploit it.

c. **Data (sensor) neutrality.** All data, from all sources, is equally valid and potentially equally valuable. This includes data that cannot be spatially and/or temporally referenced or has a large probability of error. Mission and incidental collection are equally important.

d. **Sequence neutrality.** The inherent value of data cannot be judged at the point of collection and therefore the latency of data becomes less

important. The value of historically collected data might only become apparent on receipt of new data. Similarly, newly received data might require contextualisation from historic data. Alternatively, data and information might be collected before the relevant intelligence question has even been asked.

5.7. **Activity-based intelligence in practice.** ISR planners must determine whether a traditional approach or problem-centric approach using ABI is most suitable for their operations. Relevant considerations are detailed within Table 5.1.[12]

Attribute	Traditional intelligence	Activity-based intelligence
Adversary	Predictable, doctrine based	Unpredictable, motivation based
Signature	Durable, physical, definite	Non-durable, proxies
Smallest unit	Class of equipment/object	Individual entity with unique identifier
Analytical reasoning	Inductive, linear	Deductive, non-linear
Data focus	Single-intelligence; compartmented	Cross-domain multi-intelligence
Analysis model	Phased, linear, segregated, pattern-analysis, exploit	Sequence-neutral, forensic, pattern-of-life, discovery
Target model	Facilities and target, coordinate, targeted	Area of interest, population, region, incidental collection
Motivation	Collection-driven	Analysis-driven
Reporting	Finished serial reporting	In-work products, layers, files
Collection frequency	Scheduled, desk-based	Persistent and pervasive, multi-intelligence

Table 5.1 – Attributes of traditional and activity-based intelligence

12 Table produced from Patrick Biltgen and Stephen Ryan, *Activity-Based Intelligence: Principles and Applications*, 2015, page 17.

5.8. **Activity-based intelligence and specialisation.** ABI methodology does not negate the requirement for deep single sensor or discipline PED and analysis experts. This is because complex technical data still requires translation and assurance for consumption by teams using the ABI methodology.

5.9. **Supporting concepts.** As ABI is a data-centric approach to PED, new approaches are required for capturing data, information and intelligence. Traditionally, PED translates structured machine data in a format exploitable by humans. Once exploitation has occurred, outputs are compiled into end-product reporting in formats such as written intelligence reports, storyboards or annotated imagery. Such reporting is extremely difficult to integrate and therefore a barrier to ABI. Equally problematic is that sensor-derived data is likely to be in many different formats meaning data is not easily comparable. ABI is therefore supported by two further concepts: structured observation management (SOM) and object-based production (OBP).

5.10. **Structured observation management.** SOM is a methodology for describing observations of objects, events, insights and assessments. It provides a common taxonomy to describe detections of all types so that they can be processed and exploited using ABI. SOM can be used to describe any type of observation, including radio frequency emissions, events reported in publicly available information, or information passed by a covert human intelligence source. To describe all possible observations, SOM formats are therefore complex and take significant periods of time to establish, however, they avoid taxonomical problems which hinder shared understanding, for example, a particular type of vehicle could be described as either a truck, lorry or heavy goods vehicle.

5.11. **Object-based production.** OBP is the mechanism by which SOM observations are packaged and provided for analysis as individual data objects. OBP packages observations as entities (observed objects and events), links (near, on, uses, works with, to name a few) and assessments (analytical comment on entities and links). OBP allows for a far more coherent approach to interrogating observations to find geospatial, temporal and relational links between object and events. It also allows for analysts to dynamically add, remove and change assessments of these objects. As OBP is comprised of structured data it can be easily integrated across a wide range of situational awareness and intelligence analysis tools. OBP also reduces bandwidth requirements as the messaging formats used are far smaller than sending end-product reports or streaming raw sensor data.

5.12. **Blending processing, exploitation and dissemination models.** Problem-centric PED is an activity that complements task-based approaches rather than replacing them entirely, for instance, tasks such as providing overwatch of a convoy for force protection or provision of battle damage assessment will require the enduring single-source collection and PED focus. However, by adopting problem-centric PED more widely, ABI, SOM and OBP can become a baseline standard, and will enhance the ability to conduct mission types that have traditionally been single-source. For example, whilst following a high-value target might require near real time PED using full motion video, the availability of other sensor types and data means that PED support is enhanced. The analyst can interrogate routes, locations and entities that the high-value target interacts with to quickly build situational awareness and understand the target's pattern of life. If the high-value target enters a building, the analyst can find information about the building, for example, to indicate if it is a weapons cache, or physical information about the building and its surroundings that might be required to create effects.

5.13. **Combining problem-centric techniques and methodologies.** The ways of working discussed above form a group of mutually reinforcing techniques and methodologies which deliver their full potential when combined. The key attributes of each technique are illustrated at Figure 5.4.

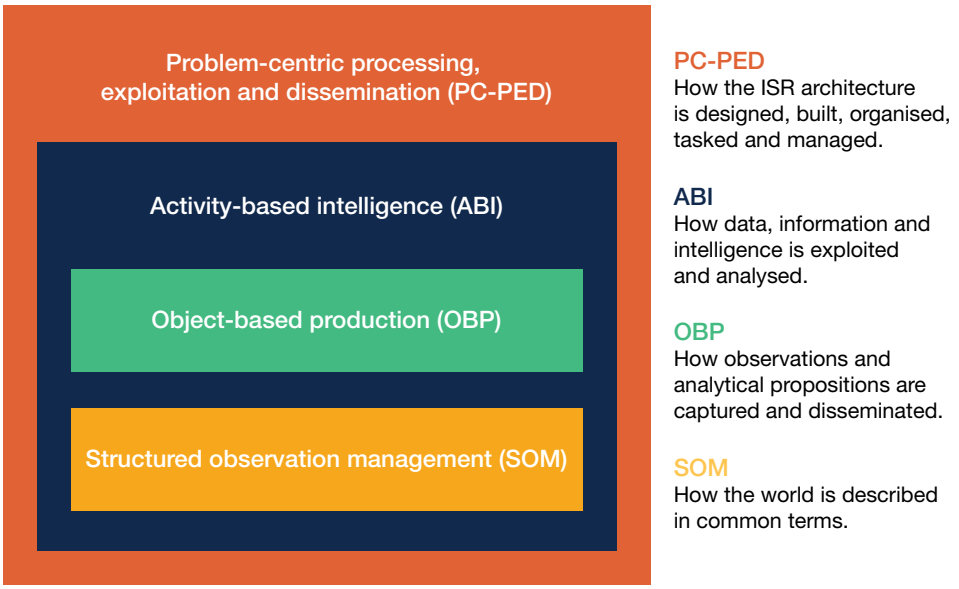


Figure 5.4 – Combining problem-centric processing, exploitation and dissemination and activity-based intelligence

5.14. **Technical versus procedural integration.** New ways of working often appear dependent on technology. While full technical integration is highly desirable, it is not essential and new ways of working can be enabled through changes in culture, organisational structure, policy and approaches. Where technological solutions cannot be implemented or where other barriers to technical integration exist, every effort should be made to enable similar functionality through procedural integration. For example, where signals intelligence and geospatial intelligence cannot be integrated on one system, respective systems and personnel can be collocated to create a multi-disciplinary team.

5.15. **Comparison of linear and activity-based intelligence processing, exploitation and dissemination.** The traditional linear model's approach to processing and exploitation, introduced in Chapter 4, and the problem-centric approach to PED and intelligence development and fusion is compared at Figure 5.5. The key difference in operation of the problem-centric model supported by ABI is the much earlier stage of data integration and fusion. In the ABI approach, all data is subject to initial platform-specific processing to turn it into useable information following collection and at the conclusion of initial processing is transferred directly to multi-source analysts with no further exploitation or assessment. In the problem-centric model, the early integration of all data from all sources for subsequent analysis therefore becomes possible, without data being discarded at the processing stage due to it not being relevant to the specific intelligence requirement that the collection was tasked against.

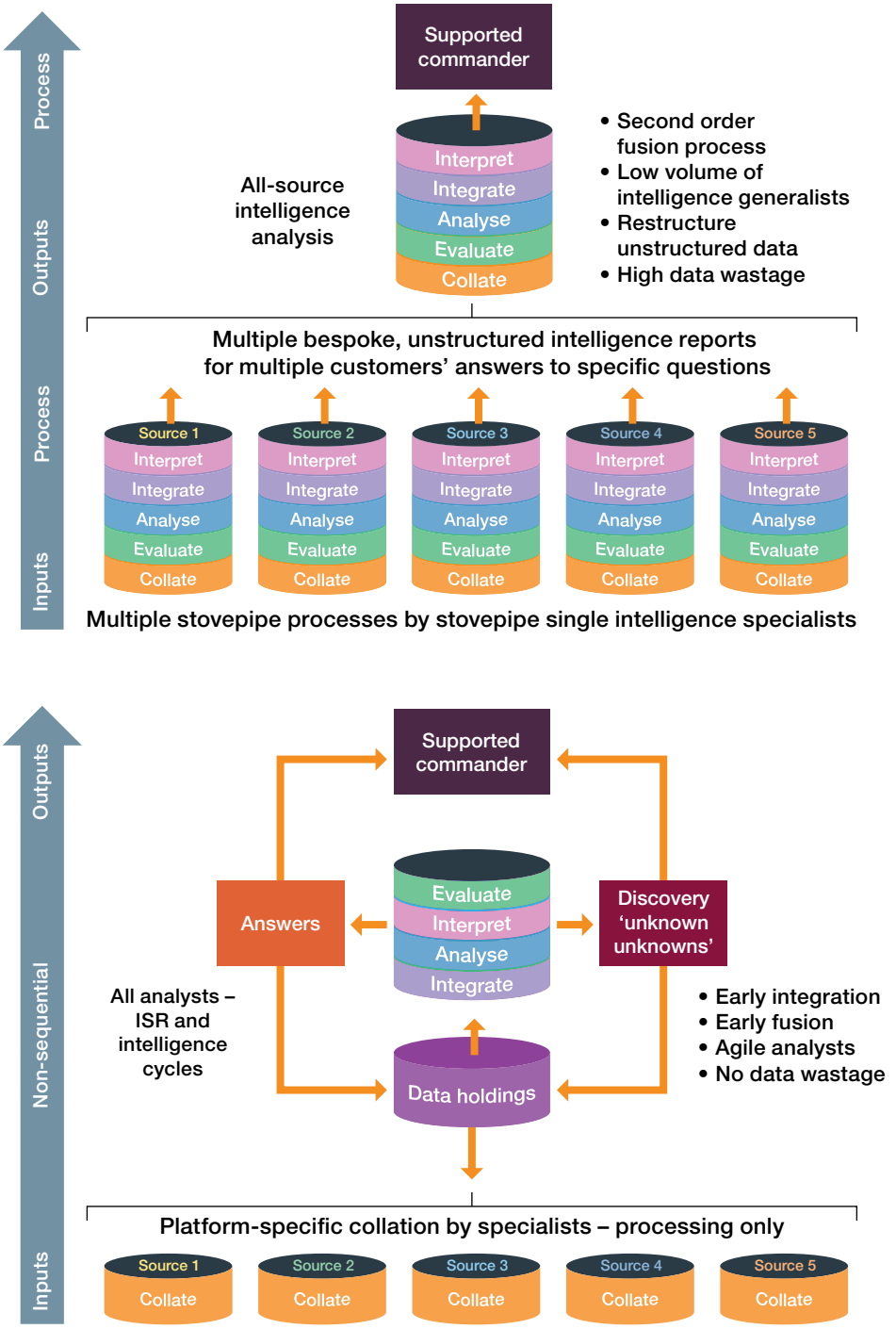


Figure 5.5 – Linear and activity-based intelligence model comparison

Section 2 – Automation, artificial intelligence and machine learning

5.16. **Processing, exploitation and dissemination, and automation.** A significant limitation of PED is the latency induced by the activity. Automation, artificial intelligence and machine learning technologies are increasingly playing a central role in PED. The growth in the volume of data available from both increasing sensor capability and diversity, and the availability and utility of publicly available information, supports the greater adoption of automation, artificial intelligence and machine learning due to finite human analytical capacity. Operating at machine speed can offer significant benefits to PED. Planners designing an ISR architecture should consider opportunities to incorporate automation, artificial intelligence and machine learning tools where appropriate as they determine the right mix of human-machine teaming, human or machine delivered processes.

a. **Speed and concurrency.** Machines optimised for a given PED task can be significantly faster that humans. Some data can only be processed, exploited and disseminated by a human sequentially. For instance, a linguist can only analyse one conversation at a time. Machines with language processing capability could process multiple conversations or detections concurrently. For all data, humans require a degree of linear process: raw data must be processed into a human readable form before it can be exploited. Exploitation, when required, must happen before dissemination. Machines could concurrently process, exploit and disseminate, or operate at speeds that make the latency in sequencing negligible.

b. **Scale.** Humans have a maximum cognitive load before their performance is degraded in speed and accuracy, insight or are unable to deliver the task. Humans struggle to comprehend and make sense of very large, diverse and dynamic data sets. The total amount of data continues to grow exponentially, which would require increasingly large analytical workforces. Machines can scale with data without degradation in performance.

c. **Accuracy.** Machines reduce some areas of human fallibility, especially during processing where data might be transferred between systems. For instance, a human may misinterpret what is being shown to them, write down or incorrectly communicate a grid reference.

5.17. **Future applications.** Artificial intelligence, machine learning and automation will have significant impact on all areas of PED. Although some higher-level functions can currently only be performed by humans, machine PED will play an increasingly important role in the future in the areas described below.

a. **Processing.** Machines will have particular applicability for data processing tasks that are time consuming, laborious and distract humans from using higher reasoning functions. Machine processing will enable faster, more accurate PED, greater concurrency in processing and greater standardisation in data.

b. **Entity extraction.** Machines will be able to detect, recognise, classify and identify objects and events in sensor data at greater speeds and at greater accuracy than humans. Machines will be able to undertake this at scale and extract from bigger data streams than human capacity allows.

c. **Contextualisation.** Machines will be able to identify anomalies and patterns in sensor data and across multiple data streams and alert a human user for higher cognitive investigations. For example, noting that traffic patterns are significantly different from baseline levels and that this might be associated with an explosion on a main supply route. Machines will have the ability to offer basic insight such as when a moving target will be in weapons range.

d. **Insight and foresight.** Machines will be able to undertake complex reasoning across huge data sets drawing links between disparate data and across multiple patterns and anomalies to provide foresight. For example, unusual foot, vehicle and electromagnetic activity could be detected across several locations and it determined that these patterns are normally associated with a terrorist attack within the next 48 hours.

e. **Dissemination.** Machines will automatically link requirements, data, information, intelligence, questions and answers dynamically.

f. **Command, control and tasking.** Machines will be able to decompose ISR problems, suggest solutions and task appropriate capabilities against them.

Key points

- Problem-centric PED is a methodology that directly task-organises all elements of ISR capability against operational problem sets, rather than distributing elements of the problem across disparate ISR capabilities and assets.
- ABI is an analytical methodology that can be used to enhance problem-centric PED. In turn, ABI is enhanced through a data-centric approach using SOM and OBP to change the way data is produced and disseminated
- Automation, artificial intelligence and machine learning will have a significant impact on ISR capability and capacity.

Chapter 6

Chapter 6 places the key roles of collection requirements management, collection management and collection operations management in the wider context of the components of intelligence, surveillance and reconnaissance (ISR) management at the operational level. It also describes representative ISR architectures and additional considerations in ISR support to the planning and conduct of operations at the operational level.

> The intelligence community are no longer looking for a needle in a haystack; the answer may not be a needle, and it may not be in a haystack.

Letitia A. Long, 'Activity Based Intelligence Understanding the Unknown', *The Intelligencer Journal of U.S. Intelligence Studies*, Volume 20, 2013

Chapter 6

Intelligence, surveillance and reconnaissance and operational planning

Section 1 – Components of intelligence, surveillance and reconnaissance management

6.1. All tactical and operational intelligence, surveillance and reconnaissance (ISR) activity operates within the framework of the Defence ISR Management Process. This comprises a number of focused boards and working groups that are designed to organise and describe Defence's priorities and plans for ISR operations in the near and longer term. The Defence ISR Management Process also ensures coherence and integration of ISR activities at the strategic and operational levels. For the joint commander and the intelligence staff charged with conducting ISR operations, the key processes are: allocations, collection requirements management (CRM), collection operations management (COM), ISR mission management and intelligence requirements management (IRM).

a. **Allocations.** Allocations is the function of appointing ISR capability to joint operations areas, commands and missions at the operational level. Ensuring the right quantity and mix of ISR capabilities is essential to ensure pervasive, persistent and appropriate ISR coverage. In general, having the right force package of joint ISR capabilities provides the operational commander with the ability to respond effectively to a range of operational settings and mission demands. Capability is allocated to the operational commander and components under a formal command and control state.

b. **Collection requirements management.** CRM is the focal point for all tasking requests from units and commands. CRM is responsible for prioritising requirements or tasking request and decides what is tasked.

c. **Collection operations management.** COM is responsible for the detailed planning and employment of ISR platforms that are needed to fulfil the tasks allocated through the collection management process. COM decides how a task is executed by balancing a range of factors including, dynamically changing priorities, availability of ISR capabilities and evolving situations within the engagement space.

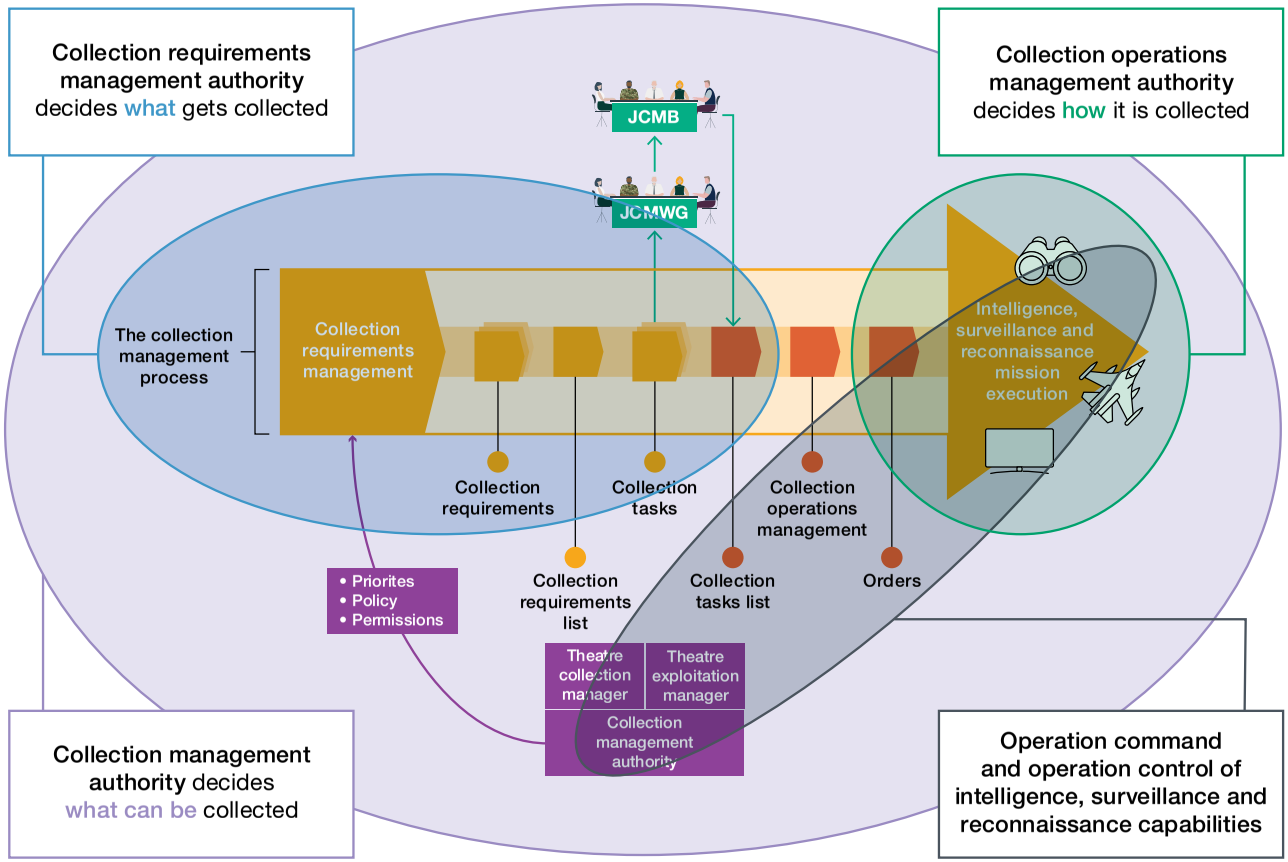
d. **ISR mission management.** The ISR mission management process executes the planning undertaken in COM.

e. **Intelligence requirements management.** The ISR management activities have a key dependency on the IRM process (within the overall intelligence cycle).

Section 2 – Intelligence, surveillance and reconnaissance authorities

6.2. Effective employment of the ISR management process relies on three ISR specific roles – collection management authority (CMA), CRM authority and COM authority – which confer certain authorities that are necessary to govern and cohere ISR activities. The main principle behind these ISR roles is centralised control and decentralised execution. These roles and the authorities vested in them complement the more recognisable command and control states assigned to units within a joint force construct. The authorities are explained below and illustrated at Figure 6.1.[13]

13 Figure developed from United States Central Command representation *ISR Management Process-U*, 27 July 2016.



JCMB joint collection management board
JCMWG joint collection management working group

Figure 6.1 – Intelligence, surveillance and reconnaissance management functions at the operational level

6.3. **Collection management authority.** The CMA is responsible for the overall authorisation, management and administration of ISR operations and activities. The CMA responsibilities are described below.

a. **Policies and permissions.** The CMA designates what can be collected by developing and implementing collection policies and permissions. This includes the framework of legal, political and military freedoms and constraints under which ISR capabilities operate. The governance of other ISR activities, such as reporting and release mechanisms, is the responsibility of the CMA.

b. **ISR burden management.** The CMA manages the level of demand placed on the ISR forces available. This includes prioritising tasking and the management of requests to higher headquarters for additional capability or capacity as necessary.

c. **ISR asset management.** The CMA apportions force elements to meet mission requirements. This includes both the apportionment of force elements assigned to the commander under operational command and operational control.

d. **Coordination.** The CMA coordinates all ISR capabilities. This includes ISR force elements kept under allied operational control.

6.4. **Collection management authority designation.** The CMA will be designated in a Chief of the Defence Staff Directive or may appear in another form of operational staff work, such as an operational order, campaign plan or force generation order in cases where a directive is not produced. For the UK, CMA is currently vested in the relevant single Service Chiefs, the joint commander or component headquarters. These authorities may delegate CMA as appropriate. Secretary of State for Defence endorsed changes are likely to result in Chief of Defence Intelligence (CDI), as the intelligence function owner, becoming the de facto CMA and ISR component commander for operations. However, in most cases, CDI would delegate the CMA role to a more appropriate level depending on the scale and complexity of ISR operations.

6.5. **Theatre collection and exploitation managers.** A CMA may decide to designate specific individuals for exercising their routine responsibilities for ISR, whilst retaining overall authority. The theatre collection manager (TCM) and theatre exploitation manager (TEM) fulfil this role for processing, exploitation and dissemination (PED) capabilities respectively. The TCM and TEM roles

advise the CMA on all relevant collection and PED considerations, ensure the execution of the CMA's direction, lead the collection management process and represent the CMA's interests in requirement planning, apportionment and allocations forums.

6.6. **Collection requirements management authority.** CRM authority is the focal point for all tasking requests from units and commands. The CRM is responsible for determining what is collected by prioritising and managing requirements in accordance with the commander's priorities, campaign plan or operational design.[14]

a. **Process.** The CRM resources requirements by matching capabilities to requirements in the most efficient manner possible and creates collection tasks, collection task lists and orders for execution. CRM is conducted at every level from strategic to tactical with each level responsible for matching tasks generated within their headquarters or directed from higher headquarters against available ISR capacity and capabilities. Where organic capability is not available, CRM staff request additional resources from the most appropriate source.

b. **Approaches to collection requirements management.** A joint task force commander typically appoints a TCM who is responsible for the CRM activities conducted within a joint operations area for a given operation. CRM can also be centrally managed by pooling capabilities and requirements management within a single, empowered headquarters. In most cases, the CRM process is implemented through a joint collection management working group and joint collection management board.

6.7. **Collection operations management authority.** The COM authority refers to the authority and responsibility to execute missions and tasks allocated by the CRM. The COM function decides how something is to be collected. It includes ISR asset management of capabilities, ISR mission planning and the execution of missions (ISR mission management). As such it is normally held by a component, formation or headquarters that holds formal command or control of ISR capabilities under a higher headquarters designated by the CMA.[15]

a. **Planning.** COM staff conduct detailed planning of how capabilities are used to achieve mission outcomes through the optimal employment

14 CRM is covered in Chapter 2, Section 2.
15 COM is covered in Chapter 2, Section 3.

of platforms, sensors and PED. COM integrates ISR operations into the operational or mission plan and can direct, schedule, prioritise and control collection operations and associated PED resources.

b. **Execution.** The COM is responsible for issuing orders to ISR force elements, maintaining the ISR common operating picture and decision-making for dynamic events that require the reallocation or reprioritisation of ISR capabilities. COM requires intimate knowledge of ISR capabilities assigned to the command and detailed understanding of optimising operational design and tactics for these capabilities. As such COM has typically been held within a headquarters that has a formal command and control state over the capability, for example, operational control. COM is also the functional authority for execution of the ISR plan, taking into consideration all the factors that may lead to dynamic changes such as changes to the available capabilities, environmental conditions in the operating environment, or modifications to command priorities and mission imperatives.

6.8. **Integrating collection authorities.** The ISR architecture must include the three ISR specific roles to function effectively and efficiently. The actual employment and integration of these authorities will vary according to the operation. Configuration will be based on the needs of the operation or mission, its size and complexity and the forces under command.

Section 3 – Operational intelligence, surveillance and reconnaissance architecture

6.9. **ISR architecture.** Establishing the ISR architecture is a key function of ISR planning. The ISR architecture refers to the physical, virtual, digital and cultural structures that deliver ISR capability. It consists of the systems, tools and information technology connecting taskers, controllers, collectors, exploiters, databases, applications, requesters of data, information and results as well as operational data in a joint environment. The ISR architecture must be integrated with command and control, intelligence and operational capabilities and comply with legal and policy permissions and security protocols. In nearly all cases, the ISR architecture is the complexity driver for any deployed communication and information systems (CIS) networked capability.

6.10. **ISR architecture model approaches.** There is no fixed model and ISR authorities are used in a manner that is optimal for the given situation and may adapt with time. Some representative configurations for complex, medium scale and simple operations are shown at Figure 6.2.

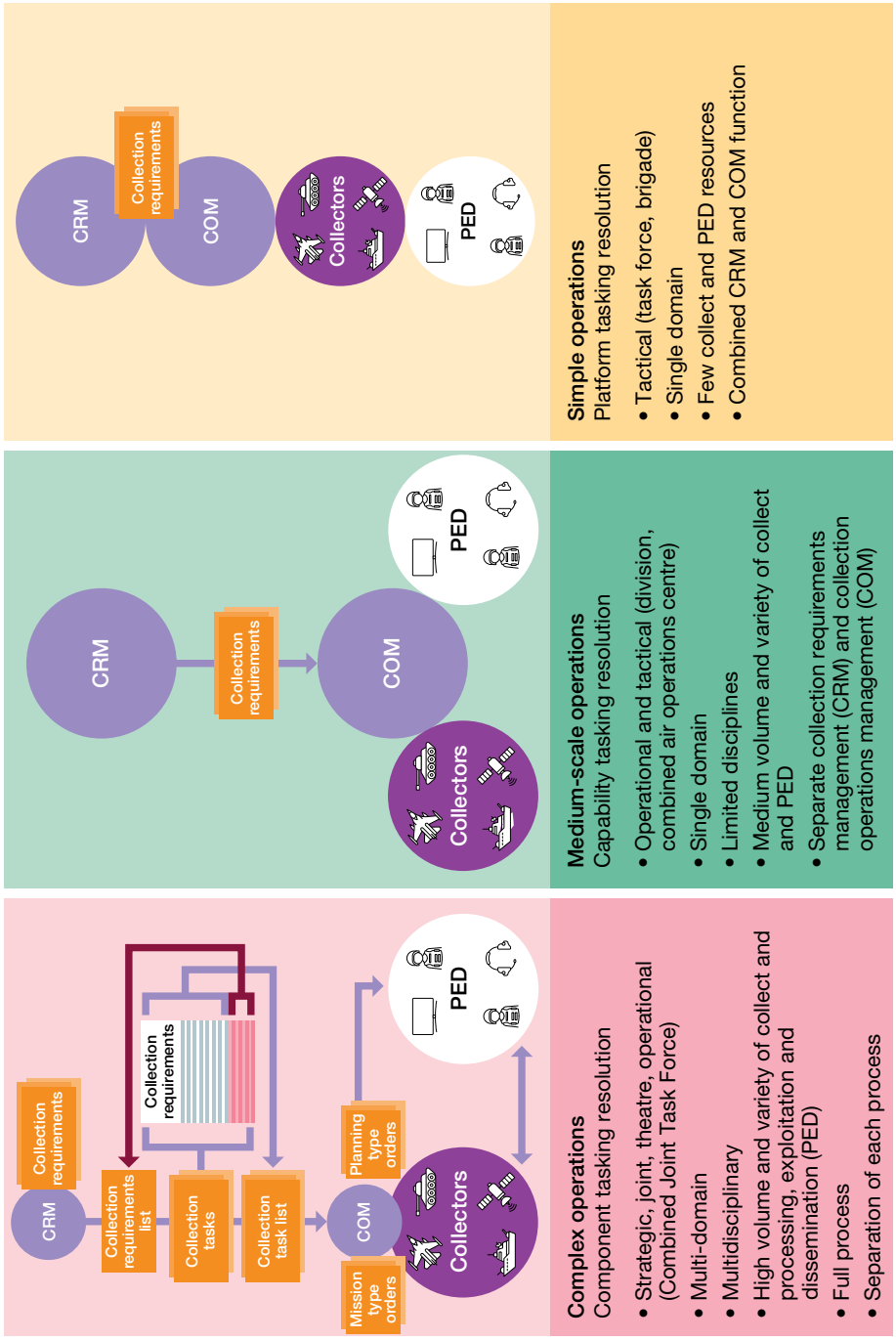


Figure 6.2 – Representative intelligence, surveillance and reconnaissance architectures

6.11. **ISR architecture design principles.** The design, establishment and management of ISR architectures for all operations, across all operational domains and at all levels of command, are based on the following principles and criteria.

a. **Flexible.** The ISR architecture must be established, practiced and evaluated to be capable of rapid transition to operations. The architecture must also be capable of being rapidly reconfigured to meet changing information needs throughout the operation.

b. **Mission tailored.** The ISR architecture must be specifically configured to support the planning and conduct of operations.

c. **Interconnected/discoverable.** The ISR architecture must connect all operational domains, levels of command, sensors, and PED, intelligence, operations and joint effects teams. By default, it should also be able to connect with allies and partners for tasking and for command and control of the enterprise. It must also facilitate the discovery and sharing of data, information and intelligence, including streaming real time data and archive data repositories.

d. **Compatible.** The ISR architecture must be compatible with both current and future technical constraints and standards. It must have sufficient network connectivity and appropriate broadband links.

6.12. **ISR networks.** ISR task, collect, process, exploit and disseminate networks should be as automated as possible. ISR networks consist of the physical, virtual and procedural components required for network integration, particularly common standards. These include the operational concepts, architecture, interoperability framework, key interfaces and formats needed to support operations.

a. **Bandwidth.** The ISR architecture reflects the communication networks and services available. The most significant focus is on bandwidths, stability and security to enable connectivity within and between components, operational domains, theatres and levels of command. Bandwidth is the key constraint in enabling the flow of data, information and intelligence, particularly where the data is large in size (such as high-definition imagery and streaming full motion video), or high volume (such as publicly available information). Sufficient bandwidth aids rapid decision-making, dynamic tasking and allows timely cross-cueing, PED reachback and access to large data stores.

b. **Data storage requirements.** ISR architectures require sufficient capability to store, share and archive data, information and intelligence to agreed standards and security requirements. For ad hoc architecture information exchange requirements, interfaces and standards must be addressed early during the planning process.[16]

c. **Full integration.** All ISR capabilities and assets should be fully integrated into the ISR architecture. ISR assets must have the ability to be responsive to every level of joint command and control (tactical, operational and strategic).

d. **Alternative structures.** Where network integration cannot be achieved, operations planning must consider the currently available systems and their respective capabilities and limitations. Operational orders should reflect these considerations and constraints.

6.13. **ISR architecture within the operation plan.** The high-level ISR architecture will be defined in a CDI Directive (which accompanies a Chief of the Defence Staff or Chief of Joint Operations Directive) and will be further refined in a subordinate Permanent Joint Headquarters (PJHQ) J2 Intelligence and Security Directive. Additional architecture refinements may feature in other operational staff work such as a concept of operations or operations plan. Regardless of which directives or operational documents are in use, the description of the ISR architecture will include the organisational responsibilities and relationships, and the supporting CIS architecture. It will also explain interoperability and integration between ISR capabilities, data, information, intelligence sources and PED tools. Defining the joint ISR architecture in the appropriate planning documents will ensure visibility within the operations, planning and communications staffs and will help identify and address potential shortfalls, risks, limitations, freedoms and constraints. ISR architecture will, at a minimum, include the following criteria, which are subject to further refinement for the duration of an operation:

- geographical location and characteristics of ISR systems and networks;

16 Information exchange requirements (IERs) define the need for information exchange between two or more parties that support a given process. IERs are pivotal inputs to the CIS planning process ensuring that all relevant command and control services required in support of the mission are identified, and adequate planning and provision of command and control services can be achieved. For more information on IERs, refer to Allied Joint Publication-6, *Allied Joint Doctrine for Communication and Information Systems*.

- asset capabilities, limitations and quantities to include PED requirements;
- functional services, bandwidth, connectivity, databases and other CIS support requirements;
- applicable/available standard operating procedures, standard operating instructions and reporting directives including data, information and intelligence reporting standards; and
- information security and information management provisions.

Section 4 – Intelligence, surveillance and reconnaissance support to operations planning and execution

6.14. **ISR support to operations planning.** ISR is critical for shaping the commander's and staff's understanding of the operating environment and informs all planning and decision-making. ISR planning is therefore an integral part of the operations planning process and must be included at the start of all planning activities. The ISR staff require clear, unambiguous direction and prioritisation on where and how ISR is to be employed. This direction should be governed by the principle of mission command with the commander describing what ISR needs to achieve, but not how the ISR staff is to achieve it. The ISR staff will integrate with the planning process to optimise the use of ISR capability in delivery of the commander's mission, tasks and intent.

6.15. **ISR operational outputs.** ISR supports the initial development of operational understanding through supporting the joint initial preparation of the operating environment, human terrain mapping and network analysis as well as support to understanding the information environment. ISR supports operations through, for example, providing support to develop the decision support overlay and decision support overlay matrix. ISR also supports targeting and joint effects through providing inputs to assist in developing the high-value target list, high pay-off target list, joint prioritised target list, full spectrum target lists and joint effects matrix.

6.16. **ISR tasking and direction.** ISR is directed through three mechanisms. These are the commander's operational design, the IRM process and the ISR request process.

a. **Operational design.** The operational design provides the commander's intent, scheme of manoeuvre, missions and tasks, and coordinating instructions. The operation order will indicate the commander's intent and priorities and the ISR annex provides direction for the ISR staff, specified ISR missions and tasks.

b. **Intelligence requirements management.** IRM is an external J2 intelligence process during which the intelligence staff analyse and refine requirements and identify intelligence gaps. Commander's critical information requirements will be generated during planning and a proportion of these requirements will be owned by the intelligence staff. The IRM process breaks these large questions down into smaller, more manageable and answerable problems. At every stage of this breakdown IRM staff will review data, information and intelligence holdings to ensure that the question cannot already be answered. The objective of this process is to reach a level where the initial question is translated into an information problem or essential elements of information (EEI). The complete breakdown of commander's critical information requirements and all their subordinate requirements to EEI-level results in a developed intelligence collection plan.[17] The intelligence collection plan is owned and managed by the intelligence staff but is linked with operations tools, including the decision support overlay, decision support overlay matrix, surveillance, target acquisition plan, commander's decision points and the operational synchronisation matrix.

c. **ISR requests.** The ISR request is the mechanism by which all other headquarters functions request ISR capability. The ISR request is used for all mission types except for indicators and warnings and joint intelligence preparation of the operating environment which use the IRM process. The ISR request process is used because many ISR tasks are not directly linked to intelligence requirements, for example, force protection overwatch of a unit conducting a strike operation. The

17 The intelligence collection plan does not constitute an actual plan for the employment of technical collectors and does not constitute an authority or direction to undertake collection; it is a tool for breaking down complex intelligence problems and understanding the IER to meet these needs.

ISR requirement would therefore not be captured within the intelligence collection plan but would be present within other planning tools such as a fragmentation order, the decision support overlay, or decision support overlay matrix. Under such circumstances the requirement has been validated during planning and the desired effect, location and timing for ISR has been confirmed. An ISR request is therefore normally communicated as a textual or visual concept of operations that explains what ISR support is required and why. This is submitted to the ISR staff for detailed, specialist planning.

6.17. **Effects-based tasking.** Irrespective of the source of external tasking, the tasking mechanism should always state the effect required, not a specific capability, platform or sensor. This allows the ISR staff a high degree of mission command and flexibility in meeting numerous, often competing priorities. It also allows for redundancy and resilience in meeting requirements. If a specific platform is requested and is not available, then the requirement would remain unsatisfied. Where a range of platforms and capabilities can be used, it may be possible to still meet the requirement using other means.

6.18. **Lateral and vertical requests and direction.** Both the IRM and CRM processes are used to request or direct ISR from higher, lower or laterally owned capabilities. Where elements of an intelligence collection plan are submitted to another headquarters in the form of a request for information, the receiving headquarters take on responsibility for answering the submitted request for information using their own intelligence staff, although this may involve them submitting requirements to their own ISR staff if collection is required. When the ISR request is used to request or task collection and PED from another headquarters it can also be a mechanism for requesting specific ISR capabilities, assets or platforms to enable the originator to fulfil requirements themselves, for example, an additional unmanned aerial vehicle platform or sensor type. It is normally used when the originating headquarters has insufficient capacity or capability to conduct one or more ISR tasks, rather than being unable to answer an intelligence question.

6.19. **Using ISR capability for non-ISR tasks.** ISR platforms and assets, like all other capabilities, may be used for purposes outside their primary role. As many ISR capabilities have considerable reach and endurance, they have broad utility for demonstrating posture, presence and profile. Additionally some ISR capabilities have utility in information operations and deception, whilst some ISR platforms can also create kinetic effects. The use of ISR capabilities for other tasks must be based on a full appreciation of the range of capabilities

and account for the cost/benefit balance and risk appetite. These must be a command decision, not a COM decision. Planning staff should ask if the required effect can be created in a manner where ISR benefit is also derived from the activity. Where this is not possible, ISR staffs should engage with the wider headquarters to establish if any requirements can be generated to take advantage of the activity. An ISR capability allocated wholly to non-ISR activity is removed from the ISR management and tasking process and subsumed into the relevant planning and operational process for the effect being created.

6.20. **Using non-ISR capability to support ISR tasks.** ISR planning staff may engage with operations planning staff to determine the availability of non-ISR assets to support the creation of effects against which ISR platforms and assets can collect against. This has particular use in identifying and assessing an adversaries' response to the creation of a particular effect.

Section 5 – Intelligence, surveillance and reconnaissance feedback and assessments

6.21. **Assessment and analysis of ISR system performance.** Assessing ISR performance is a critical aspect of ISR management. All ISR process functions are responsible for measuring their activity, performance and effectiveness and for actively seeking feedback. As ISR capability is frequently high value and low density and continual monitoring is required to optimise the value of resource and identify risks, issues, strengths and weaknesses. Assessments determine how well an ISR activity has performed and what is needed to better prepare for the next mission. Assessments are conducted on a continuous basis occurring after each mission. Measures of performance to assess ISR capabilities include those listed below.

- Did the ISR capabilities perform within technical standards?
- What were the volume requirements collected during the mission?
- Were mission objectives achieved?
- How did the mission contribute to answering the information and intelligence requirement?

- Do the mission objectives need to be adjusted for the next mission?
- Should a different capability be considered to meet mission objectives?
- If an objective was partially met, what is required for the objective to be fully met?
- Were the right mix of capabilities tasked to meet mission objectives?
- Did the command and control of the mission contribute to successful intelligence collection?
- Were there other capabilities which could have been used to cross-cue?
- What level and extent of interaction was there between the IRM and collection management staff, collection managers, operators and PED nodes?

6.22. **ISR support to evaluation.** In addition to assessment of ISR's performance and effectiveness itself, ISR is a vital tool for evaluating operations as a whole. In the operational context, evaluation is the observation and interpretation of progress towards desired conditions against selected criteria. ISR provides sensing and interpretation of detected objects, events, patterns and anomalies that assist the intelligence and operations staff in establishing initial baseline assessments from which deviation can be observed or assessed. This allows commanders and their staff to develop insight on successes or failures and to make decisions on future activity. From an ISR perspective, support to the evaluation of operations typically comprises missions to support assessments of effectiveness and performance.

a. **Assessments of effectiveness.** 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.[18] Assessments of effectiveness examine whether an operation is achieving its purpose. They monitor and assesses progress, including setbacks, to support planning decisions.

18 NATOTerm.

b. **Assessments of performance.** Measure of performance is defined as: a criterion that is tied to measuring task accomplishment in order to assess friendly actions.[19] ISR will support the work of intelligence staff to produce assessments that provide the commanders with agreed measures of performance.

6.23. **ISR support to battle damage assessment.** Battle damage assessment is defined as: the assessment of effects resulting from the application of military action, either lethal or non-lethal, against a military objective.[20] In addition to supporting more general assessment of operational performance and effectiveness, ISR provides specific support to targeting by providing battle damage assessment. ISR will often be a key provider of initial damage assessment. ISR may also provide or assist in providing functional damage assessment. While the target systems assessment is primarily an intelligence function, ISR plays a key supporting role in providing data and information which indicates how effects have changed observed systems from the baseline assessment, and to what extent.

Section 6 – Legal considerations

6.24. **ISR policy, permissions and legal considerations.** Adherence to the law is crucial in underpinning the legitimacy and campaign authority of any UK operation. ISR activity conducted within the context of a military operation will have legal considerations; there must be a basis for the activity and it must be conducted in a lawful manner. The applicable law will depend upon the overarching legal framework for a particular operation as well as the particular function conducted within each stage of the ISR process. Within PJHQ, for example, the legal annex of a Chief of Joint Operations Directive provides further guidance for specific operations. ISR activity must be consistent with the UK's obligations in international law, issued rules of engagement and applicable domestic law as well as relevant aspects of host-nation law and international human rights. To these may be added rights and obligations under United Nations Security Council resolutions or bilateral and multilateral agreements. Legal considerations applying to intelligence support to joint operations are detailed further in Joint Doctrine Publication 2-00, *Intelligence, Counter-intelligence and Security Support to Joint Operations*.[21]

19 NATOTerm.
20 NATOTerm.
21 Joint Doctrine Publication 2-00, *Intelligence, Counter-intelligence and Security Support to Joint Operations*. The 4th Edition is due to publish in 2023.

Key points

- ISR on operations is subject to three key authorities: CMA, CRM and COM.
- A CMA authorises and administers ISR activities and decides what can be collected.
- A CRM prioritises tasks and allocates resources. It decides what will be collected.
- A COM plans and executes ISR activities. It decides how collection will occur.
- ISR architectures must be flexible, tailored to the mission, interconnected and compatible with applicable technical standards.
- Bandwidth is the key constraint in enabling the passage of data, information and intelligence, especially large-sized data such as full motion video, or high-volume data such as publicly available information.
- ISR system performance must be continually reviewed for effectiveness and efficiency.
- ISR performs a key role in enabling wider evaluation of operational effectiveness.
- ISR operations must adhere to law and operation specific rules of engagement.

Lexicon

Section 1 –Acronyms and abbreviations

ABI	activity-based intelligence
AIntP	Allied intelligence publication
AJP	Allied joint publication
CDI	Chief of Defence Intelligence
CIS	communication and information systems
CMA	collection management authority
COM	collection operations management
CRM	collection requirements management
CTL	collection task list
DCDC	Development, Concepts and Doctrine Centre
EEI	essential elements of information
IER	information exchange requirement
IRM	intelligence requirements management
ISR	intelligence, surveillance and reconnaissance
JCMB	joint collection management board
JCMWG	joint collection management working group
JDN	joint doctrine note
JDP	joint doctrine publication
JISR	joint intelligence, surveillance and reconnaissance
MOD	Ministry of Defence
MTO	mission-type order
NATO	North Atlantic Treaty Organization
NDISR	non-dedicated intelligence, surveillance and reconnaissance
NIB	non-interference based
NTISR	non-traditional intelligence, surveillance and reconnaissance

OBP	object-based production
OODA	observe, orient, decide, act
PED	processing, exploitation and dissemination
PJHQ	Permanent Joint Headquarters
SOM	structured observation management
TCM	theatre collection manager
TCPED	task, collect, process, exploit and disseminate
TEM	theatre exploitation manager
UK	United Kingdom

Section 2 – Terms and definitions

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)

battle damage assessment
The assessment of effects resulting from the application of military action, either lethal or non-lethal, against a military objective. (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 NATO agreement)

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)

communications intelligence
Intelligence derived from electromagnetic communications and communication systems. (NATOTerm)

dissemination
The timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it. (Awaiting NATO agreement)

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

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)

information
Unprocessed data of every description which may be used in the production of intelligence. (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)

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 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, surveillance and reconnaissance request
A formal request for joint intelligence, surveillance and reconnaissance assets from adjacent or subordinate commands to support their prioritized intelligence requirements for a specific mission, operation or time period. (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-type order
An order issued to a subordinate unit that indicates the mission to be accomplished without specifying how it is to be done. (NATOTerm)

non-dedicated intelligence, surveillance and reconnaissance
Those assets not procured by the Ministry of Defence for specific intelligence, surveillance and reconnaissance tasks, but can contribute to the intelligence picture as part of their routine operations. (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)

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)

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

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

strategic intelligence
Intelligence required for the formulation of policy, military planning and the provision of indications and warning at the national and/or international levels. (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
In intelligence usage, a country, area, installation agency or person against which intelligence activities are directed. (NATOTerm)

target
An area, infrastructure, object, audience or organization against which activities can be directed 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)

Notes

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