NATO STANDARD

AJP-2.7

ALLIED JOINT DOCTRINE FOR JOINT INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE

Edition A Version 2

OCTOBER 2022

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

Intentionally blank

NORTH ATLANTIC TREATY ORGANIZATION

(NATO) STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

7 October 2022

1. The enclosed Allied Joint Publication AJP-2.7, Edition A, Version 2, ALLIED JOINT DOCTRINE FOR JOINT INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE, which has been approved by the nations in the Military Committee Joint Standardization Board, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 7107.

2. AJP-2.7, Edition A, Version 2, is effective upon receipt and supersedes AJP-2.7, Edition A, and Version 1, which shall be destroyed in accordance with the local procedure for the destruction of documents.

3. This NATO standardization document is issued by NATO. In case of reproduction, NATO is to be acknowledged. NATO does not charge any fee for its standardization documents at any stage, which are not intended to be sold. They can be retrieved from the NATO Standardization Document Database (https://nso.nato.int/nso/) or through your national standardization authorities.

4. This publication shall be handled in accordance with C-M(2002)60.

Dimitrios SIGOULAKIS
Major General, GRC (A)
Director, NATO Standardization Office

Intentionally blank

Reserved for national promulgation letter

Intentionally blank

RECORD OF NATIONAL RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

Intentionally blank

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
ALB	Intelligence assets of Albanian Armed Forces are not in compliance with this STANAG's requirements; therefore theyare not assuring interoperability in joint operations/activities with NATO.
GBR	Given the UK's close cooperation and integration with the US and Five-Eyes (AUS, CAN, NZL, UK, USA) intelligence communities (on specific operations and peace-time) the full-scale and enduring adoption of processes and procedures within AJP-2.7 across UK Defence may be compromised. Despite this, the UK's intention is it shalll be fully interoperable with NATO, especially when engaged on NATO multinational operations where NATO doctrine is accepted as the authorative standard.
USA	A number of terms introduced in this AJP do not conform to approved NATO terminology, of have been incorrectly introduced (ref NATO Terminology guidance found in C-M(2007)0023. The US recognizes only NATO approved terms. This reservation will be lifted when the correct NATO terms are cited and proper procedures followed for introducing new terms.
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

Intentionally blank

Summary of changes

- Expands description of JISR capabilities to include non-dedicated JISR assets/capabilities.

- Includes a more concise preface.

- Introduces description of federated process, exploit, disseminate management.

- Aligns with current NATO policy on JISR.

- Adds new figure depicting JISR synchronization and integration.

- Revises figure illustrating the JISR process and workflow.

- Adds figure depicting the relationship between the JISR process and the intelligence cycle.

- Deletes section on JISR-related terminology and adds NATO agreed JISR-related terms and definitions to the lexicon.

- Deletes section on JISR personnel and training requirements.

- Adds new annex describing how JISR supports joint targeting.

- Updates the description of JISR architecture.

- Enhances coherency by re-structuring the document and relocating relevant content.

.

Intentionally blank

Related Documents

Policy and MC documents

MC 0114	*Procedures for Production of NATO Agreed Intelligence*
MC 0128	*Policy Guidance for NATO Guidance*
MC 0582	*NATO Joint Intelligence, Surveillance and Reconnaissance Concept*
MC 0593	*Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations*
MC 0635	*WMD Disablement Functional Concept*
MC 0646	*NATO Joint Intelligence, Surveillance and Reconnaissance Policy*

Allied publications

AJP-01	*Allied Joint Doctrine*
AJP-2	*Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*
AJP-2.1	*Allied Joint Doctrine for Intelligence Procedures*
AJP-2.2	*Allied Joint Doctrine for Counter-Intelligence and Security Procedures*
AJP-2.3	*Allied Joint Doctrine for Human Intelligence*
AJP-2.4	*Allied Joint Doctrine for Signals Intelligence (SIGINT)*
AJP-2.6	*Allied Joint Doctrine for Imagery Intelligence (IMINT)*
AJP-2.8	*Allied Joint Doctrine for Measurement and Signature Intelligence*
AJP-2.9	*Allied Joint Doctrine for Open Source Intelligence (OSINT)*
AJP-3	*Allied Joint Doctrine for the Conduct of Operations*
AJP-3.1	*Allied Joint Doctrine for Maritime Operations*
AJP-3.2	*Allied Joint Doctrine for Land Operations*
AJP-3.3	*Allied Joint Doctrine for Air and Space Operations*
AJP-3.5	*Allied Joint Doctrine for Special Operations*
AJP-3.6	*Allied Joint Doctrine for Electronic Warfare*
AJP-3.8	*Allied Joint Doctrine for Comprehensive Chemical, Biological, Radiological and Nuclear Defence*
AJP-3.9	*Allied Joint Doctrine for Joint Targeting*
AJP-3.10	*Allied Joint Doctrine for Information Operations*
AJP-3.17	*Allied Joint Doctrine for Geospatial Support*
AJP-3.20	*Allied Joint Doctrine for Cyberspace Operations*
AJP-5	*Allied Joint Doctrine for the Planning of Operations*
AJP-6	*Allied Joint Doctrine for Communication and Information Systems*

Standardization documents

AIntP-10	*Technical Exploitation*
AIntP-13	*Human Network Analysis and Support to Targeting (HNAT)*
AIntP-14	*Joint Intelligence, Surveillance and Reconnaissance (JISR) Procedures in Support of NATO Operations of NATO Operations*
AIntP-16	*Intelligence Requirement Management and Collection Management*
AIntP-17	*Joint Intelligence Preparation of the Operating Environment (JIPOE)*
AIntP-18	*Intelligence Processing*
AIntP-24	*Intelligence Support to Targeting*

Other

Allied Command Operations *Comprehensive Operations Planning Directive* (COPD)
NATO *Lessons Learned Policy*, PO(2011) 0293-AS1, 09 September 2011
BI-SC DIRECTIVE 080-006, *Lessons Learned,* 23 February 2018

Table of contents

Lexicon

List of figures

Preface

Context

1. The joint intelligence, surveillance and reconnaissance (JISR) process is central to providing intelligence for decision-making for support to NATO operations. As a framework for interoperability, the JISR process ensures the most efficient integration and usage of JISR capabilities supporting the wider collection management process. Sharing the information and intelligence derived from JISR capabilities benefits commanders, staff and operators by enabling informed, proactive decision-making.

Scope

2. *Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance* (AJP-2.7) provides the fundamentals, principles, activities and planning considerations for the conduct of JISR activities at the NATO joint force command (JFC) headquarters. As an operational-level publication, applicable to all levels of operations, AJP-2.7, focuses on the JISR process, describing how intelligence collection disciplines, collection capabilities (dedicated and non-dedicated JISR capabilities) and intelligence exploitation activities can provide data, information or intelligence to satisfy collection requirements. It does not dictate detailed arrangements and procedures but refers where appropriate to the level 3 series of allied intelligence publications (AIntPs).

Purpose

3. The purpose of AJP-2.7 is to describe the procedures and considerations required to conduct JISR activities that support the decision cycle and enhance the intelligence cycle.[1] AJP-2.7 improves coordination and interoperability by providing guidance for NATO JFC commanders and staffs executing JISR activities.

Application

4. AJP-2.7 primarily applies to NATO JFC commanders and staff at the JFC operational level. The doctrine also provides a general framework to facilitate a common understanding of JISR activities throughout all levels of NATO's command structure.

Structure

5. AJP-2.7 consists of four chapters.

- Chapter 1 – Overview. Defines the term "JISR" and describes its relationship with the intelligence and decision cycles.

[1] The intelligence cycle is also referred to as the intelligence process. Some nations use different intelligence processes and models in accordance with their national doctrines.

- Chapter 2 – JISR fundamentals. Identifies the key principles, staff management functions and planning considerations for the successful conduct of JISR.

- Chapter 3 – JISR process. Describes each step of the JISR process in answering a collection requirement.

- Chapter 4 – JISR architecture considerations. Provides key JISR planning and architecture design considerations.

Linkages

6. Within the hierarchy of intelligence doctrine publications, AJP-2.7 is subordinate to the keystone intelligence document *Allied Joint Doctrine for Intelligence, Counter-intelligence and Security* (AJP-2). However, AJP-2.7 is closest to and should be read in conjunction with the following intelligence doctrine publications:

- *Allied Joint Doctrine for Intelligence Procedures*, (AJP-2.1), which describes procedures, interdependencies and considerations required to conduct intelligence operations in support of NATO;

- *Allied Intelligence Publication* (AIntP-14), *Joint Intelligence, Surveillance and Reconnaissance Procedures in Support of NATO Operations,* which provides JFC commanders and their staffs with detailed procedures and tactics; and

- *Allied Intelligence Publication,* (AIntP-16), *Intelligence Requirement Management and Collection Management,* which explains the role of intelligence requirements management and collection management (IRM&CM) as a core function within the intelligence cycle and describes how IRM&CM activities are planned, conducted and assessed in NATO.

7. AJP-2.7 is linked to:

- MC 0646 (2017), *NATO Joint Intelligence, Surveillance and Reconnaissance Policy*, to transfer policy and conceptual thinking into established doctrine:

- AJP-2 series doctrine publications, which include descriptions of the intelligence collection disciplines;

- AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, to provide coherence with the NATO approach to operations; and

- AJP-5, *Allied Joint Doctrine for the Planning of Operations*, to provide coherence with the operations planning process

.

Chapter 1 – Overview

Section 1 – Introduction

1.1 **Role of intelligence.** The primary role of intelligence is to contribute to a continuous and coordinated understanding of a complex environment, to provide new knowledge and to enhance the decision-making process and facilitate mission accomplishment.[2] Decision-makers and planning staffs must have accurate and timely information[3] and intelligence[4] about the dynamic and multifaceted security and operating environments (OE). Joint intelligence, surveillance and reconnaissance (JISR) activity is crucial in seeking information advantage not only during crisis and conflict but is also crucial to develop and maintain basic intelligence.[5]

1.2 **Understanding the operating environment.** To aid the commander and staff in gaining an understanding of the complex and interconnected OE, intelligence analysts develop and produce joint intelligence preparation of the operating environment (JIPOE) products. To address knowledge gaps identified through the JIPOE process, there is a need for ongoing data and information collection. JISR collection capabilities are the means that enable JIPOE analysts to develop and apply appropriate analytical strategies to develop the type of knowledge necessary to define and understand the OE.

Section 2 – Joint intelligence, surveillance and reconnaissance approach

1.3 **Definition.** JISR is an integrated intelligence and operations set of capabilities, which synchronizes and integrates the planning and operations of all collection capabilities with processing, exploitation, and dissemination of the resulting information in direct support of the planning, preparation, and execution of operations. The term “JISR” consists of four distinct elements.

a. **Joint.** The term “joint” refers to the activities, operations and organizations in which elements of at least two services participate. During operations, components and services operate with greater effectiveness

[2] Intelligence is one of many sources that assist a decision-maker. It offers a unique and valuable alternative insight to decision-makers, thereby enhancing their ability to bring their influence to bear towards the achievement of objectives. Ideally, intelligence is provided by staff who are attuned to the decision-maker's dilemma.

[3] Information is defined as unprocessed data of every description, which may be used in the production of intelligence.

[4] Intelligence is defined as 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.

[5] Basic intelligence is intelligence, derived from any source, that may be used as reference material for planning and as a basis for processing subsequent information and intelligence. It is produced as part of routine monitoring or on a contingency basis, for example: orders of battle; equipment capabilities and performance; profiles of personalities, infrastructure factors, socio-political descriptions and environmental aspects. Basic intelligence, continuously reviewed and updated, is useful reference material on which to develop current intelligence. Basic intelligence provides the context and backdrop against which current intelligence is reviewed.

and efficiencies by integrating available intelligence, surveillance and reconnaissance (ISR) capabilities. JISR integration is not only the technical connection of various ISR data sources but also the operational integration, command and control and tactical employment of ISR capabilities.

b. **Intelligence.** The term “intelligence” refers to all intelligence collection disciplines to include their collection, processing, exploitation and dissemination capabilities/assets and the results they can deliver to the commander, intelligence staff or other staff elements. Intelligence collection disciplines are the means or systems used to observe, sense and record or convey information about conditions, situations, threats, opportunities and events. Intelligence collection disciplines include:

(1) **Acoustic intelligence (ACINT).** ACINT results are based on the collection and exploitation of acoustic signals or emissions.

(2) **Human intelligence (HUMINT).** HUMINT results are based on information which is collected and provided by human sources.

(3) **Imagery intelligence (IMINT).** IMINT results are based on imagery acquired from sensors that can be ground-based, seaborne or carried by air or space platforms.

(4) **Measurement and signature intelligence (MASINT).** MASINT results are based on 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.

(5) **Open source intelligence (OSINT).** OSINT results are based on openly available information.

(6) **Signals intelligence (SIGINT).** SIGINT results are based on the collection and exploitation of electromagnetic signals or emanations. The main subcategories of SIGINT are communications intelligence and electronic intelligence.

The intelligence collection disciplines are best used to contribute to fused products where relevant data and information from all disciplines are used to contextualize and inform reporting. However, the collection results derived from one or more of the intelligence collection disciplines can contribute to intelligence sub-disciplines, applications and activities resulting in specialized intelligence products.[6] Intelligence sub-disciplines, applications, activities and products include, but are not limited to:

[6] Refer to *Allied Joint Doctrine for Intelligence, Counter-intelligence and Security* (AJP 2) for more detailed information on specialized intelligence products.

- armed forces intelligence;
- chemical, biological, radiological and nuclear-related intelligence;
- biometrics-enabled intelligence;
- identity intelligence;
- document and media exploitation;
- technical exploitation;
- human network analysis;
- geospatial intelligence;
- medical intelligence;
- scientific and technical intelligence;
- security intelligence; and
- ▪ target intelligence.

c. **Surveillance.** Surveillance is the systematic observation across all domains, places, persons or objects by visual, electronic, photographic or other means. Surveillance is designed to provide indications and warning of adversary initiative and threats and to detect changes in adversary activities. Surveillance may also be used to observe changes in friendly (non-adversary) activities.[7] It can provide early warning of activity over a wide area, or can focus upon a particular location, facility, activity or actor within the OE to include cyberspace. Over extended periods of time, surveillance enables pattern of life analysis, which can lead to an in-depth understanding of threats, activities or behaviour.

d. **Reconnaissance.** The term **“**reconnaissance” refers to an information-gathering 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. It is a focused method of collecting information about specific locations, facilities or people. In addition to national and theatre assets, special reconnaissance operations can also be tasked to obtain specific, time-sensitive information of significance.[8] However,

[7] Conventional surveillance radar is used to conduct surveillance of airspace and create a recognized air picture that underpins all operations, be it to detect and monitor threats; safeguard civil air traffic or assist the command and control of friendly aircraft.

[8] Special operations forces conduct reconnaissance and surveillance activities in high-risk environments to include human intelligence collection, close target reconnaissance, or the employment of ISR assets.

reconnaissance tasks are not confined to specific reconnaissance units, but may be undertaken by other force elements in the course of their duties. Reconnaissance enables the collection of specific information within the joint operations area in support of current and future operations. It collects results through visual observation or other detection methods to provide specific information to the requester.

Section 3 – Joint intelligence, surveillance and reconnaissance and the intelligence cycle

1.4 As a multi-disciplined and methodical approach, JISR is designed to satisfy the information requirements of commanders and operational staffs for the preparation, planning, execution and assessment of operations and the conduct of headquarters functions. JISR is the active collection of information about all aspects and dimensions of the OE through the use of sensors and application of intelligence methods. The JISR process is interlinked with the direction, collection and processing stages of the intelligence cycle (Figure1.1).

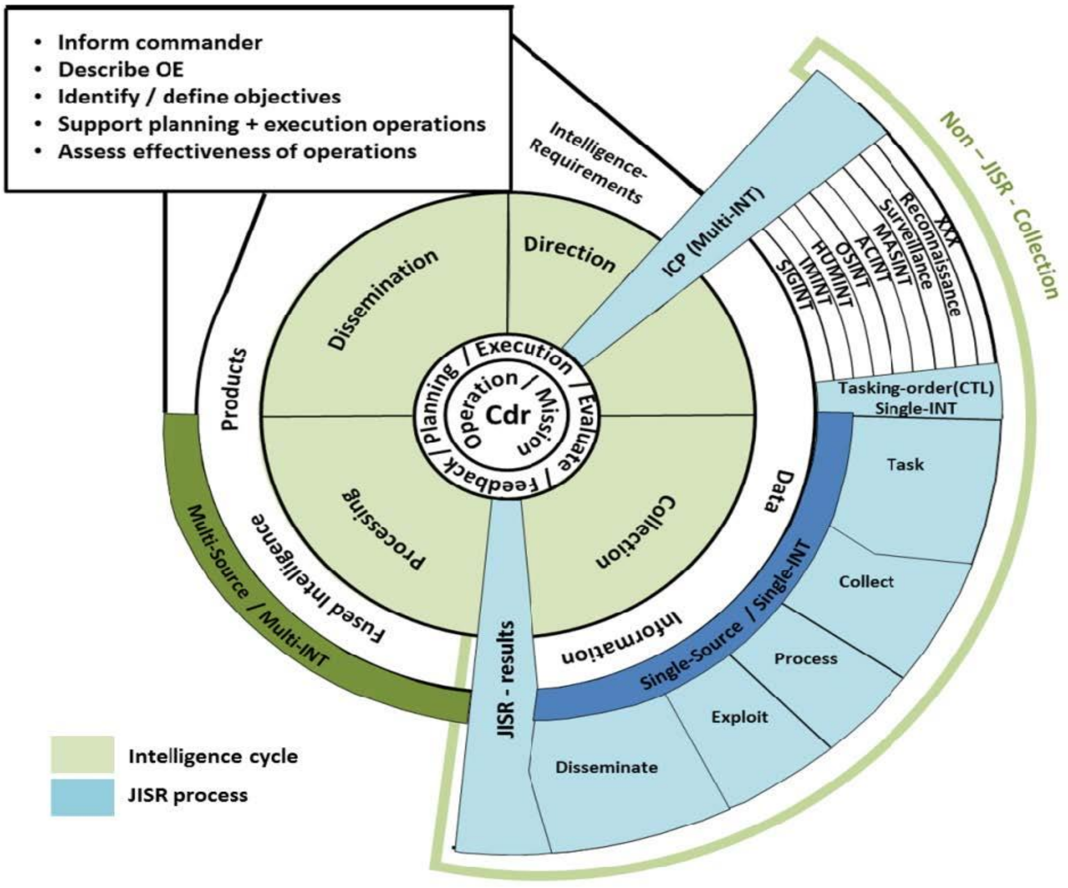

Figure 1.1 – Relationship between the intelligence cycle and the JISR process

1.5 The JISR process is the means to provide data, information and single discipline intelligence to address an intelligence requirement. The JISR process consists of five steps: task, collect, process, exploit, disseminate (TCPED) to convert collection tasks into single source/discipline JISR results. JISR results, in turn, can be fused with other information to produce intelligence, or sent directly to the requester to meet time critical requirements.

1.6 All-source intelligence analysts rely on a variety of collection capabilities as well as surveillance and reconnaissance activities to collect data and information. To draw intelligence, surveillance, and reconnaissance collection capabilities into a coherent whole, the JISR process provides for the effective management, coordination and tasking of these collection assets to address information or intelligence requirements in a deliberate, ad hoc or dynamic time frame. As an operations-intelligence process, JISR brings the intelligence disciplines and collection capabilities, including processing, exploitation and dissemination capabilities, together within a construct to enable the retrieval and sharing of information required for mission accomplishment.

1.7 JISR is a continuous process that not only contributes to understanding and can provide information advantage in times of crisis and conflict, but can also play an essential role in supporting peacetime operations. JISR, as a capability, provides support to a wide range of operational activities and intelligence mission requirements. JISR capabilities and activities provide measurements, images and other samples of the OE. These, along with predictive analysis, can provide planners, operators and decision makers with awareness and knowledge of the terrain, weather, the locations, as well as the status and intentions of the threat. The specific type of mission will shape JISR employment in the OE. JISR activities and results can provide support and contribute to:

- understanding the OE and the electromagnetic environment;
- identifying and prosecuting high value targets;
- operations;
- targeting;
- indications and warning;
- threat warning;
- orders of battle development (ground, air, missile, naval, electromagnetic, cyber and space);
- technology and capability development analysis;
- countermeasure development;
- force protection;
- fixed point security; and

- database maintenance.

Section 4 – Joint intelligence, surveillance and reconnaissance synchronization and integration

1.8 This section highlights how the JISR process and TCPED steps are synchronized within the intelligence cycle and integrated within the decision cycle to satisfy information and intelligence requirements (Figure 1.2). In addition to linkages with these cycles, JISR is also linked to the joint planning process.

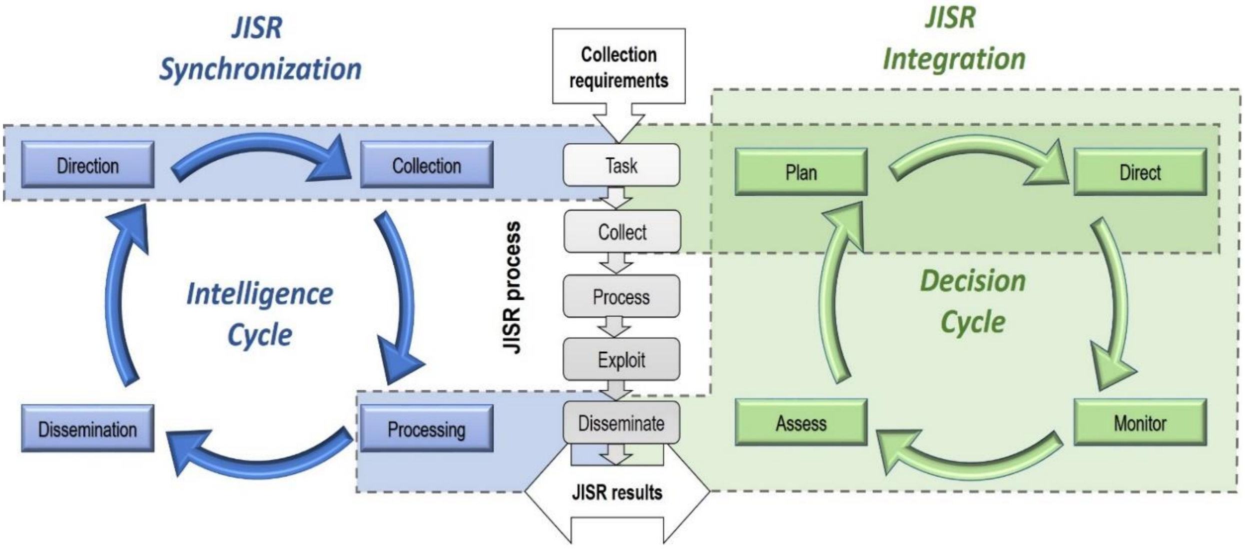

Figure 1.2 – JISR synchronization and integration

a. **JISR synchronization.** The JISR process should not be viewed as a process that is conducted in isolation from the intelligence cycle. The JISR process is synchronized with the direction, collection, and processing stages of the intelligence cycle. Within the direction and collection stages, the JISR process is initiated by identifying intelligence and information requirements and developing collection plans to satisfy them. As data and information are collected, analysts fuse these results with other sources of data and information during the processing stage of the intelligence cycle or within the TCPED process itself. Therefore, a dialogue needs to be maintained between the intelligence planners, analysts, collection requirements and collection operations management staffs to ensure JISR capabilities are efficiently and effectively optimized. JISR synchronization ensures the commander's requirements drive JISR planning and execution activities and ensures reporting responds in time to support decision-making and the conduct of operations.

b. **JISR integration.** The operations process and the intelligence process are mutually dependent. The commander, through the operations process, provides the guidance and focus through the commander's critical information requirements and priority intelligence requirements that drive the intelligence process and JISR process providing the continuous intelligence essential to the operations process. JISR integration refers to the coordination between the collection management function and operations staff for the effective and efficient planning and execution of JISR operations. As collection requirements and tasks are developed, the operations staff responsible for tasking and controlling JISR capabilities, will integrate JISR assets into the mission planning phase of the decision cycle. This enables the actual execution of collection and the integration within the overall joint operations process. Moreover, JISR mission integration is not limited to deliberate planning aspects and becomes even more demanding when satisfying emerging ad hoc or dynamic collection when missions are already underway.

Intentionally blank

Chapter 2 - Joint intelligence, surveillance and reconnaissance fundamentals

Section 1 – Introduction

2.1 Joint intelligence, surveillance and reconnaissance (JISR) capabilities and activities need to fulfill the broadening scope of information and intelligence requirements to support the planning, preparations and conduct of operations by NATO at the strategic, operational and tactical levels and in all phases of operations. This chapter describes the fundamental aspects of the JISR process to include the key principles, management functions and planning factors.

Section 2 – Joint intelligence, surveillance and reconnaissance principles

2.2 The harmonization of intelligence and operations functions provides decision-makers with timely intelligence and maximizes the efficiency and effectiveness of JISR capabilities. Within the JISR process, there are six key principles that are appropriate at all levels across the full range of NATO operations.

a. **Centralized direction; decentralized execution.** The JISR process encompasses the principle of centralized direction with decentralized execution. JISR activities must be command-led and centrally coordinated to set the conditions for mission success, while enabling delegation of JISR planning and execution at lower levels when necessary or appropriate. Commanders should set priorities and direct the JISR effort to meet operational requirements and to integrate intelligence with operations planning.

b. **Responsive.** JISR capabilities should be responsive, timely and flexible to satisfy the needs of the requester in accordance with extant prioritization. The JISR process should be adaptable and able to respond to evolving situations, new information and revised requirements at all times. The right mix and numbers of JISR capabilities with associated process, exploit, disseminate (PED) resources will provide commanders the flexibility and agility to respond effectively. This can be achieved through layering, massing and sequencing as well as cross-cueing between assets of differing capabilities.[9] JISR results should be delivered with due timeliness according to the needs specified in the collection requirement (CR). The collected data, information or intelligence will

[9] ISR layering is the opportune stacking of ISR capabilities overlapping in time within a defined area, which is not part of a pre-mission plan to maximize synergistic ISR effects. ISR massing is the deliberate stacking of ISR capabilities in time within a defined geographic area. Sequencing is the deliberate use of multiple assets at different times to exploit a defined area of interest or target. Cross-cueing is when one asset or sensor receives an indication and sends that information to another asset to perform some action, usually collection in order to confirm, corroborate, or refine the data and information from the first asset or sensor.

be of limited or no value if it is not available when needed.[10] Moreover, the JISR process should be responsive across the joint operations area to the requests and tasks from all levels of command. To that end, JISR assets typically tasked at the operational level must be able to integrate with and provide direct support to tactical units. Conversely, tactical units and assets may be required to support operational and strategic requirements.

c. **Accessible.** To the extent possible, JISR results should be available and accessible to those who require it and in accordance with NATO information exchange and information security procedures. An enterprise architecture and interoperable mechanisms are required to allow timely and seamless sharing of information and intelligence across NATO. Elements of information/intelligence at the strategic level will have utility at the tactical level but will often reside on higher classification systems and the information itself will often be at a higher classification. The JISR architecture needs to take into account both the classification of the system as well as the classification of the JISR result.

d**.** **Sustainable.** JISR capabilities need to be sustainable to meet mission requirements. JISR collection assets are often scarce and should be considered high value assets by commanders which must be appropriately defended where necessary. If an asset is destroyed, disabled, or becomes unavailable, commanders need to consider how to compensate for the loss of JISR capabilities. In addition, commanders need to consider how to resource and sustain continuous PED activities across the multiple intelligence collection disciplines.

e. **Reliable.** To give commanders and their staff confidence in JISR results, the results must be disseminated in a way that clearly and honestly outlines the likelihood of the capability to obtain the desired results and any factor that may have affected the collection and thus the results. PED elements will need to provide timely results contributing to accurate situational awareness and understanding allowing commanders to maintain an information advantage.

f. **Accurate.** JISR results should help to answer intelligence requirements in the most accurate way possible. Accuracy needs to be continuously maintained throughout the JISR process, from the initial tasking through collection, processing, exploitation and dissemination. Objective, clear, unbiased and undistorted JISR results are critical to support subsequent all-source intelligence processing, as well as to prevent reliance on single-source confirmation or circular reporting.

[10] Response time is the time between the initiation of an intelligence requirement and the receipt of an answer. Reporting time is the lapsed time between a source collecting an item of data and when it is processed and disseminated in the desired format.

Section 3 – Joint intelligence, surveillance and reconnaissance management staff functions

2.3 **Introduction.** The JISR process seeks to enhance and optimize how decision makers, operators, planners, staff and requesters are provided with the information they need to fulfil their mission. The JISR process is supported by all staff elements. However, the core JISR management functions are performed by an intelligence, surveillance and reconnaissance (ISR) staff comprised of intelligence and operations staff elements. This section describes the management staff functions and staff elements at the joint force command (JFC) operational level that play key roles in implementing and executing the JISR process and the task, collect, process, exploit, disseminate (TCPED) activities.

2.4 **Intelligence requirements management (IRM).** As a pre-requisite to the JISR process itself, IRM is an intelligence management staff function that validates, refines, and prioritizes intelligence requirements (IRs). The IRM function initiates the search for available products/results that may answer the requirement, ensures quality control of processed outputs and oversees the dissemination of products and results. IRM occurs at all levels of command and is an integral function within the direction and dissemination phases of the intelligence cycle. IRM responsibilities include:

a. **IR processing.** If existing products/results are available in a database that can satisfy the IR, an analytical review by intelligence analysts should be conducted prior to disseminating the response to the requester. If a product does exist, the analyst must seek approval from the originator/requester to determine if the product meets the operational need. If existing products/results are not available, the IR is either handled as a request for information and sent to a higher or adjacent formation or the IR is converted into a CR through the collection management (CM) function.[11]

b. **Intelligence collection plan (ICP).** Based on the commander's prioritized intelligence requirements (PIRs),[12] the intelligence requirements management and collection management (IRM&CM) function develops the ICP.[13] The ICP serves as one source for the planning and requesting of collection activities using available assets or requesting information from various sources. The ICP details which JISR assets will be allocated against each collection task.

2.5 **Collection management (CM).** CM is the process of satisfying CRs by tasking, requesting or coordinating with appropriate collection sources or agencies,

[11] Refer to Allied Intelligence Publication*, Intelligence Requirements Management and Collection Management* (AIntP-16) for detailed information on the RFI process.

[12] Prioritized intelligence requirements (PIRs) are produced by intelligence staff and form the J2 function's internal direction. PIRs are derived from the direction given by the hierarchy through the commander's critical information requirements.

[13] The intelligence collection plan (ICP) is a detailed breakdown of how each intelligence requirement is to be satisfied and includes the organizations, agencies or assets best suited to accomplish the task. The ICP is developed as a tool for the IRM&CM function inside the intelligence cycle.

developing PED plans, monitoring results and re-tasking, as required. CRs are tied to the essential elements of information (EEI) in order to answer PIRs necessary for decision making. EEIs are broken down into observables expected from ISR sensors. CRs are best stated in time, space, and purpose and linked to a specific desired effect which must be supported with ISR. The aim of the CM staff is to ensure JISR tasks are focused on the commander's intelligence and operations priorities. Within CM, collection management authority (CMA) is a delegated authority that establishes the guidance and policies associated with the planning and the execution of collection operations.[14] The CM function includes the two sub-functions: collection requirements management (CRM) and collection operations management (COM).

a. **Collection requirements management (CRM).** The CRM staff management function determines what is to be collected based on the prioritization of requirements from the IRM function and operational staffs. As a CM sub-function, CRM is responsible for the prioritization, development and control of collection, processing, exploitation and information reporting requirements. Within this function, CRM staff elements receive validated IRs from the IRM function or requests for collection and then validates them. The collection manager will either forward tasking requirements to units over which the commander has authority or generate requests for the use of additional assets to accomplish the collection mission. CRM functions include:

- prioritizing CRs that should be based on the commander's intent, objectives, approved PIRs, and the current situation to ensure that the limited assets or resources are directed against the most critical requirements;

- developing a coordinated, coherent, collection strategy to satisfy validated and prioritized CRs. The collection strategy is a scheme for collecting information from all available sources to satisfy intelligence and operational requirements;

- supporting the deliberate planning effort and development of specific collection, exploitation and dissemination directives matching emerging CRs; and

- ensuring the synchronization of deliberate, ad hoc, and dynamic JISR asset tasking and the coherence of the overall collection, processing, exploitation and dissemination effort.

b. **Collection operations management (COM).** COM is an ISR staff function exercised by the component, formation or unit and integrates collection operations into the overall operations plan. The COM sub-function plans and executes JISR tasks issued by the CRM and decides how collection capabilities

[14] CMA is a delegated responsibility that ensures unity of the collection effort, effectively employs synchronized collection to support operations, assesses the collection process and may reside at the JTF level or may be delegated to components.

are employed and optimized to meet requirements. Key tasks of the COM sub-function involve managing the operation of JISR assets, performing collection, the processing and exploitation of data and information, and the dissemination of JISR results as well as assessing how well JISR capabilities satisfy requirements. COM responsibilities include:

- directing, scheduling, prioritizing and controlling specific collection operations and associated processing, exploitation and information reporting resources;
- conducting mission integration;
- developing a JISR synchronization matrix;[15]
- coordinating with PED nodes;
- maintaining situational awareness of ongoing JISR missions;
- responding to dynamic situations and making recommendations for the reallocation of JISR collection assets;
- adjusting the resourcing of collection tasking plans within the resourcing available in order to meet mission requirements. This is necessary given the likely dynamic loss and gain of available capabilities during mission execution;
- assigning JISR tasks to assets over which the command has authority; and
- preparing the collection and exploitation plan (CXP).[16]

2.6 The principal CM positions and coordination management entities that are integral to the JISR process include the following:

a. **Collection managers.** Collection managers play a key role in preparing a collection strategy that details which JISR asset will be allocated against each collection task.

b. **Theatre collection manager (TCM).** The commander may appoint a TCM to conduct CRM and COM activities at the theatre level for a given

[15] The CM will track the status of planned collection assets and their tasking using a JISR synchronization matrix. The matrix may include station times, track names, sensor types, call signs, mission numbers, day/night transition times, strike and/or operations windows, major decision points and other information as needed. In creating the JISR synchronization matrix, opportunities for cross-cueing assets should be considered and scheduled if possible.

[16] The collection and exploitation plan (CXP) is a plan that provides detail of the tasks assigned to specific JISR capabilities, including PED, to meet the formation's JISR collection and exploitation requirements. The CXP is based upon CRs and direction from the JCMB articulated through the CTL.

operation. The TCM, at the joint force command with this authority, executes CRM and COM as a collective and joint function and is supported by subordinate tactical commands. While each level of command can execute a degree of CRM, the overall CRM authority is vested in the TCM. Each level of command develops and prioritizes its own CRs then forwards the CRs to the CRM authority (TCM) for theatre prioritization in the collection task list (CTL).

c. **Joint collection management board (JCMB).** A JCMB should be established and comprised of representatives from the intelligence, operations and targeting staff, intelligence collection disciplines and liaison officers (LOs) as well as LOs from adjacent and higher echelons.[17] A JCMB is established to facilitate the coordination of JISR activities between the different service components and the intelligence and operations staffs. The JCMB meets to synchronize, prioritize and deconflict competing collection requirements across the joint operations area. The JCMB may establish a joint collection management working group to support the preparation, approval process and distribution of the CTL.

2.7 **JISR synchronization and integration activities.** The CRM and COM staffs, together with the TCM and the JCMB, ensure JISR tasks are integrated in time and space into ongoing operations at all levels. JISR synchronization and integration activities demand robust collaboration and communication between requesters who submit requests and requirements and the intelligence and operations staffs who coordinate to satisfy them. The timely harmonization of the working procedures between the intelligence and operations staffs is achieved through an adapted battle rhythm and established planning. These activities will require commanders and staffs to:

- establish appropriate command and control relationships;
- implement tasking and reporting procedures supported by data, information, intelligence and communication systems;
- manage CRs and collection operations;
- determine priorities;
- articulate requirements; and
- allocate JISR capabilities to specific commands.

[17] LOs bring knowledge of their component's intelligence, surveillance and reconnaissance (ISR) capabilities to the joint operating environment. LOs should work closely with the CM function and liaise with CRM and COM elements to coordinate, plan and manage JISR operations. LOs are assigned to host organizations and work according to the given battle rhythm.

Section 4 – Process, exploit, and disseminate management

2.8 **PED management.** PED management is part of the CM function. PED management ensures the exploitation workload is deconflicted and distributed among the various PED nodes in accordance with their capability and capacity to exploit collected data, information and material. Once the PED nodes are identified, a PED manager coordinates with the PED nodes to optimize exploitation capabilities across all levels of command and operations.

2.9 **Process, exploit, and disseminate (PED) capabilities.** PED capabilities are integral to the JISR process. A PED capability includes:

- equipment that receives, processes (turns the data into a usable form), relays and stores or transmits collected data;
- communications systems architecture and associated bandwidth/throughput that moves collected data to an exploitation centre;
- exploitation teams that receive processed data, assess the data to generate a JISR result and disseminate the JISR result; and
- appropriately trained and qualified personnel.

2.10 PED capabilities may also include remote or distributed sensor control and data link operations depending on the technical design of the specific ISR asset or capability. For example, artificial/automated intelligence or machine learning algorithms are incorporated into the design of the distributed sensor(s).

2.11 **Federated processing, exploitation and dissemination.** Traditionally, PED has been conducted within a single unified chain of command with strictly defined command and control relationships. Given a high volume of collected data, a federated approach is needed using multiple PED capabilities. Federation is achieved by tasking different PED nodes to process and exploit data and information from collection capabilities controlled by other entities and disseminate JISR results. The aim is to maximize the efficient usage of PED capabilities that are available across all echelons or commands and national entities. Federated PED:

- optimizes and maximizes the analytical capabilities across all levels of command and operations;
- increases sharing data/information and the exchange of processed intelligence;
- distributes exploitation workload among the federated PED efficiently;
- satisfies a higher volume of exploitation tasks in a timely manner; and
- increases the possibility for sensor/platform cross cueing.

2.12 Federated PED encompasses designated PED nodes, centralized management, a systems architecture, an information management system and requires a protected communications network.

a. **PED nodes.** A PED node is an entity that uses data or information collected by a sensor or source to generate a JISR result. JISR results contribute to describing the operating environment (OE) and could have an immediate impact as actionable intelligence. However, a PED node can only support the types of JISR missions that collect data that is exploitable by the capabilities present at the PED node. Each contributing PED node is responsible for reporting its results and satisfying mission requirements. For example, one nation could be tasked with a collection requirement for signals intelligence ISR. The raw data that is collected could then be transmitted to another nation's PED node for exploitation and the dissemination of the JISR result.

b. **PED systems architecture.** A federated PED systems architecture enables collection managers to better leverage JISR resources within the Alliance where raw data collected by one ISR asset is accessible or transmittable for exploitation and dissemination by a PED node from another system or nation.

c. **PED visualization.** To satisfy information management requirements, an integrated geospatial information system should enable the visualization and planning of geographically-focused tasks while allowing the direct interaction with underlying data.

2.13 Federation of collection assets and PED capabilities enables a more efficient execution of JISR by effectively increasing the total number of available sensors. Given the low density/high demand of certain available assets capable of intelligence collection, it is essential that nations contribute as many different types of sensors as possible. Within the federated PED method, synchronization and deconfliction mechanisms are needed to minimize duplication and maximize collection and PED efficiency. To that end, each component commander should have a single focal point for the coordination and communication with sensor providers. In addition, sensor providers must be able to transfer data into a common network accessible by federated PED nodes. Furthermore, nations should be proactive in seeking solutions to share classified data and information from national capabilities within a wider NATO federated PED network.

Section 5 – Joint intelligence, surveillance and reconnaissance planning considerations

2.14 To ensure effective coordination and collaboration among all staff elements, it is imperative that all elements gain an understanding of the OE, the assigned mission and the array of JISR capabilities that are available to the JFC commander.

2.15 JISR planning is collaborative and occurs simultaneously across all levels to synchronize missions and tasks. It is an integral part of the operations planning process and must be included at the onset of all planning activities. Ensuring the commander's access to the right set of JISR capabilities before, during and after mission execution is as vital as providing data, information, JISR results and intelligence during operations planning. Thus, it is essential to develop the necessary JISR strategies, plans, tasks and architecture required for mission execution during operations planning. Based on mission analysis, JISR planning requirements are part of the combined joint statement of requirements (CJSOR) and the force generation task list.[18] These requirements will feed directly into the operations plans, planning directives and detailed annexes. JISR key planning considerations include, but are not limited to:

- understanding the commander's direction and guidance;
- understanding JISR collection capabilities and availability;
- integrating ISR capabilities with operations;
- synchronizing collection activities to requirements;
- complying with the legal framework and national caveats on the use of ISR capabilities;
- establishing operations security measures and counter-intelligence; and
- defining the JISR architecture needed to efficiently execute JISR.

2.16 **Operational planning factors.** At the operational level, once strategic guidance is given, operational planning translates this guidance into specific component command activities and at achieving strategic and operational level objectives and attaining the desired end state. Broad strategic guidance needs to be translated into specific JISR roles, objectives, tasks and effects. Strategic guidance can include both specified and implied JISR tasks. Key operational planning factors may include:

- What do the commander's decision points necessitate for JISR employment?
- What are the commander's and component command's priorities?
- What are the information gaps?
- How to employ JISR collection assets and methods?

[18] The CJSOR is the document/tool that contains the (generic) force requirements of a commander for a specific operation. The CJSOR, including preliminary deployment information, must be developed in parallel with the operational CONOPS. For further information, refer to *Allied Joint Doctrine for the Planning of Operations* (AJP-5) and Allied Command Operations' *Comprehensive Operations Planning Directive* (COPD).

- What are the threats to JISR employment?
- What accesses does JISR have in the OE?
- What are the consequences if JISR assets are not employed?

2.17 **Collection capabilities.** JISR aims for the integration and harmonization of NATO and national collection assets at all levels. Collection capabilities include the platforms and sensors that gather the data and information necessary to complete the JISR process. Commanders need to understand that their requirements will likely exceed the availability of JISR assets. Consequently, there is a need to prioritize the requirements based on mission objectives to optimize the use of available capabilities. JISR capabilities and limitations, especially the time the information is of value, must be weighed against the mission objective at all times.

a. Collection strategies should identify the complementary strengths of various collection capabilities in order to minimize the impact of capability limitations and maximize the quality and quantity of JISR results. As a multidisciplinary approach, JISR allows sensors and capabilities to complement one another and collect against multiple targets within a single mission. On other occasions, it may be necessary for multiple JISR assets to be tasked against a single high-priority requirement to ensure that it is satisfied.

b. JISR collection capabilities and their supporting resources can be employed in all operational domains and environments, including the electromagnetic spectrum. JISR collection capabilities can include airborne, land-based, maritime and space-based collection and sensing capabilities as well as cyberspace collection capabilities. The composition of a JISR capability could include the following components:

- platform and crew;
- collection sensors and operating crew;
- command, control and communications equipment and personnel;
- mission-planning and tasking equipment and personnel; and
- logistics, training and maintenance support.

2.18 **Integrating JISR capabilities with operations.** JISR sensors that could be tasked should be in compliance with agreed NATO standards for technical interoperability. JISR system architecture personnel should work with sensor owners to identify the most efficient method of routing collected data to the most appropriate customer(s). JISR sensors also need to have the ability to be responsive to several command and control entities. In addition, these sensors need the ability to push JISR data to a range of tactical operators but also to both the operational-level headquarters (joint task force headquarters) and the strategic-level headquarters (SHAPE or NATO headquarters) echelons. Thus, JISR assets at the tactical command component level should be able to integrate at all levels so they are able to cover any collection requirement generated by any of them, if assigned.

2.19 **Synchronizing collection activities to requirements.** The JISR process starts with a validated CR. The process consists of a set of interrelated and interacting activities through which the CR is satisfied by a JISR capability. Within the task step, ISR management staff elements identify, coordinate, task and position JISR assets or resources against prioritized CRs. Factors such as the availability of JISR assets, platform and sensor capabilities, adversarial threats to JISR assets as well as timeliness of the JISR response are taken into consideration. Once the unprocessed (raw/unstructured) data and information is collected, it is then processed, exploited and disseminated. The PED part of the JISR process (TCPED) takes data or information collected by a sensor, processes it into a useable format, exploits it, and then disseminates a JISR result to the requester (Figure 2.1). JISR results, in turn, can support the intelligence cycle contributing to the production of fused and all-source intelligence as well as deliberate and crisis response planning processes and strategic awareness for decision-makers.

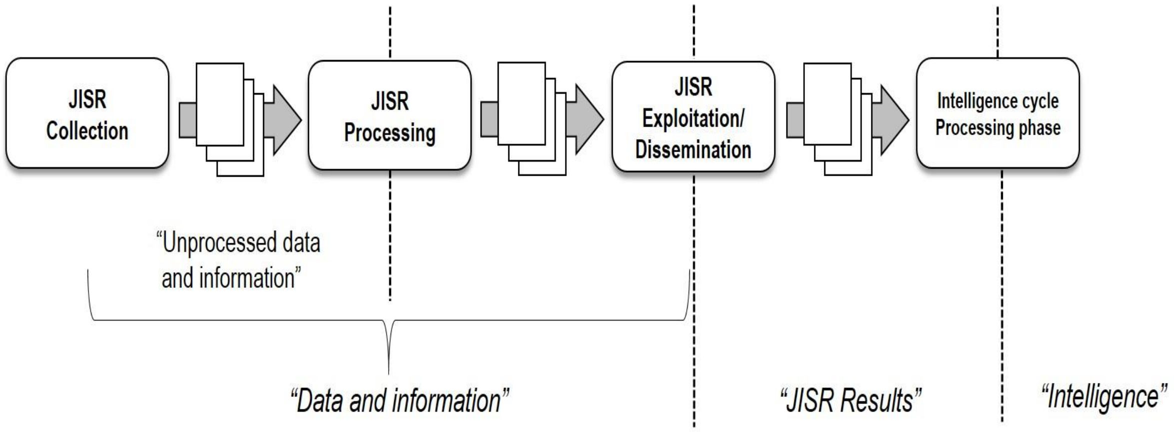
JISR Collection
JISR Processing
JISR Exploitation/ Dissemination
Intelligence cycle Processing phase
"Unprocessed data and information"
"Data and information"
"JISR Results"
"Intelligence"

Figure 2.1 – The conversion of collected data and information into intelligence

2.20 **Legal considerations on the use of JISR capabilities.** Commanders and staffs need to be aware of the constraints of international and national laws that may impact JISR planning activities. NATO forces and NATO-led forces operate in accordance with international law. All operations, which have a legal framework, will have operational limitations and authorizations regarding the employment of ISR capabilities. Legal limitations may be reflected in international law, national and

domestic law, the rules of engagement (ROE) agreements or arrangements with a host nation, or other legal and policy directives. Relevant ROE need to be established early in the planning process to provide political, legal and policy direction to commanders at all levels for the conduct of military operations.[19]

2.21 **Operations security measures.** NATO's adversaries will likely implement measures aimed at denying and defeating NATO JISR capabilities. Commanders should take into account during the planning process that NATO's JISR sources, methods, activities, and capabilities should be protected with effective operations security practices, information security measures, and robust counter-intelligence.

2.22 **JISR architecture.** A JISR architecture consists of the systems, tools, and information technology connecting taskers, controllers, collectors, exploiters, analysts, databases, applications and requesters of data, information and results as well as operational data in a joint environment. This architecture facilitates the management of JISR results at the appropriate classification, enables the JISR process including collection management functions and sub-functions and supports the harmonization of intelligence and operations functions at all levels. The JISR architecture is an essential part of the overall operational architecture and operational design. The JISR architecture must be integrated with command and control, intelligence and operational capabilities and comply with host nation, national and international law as applicable.

[19] Rules of engagement (ROE) are authorized by the North Atlantic Council (NAC) for NATO/NATO-led operations on approval of the OPLAN.

Chapter 3 – Joint intelligence, surveillance and reconnaissance process

Section 1 – Introduction

3.1 The joint intelligence, surveillance and reconnaissance (JISR) process is a coordination mechanism through which intelligence collection disciplines, other collection capabilities and exploitation activities provide data and information to address a collection requirement in a deliberate, ad hoc, or dynamic timeframe in support of operations planning and execution. The JISR process consists of staff management functions and staff management activities conducted at all levels of operations and throughout the whole conflict spectrum.

3.2 **Key functions within the JISR process**. The key function within the JISR process is collection management (CM) consisting of collection requirements management (CRM) and collection operations management (COM). The CRM and COM sub-functions play key roles in handling requests for information within the JISR workflow. While intelligence requirements management and collection management (IRM&CM) is a core function within the intelligence cycle, it also influences and informs the JISR process and workflow. The basic workflow including the key functions, activities, organizational elements, decision points and products for deliberate JISR tasking is shown in Figure 3.1.

3.3 **JISR process and workflow**. CM is initiated upon receipt of a validated intelligence requirement from the intelligence requirements management staff. The CM staff translates the validated intelligence requirement into a collection requirement (CR). CRs are then consolidated to form a collection requirements list (CRL) and resourced on a priority basis with the resourced proportion of the CRLs being taken forward as collection tasks (CTs) and populating the collection tasks list (CTL).[20] An additional entry point into the JISR workflow are intelligence surveillance, reconnaissance requests (ISRRs). An ISRR can also be added to the CTL.[21] The individual CTs are then sent to COM elements for execution. JISR results are disseminated to the requester. Feedback on COM activities are provided to CRM, to ensure comprehensive measures of performance (MOPs) and measures of effectiveness (MOEs) can be completed to inform future planning activities.

3.4 **Transitioning from requirements to JISR tasks.** A key aspect of the JISR process and workflow is the transition from the requirements stage to JISR tasking. Through mission integration, JISR tasking includes converting JISR tasks into orders and passing these orders to the appropriate JISR assets. Each order should contain direction and guidance for processing, exploitation, and dissemination of the collected data and information to enable the successful accomplishment of the mission.

[20] CTL is a list of prioritized JISR collection and PED requirements, developed from the CRL, which are allocated to JISR capabilities.

[21] An intelligence surveillance, reconnaissance request (ISRR) is 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.

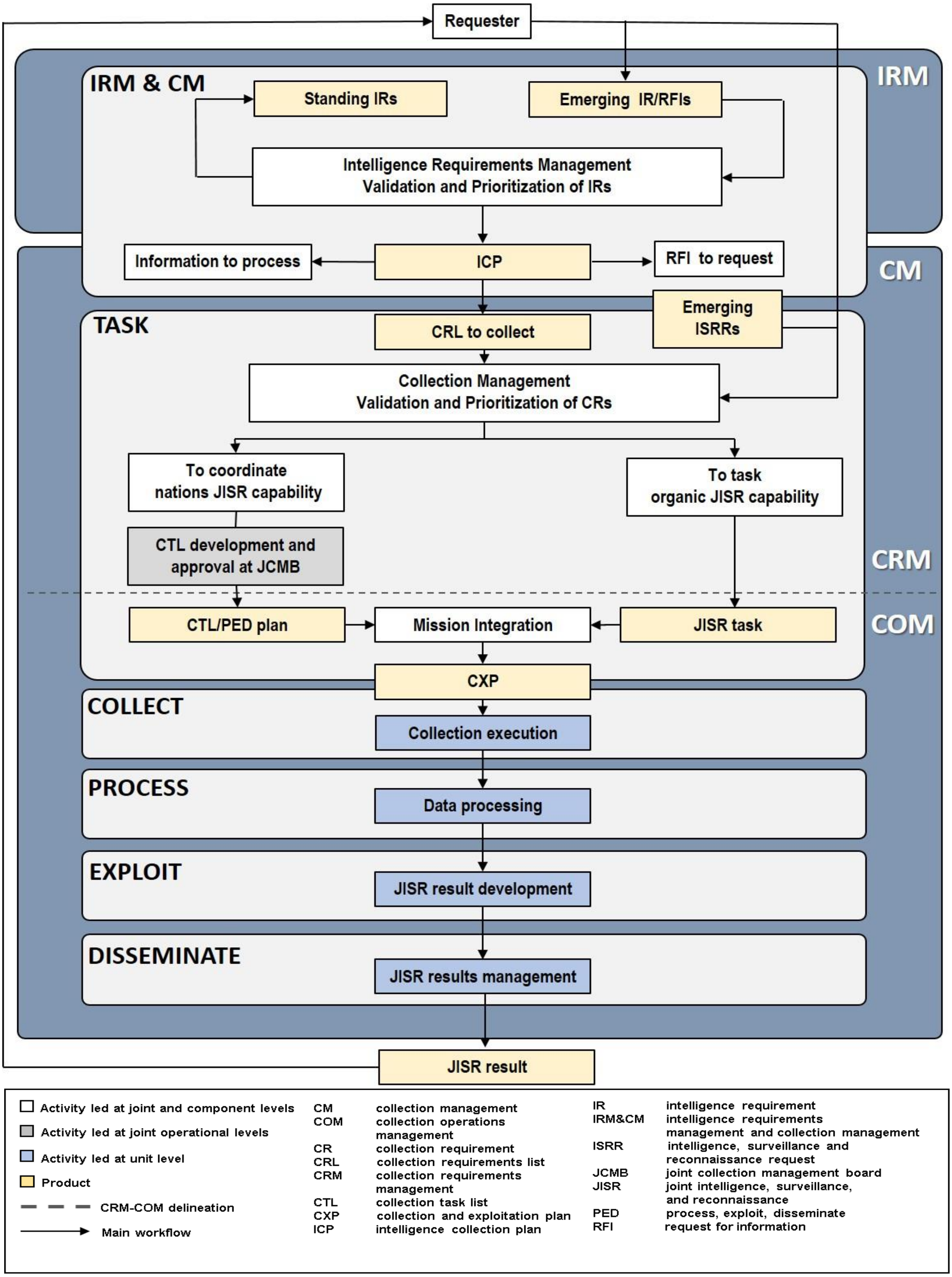
Requester
IRM
IRM & CM
Standing IRs
Emerging IR/RFIs
Intelligence Requirements Management
Validation and Prioritization of IRs
CM
Information to process
ICP
RFI to request
TASK
CRL to collect
Emerging ISRRs
Collection Management
Validation and Prioritization of CRs
To coordinate nations JISR capability
To task organic JISR capability
CTL development and approval at JCMB
CRM
COM
CTL/PED plan
Mission Integration
JISR task
CXP
COLLECT
Collection execution
PROCESS
Data processing
EXPLOIT
JISR result development
DISSEMINATE
JISR results management
JISR result
□ Activity led at joint and component levels
▨ Activity led at joint operational levels
🟦 Activity led at unit level
🟨 Product
CRM-COM delineation
Main workflow
CM collection management
COM collection operations management
CR collection requirement
CRL collection requirements list
CRM collection requirements management
CTL collection task list
CXP collection and exploitation plan
ICP intelligence collection plan
IR intelligence requirement
IRM&CM intelligence requirements management and collection management
ISRR intelligence, surveillance and reconnaissance request
JCMB joint collection management board
JISR joint intelligence, surveillance, and reconnaissance
PED process, exploit, disseminate
RFI request for information

Figure 3.1 – JISR process, activities and workflow

Section 2 – Task, collect, process, exploit and disseminate

3.5 The JISR process consists of five steps: task, collect, process, exploit and disseminate (TCPED). The execution of the TCPED construct normally relies on a federated and collective effort from all levels, across components, and may be supported by national and/or out-of-theatre capabilities. Multiple TCPED cycles occur at different stages simultaneously, as operations, intelligence production, and theatre information pertaining to the operating environment evolves.

Task

3.6 The task step is initiated with the clear articulation of CRs and/or CTs and consists of developing collection, exploitation and dissemination guidance, directives or orders to coordinate and control JISR activities and assets. JISR tasking should be coordinated among all levels of command to enable mutual support between services/component commands and to make the most efficient use of available collection and exploitation capabilities. JISR tasking encompasses deliberate planning aspects and standing CRs, as well as ad hoc or dynamic tasking in response to emerging CRs. JISR tasking is planned through CRM, and its outputs are executed through COM.

3.7 When articulating and submitting intelligence requirements, CRs or intelligence, surveillance and reconnaissance requests, requesters should consider the following:

a. **Support to operations.** Describe how the required information supports current or future operations and the impact if the information is not obtained. This assists the CRM function when it is received with the validation and prioritization of the requirement. CRs should request a JISR result that is needed and not specify a particular collection asset.

b. **Classification.** Identify the desired level of classification for the results. This potentially impacts not only the collection and the dissemination of the result but also the contents, the level of details and accuracy of the result.

c. **Releasability.** Identify nations, groups of nations and entities concerned and/or allowed to obtain the information.

d. **Time.** Specify the time when the result is required.

e. **Type of result and format.** Describe the type and the format of the result when applicable, and the preferred means of dissemination.

f. **Periodicity.** Identify and formulate how often the collection and exploitation is to occur.

g. **Communications.** Include accurate contact information to ensure IRM&CM elements can maintain contact with the requester when the JISR asset or capability is tasked and throughout the JISR process.

3.8 **Assigning a JISR task to a JISR asset.** Because of limited availability of JISR assets, tasking should only occur when the requested information or effects are not being generated from existing activity or where there is a need to continually update or check baselines against data/information already held. In addition to tasking NATO-owned JISR assets, the feasibility of using non-dedicated JISR assets, as well as requesting nation-owned assets, should be considered, so that all available capabilities are efficiently employed to support the commander's intelligence and operational requirements. When assigning a JISR task to an appropriate JISR asset to meet a CR, the CM element should consider the following:

a**. Suitability.** Assets that are tasked to support JISR activities must be capable of completing the task and disseminating the results in the requested manner. There will be occasions when more than one asset is capable of carrying out a JISR task. Careful consideration must be given to the attributes of competing assets to ensure that the most appropriate mix of assets is selected. One key attribute for consideration is the ability of the JISR asset to meet timing factors associated with the requirement. JISR timing considerations could be associated for example with flight profiles, ground reconnaissance missions, maritime mission profiles, information download capacity/capabilities or other key factors.

b. **Risk.** JISR asset capabilities must be adequately protected whilst still being able to gather the required information. Failure to protect such capabilities may result in the loss or compromise of the asset. There will often be an element of political and/or military risk involved in the employment of a particular asset. Any such risk must be weighed against the value of the information sought.

c**. Operating environment.** The nature of the operating environment to include all relevant geospatial, political, military, economic, socio-cultural, infrastructural and informational aspects must be taken into consideration.

d**. Corroboration.** Where required, reasonable or useful, JISR capabilities should be synchronized, fused, massed and layered to collect against the same CR. The effective management and employment of independent JISR assets or capabilities within a specific time frame and area provides multiple JISR results to intelligence analysts for confirmation. The employment of multiple assets also increases the level of confidence in the results and helps guard against deception. To this end, the designation of a JISR mission commander may be necessary.[22] The role of the JISR mission commander is to ensure coordinated data collection when several assets are needed to respond to the same CR or to provide intelligence, surveillance and reconnaissance (ISR) support to a given operation, in a specific area and for a given time slot.

[22] A JISR mission commander is also known as "sensor warden" or "ISR coordinator."

3.9 **JISR asset tasking.** In an increasingly complex and dynamic environment, JISR tasking will not only require deliberate, planned activity but will also be required to support ad hoc and dynamic requests (Figure 3.2). Support of an ongoing operation may require immediate changes to already issued tasking orders or rapid reallocation of a JISR asset that is already collecting to support an evolving tactical situation. The reassignment of collection assets requires careful consideration.

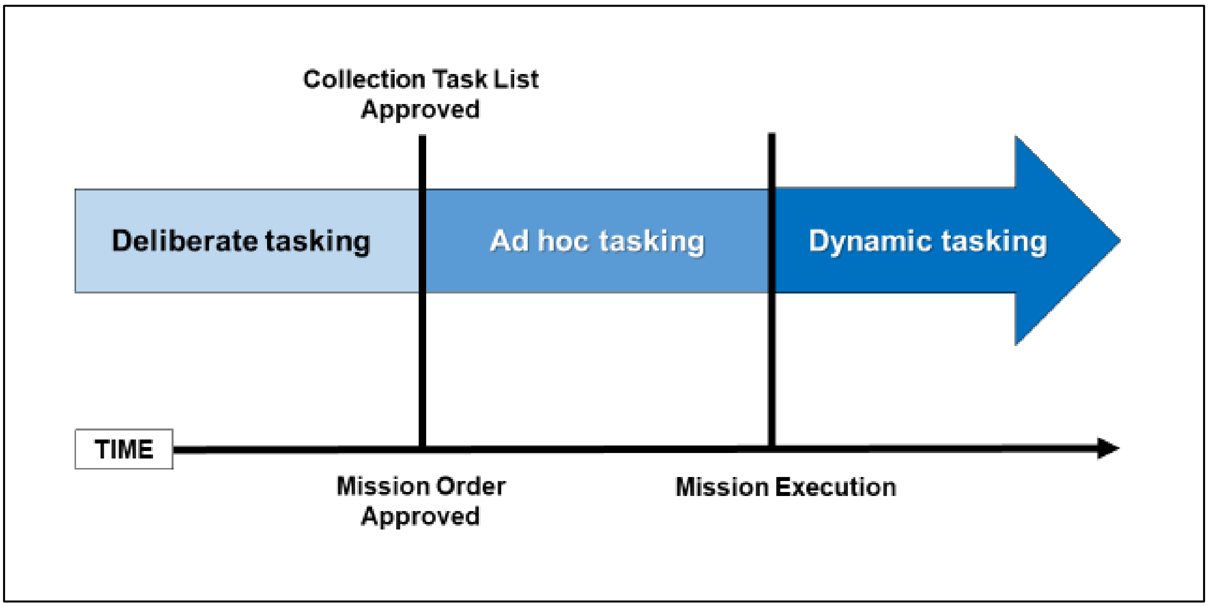

Figure 3.2 – JISR asset tasking relative to mission execution

3.10 Deliberate JISR tasking is the typical mechanism to develop, coordinate and assign JISR tasks to JISR assets. Deliberate tasking guarantees sufficient time for mission integration, mission planning, mission tasking and mission preparation. Ad hoc tasking is the process for integrating emerging and urgent CRs in an already released CTL and prior to mission execution. Dynamic tasking allows for the integration of emerging CRs requiring immediate satisfaction into current collection operations.

a. **Deliberate tasking of JISR assets.** Deliberate JISR tasking can be accomplished directly for dedicated JISR assets. It also occurs when there is sufficient lead-time for CRs to be incorporated into a CRL and finally into a CTL which is approved at the joint collection management board (JCMB). Within the deliberate JISR tasking process, there is sufficient time for the theatre collection manager (TCM) to issue JISR tasks from the approved CTL and for mission tasking to JISR assets and when nations provide tactical command of JISR assets to the commander.[23] This occurs when the development of CRs and JISR tasks are synchronized with other relevant staff rhythms and integrated for mission tasking. Deliberate tasking activities include:

[23] Tactical command (TACOM) is the authority delegated to commanders to assign tasks to forces under their command for the accomplishment of the mission assigned by higher authority.

(1) **Validating the CR.** If the information/intelligence is not available to answer an intelligence requirement, a CR can be developed. The CM element would then review the unvalidated CR and create a validated CR.

(2) **Developing the CRL.** With the decision to collect, the CM element, with CRM authority, determines whether dedicated JISR assets at the considered level of command can fulfil the CRs. If CRs cannot be satisfied by available organic ISR assets, the CM element must request collection support from higher and/or adjacent commands and organizations. In the event JISR assets are available at the considered level of command, JISR tasks are developed and integrated directly into mission planning for collection mission tasking. For CRs requiring operational level management, CRs are consolidated and prioritized into a draft CTL with synchronized collection tasking which is discussed at the JCMB. The CRL development occurs at all levels. The assets available for collection tasking are those that are under the tactical command of a specific level. If collection managers do not have a suitable asset at their level, they will add it to the CRL for the consideration of the JCMB at the level above.

(3) **Developing the CTL.** The CTL, developed by the CRM staff element, is discussed and endorsed by a joint collection management working group (JCMWG) for presentation and ratification at the JCMB.[24] The CTL serves as the authoritative CM tasking document for a commander, theatre or formation and is consistent with the joint forces commander's overall mission priorities and the theatre collection priorities. As part of the CTL development, CRM elements from the operational and service/component levels identify the appropriate JISR asset(s) likely to satisfy the CR. After coordination, the CRM element assigns the CR and the related JISR task to a servicing component command. Furthermore, the CTL provides a list of approved and prioritized JISR CRs, JISR tasks and, as required, dynamic re-tasking priorities. The CTL aligns the CRs or operational lines of effort with the specific capabilities/assets that may be used to collect against.

(4) **Role of the JCMB.** To facilitate the coordination of JISR activities between the different service components and the intelligence and operations staffs, a JCMB is established for this purpose and consists of the respective intelligence and operations staff members as well as liaison officers from higher and adjacent echelons and subject matter experts. The TCM, as lead of the JCMB, ratifies and endorses the CTL, which is produced by the CRM staff and developed in a JCMWG. The CTL serves to resolve potential areas of conflict, assign execution

[24] To ensure continuous coordination in developing the CTL, the JCMB may establish a JCMWG to support the preparation, approval process and distribution of the CTL.

responsibilities, de-conflict, and synchronize collection activities.[25] The TCM issues priority guidance across the service components to ensure that the overall JISR effort is coordinated, prioritized, appropriately balanced, and focused on the commander's objectives. The CTL may be published and disseminated on a daily basis in accordance with the operation and/or exercise battle rhythm.

(5) **Coordinating with the operations staff for mission integration.** COM sends the task to the unit who will be conducting the collection based on validated and prioritized CTs. JISR tasks are coordinated with the operations staff for mission integration, the issuance of orders to the JISR asset for execution of the collection mission and to ensure the collected data or information will be processed, exploited and disseminated. To accomplish this part of the process, the CM element needs to develop a good working relationship with the intelligence requirements management staff to clearly understand the requirement to avoid any negative or delaying impacts on execution. Requirements from both the intelligence and operations functions should be capability and discipline agnostic, and request an ISR effect. The CM staff will determine the appropriate method of collection to meet the requirement. For example, if imagery intelligence collection is the appropriate JISR capability to answer the requirement, the CR must be tailored for imagery collection. Likewise, signals intelligence CRs must be tailored for the appropriate sensors. Additional information may be required from the requester in order to develop the CR to optimize collection and maximize the chances of a successful first-time collect.

(6) **Maintaining visibility on component CRs.** The TCM, or others holding collection management authority at other levels of commands, requires visibility on all validated CRs generated by subordinate formations and units, to at least two levels below. Although subordinate formations and units may be able to fulfil their own requirements with their dedicated JISR assets, they must forward their declared CRs up the chain of command so that the higher headquarters can coordinate and optimize the use of all available JISR assets and ensure that any unintentionally redundant collection requirements are de-conflicted. CM elements at the component level are responsible for submitting their coordinated and prioritized CRs to the operational level CM. To this end, a coordination process and a CM board should be established at each subordinated command level to develop a CRL based on their CRs.

(7) **Developing the processing, exploitation and dissemination plan.** The CM element also develops synchronized planning for the processing, exploitation and dissemination (PED) of the collected data or information. The PED plan provides details of the tasks to be assigned to dedicated and subordinate JISR exploitation units to meet the CRs.

[25] For additional information on the JCMB refer to Allied Intelligence Publication*, Intelligence Requirements Management & Collection Management (IRM&CM),* (AIntP-16).

The plan must include details indicating where and how JISR results are to be conveyed to the requester, including any release caveats. Contact information for the requester and probable JISR collection and exploitation units are also included in the plan. This plan should specify how JISR assets and capabilities amongst the coalition are best utilized where collected JISR data or information from one JISR asset and capability can be appropriately exploited using the PED resources from another JISR asset and capability either NATO-owned or nation-owned.

(8) **Integrating JISR tasks within mission planning.** COM starts with the issue of a validated CTL to COM components, formations and units. The operations staff integrates the JISR tasks within mission planning taking into consideration other tactical activities, such as air, ground, maritime or electromagnetic spectrum operations and cyber battlespace management, as well as force protection aspects associated with the execution details of the JISR task. This encompasses mission planning at the service component level, leading to the preparation of the mission at the unit level. The key responsibilities within COM function are to manage the operation of JISR assets

(9) **Coordinating with the requester.** Coordination between collectors and PED units and the requester should be accomplished via the IRM&CM staffs to maintain centralized control. It is important for IRM&CM staffs to inform the requester that the ability to deliver the JISR result is dependent on the time needed to process, exploit and disseminate the result.

(10) **Reallocating JISR assets.** The COM element maintains situational awareness (SA) on JISR missions being conducted and dynamically responds to changing situations that may necessitate reallocating JISR assets against tasking priorities.

(11) **Assessing JISR activities.** The CM staff need to assess to what extent JISR assets have satisfied the CRs so that assets are continuously used in the most efficient way, and the probability of actionable information reaching decision-makers is maximized. This assessment is accomplished through a combination of measures of performance (MOPs) and measures of effectiveness (MOEs) providing sufficient feedback for follow-on actions (e.g., completion and close, delay to another time, change of periodicity, change of location, relocation to another asset or cancellation due to inability to effectively satisfy the CR).[26] Effective MOEs are critically dependent on the assessor's understanding of the operational environment. The intelligence function is therefore a key enabler for MOEs, which can be a labour-intensive endeavor. Lessons from assessments can be used to

[26] Refer to Allied Intelligence Publication, *Intelligence Processing*, (AIntP-18), for information on assessing and evaluating the relevancy and quality of JISR results.

improve JISR support to operations in the future.[27] If formal feedback is unavailable, informal feedback via chat, voice communication and the JCMB can be just as useful. CM staff track the status of ongoing and JISR collection operations and results. All-source intelligence analysts are best positioned to evaluate the quality and relevance of the JISR results. Therefore, these two functions must work in parallel.

(12) **Coordinating JISR operations within theatre.** In deployed NATO missions, JISR activities conducted by the different service components are coordinated at the theatre or joint force level.

b. **Ad hoc and dynamic tasking of JISR assets.** Requesters submit ad hoc and dynamic requests for tasking after the deliberate tasking process has occurred in an emerging or changing situation and when the CTL is already produced and endorsed in the JCMB. The ad hoc and dynamic types of requests are validated and processed by the CM element, given a higher priority, and categorized as either ad hoc or dynamic taskings. For ad hoc JISR tasking, this procedure is accomplished while the operation is being planned, but has not yet been executed. For dynamic JISR tasking, this procedure is accomplished during mission execution, but with sufficient time to be integrated into the mission as an additional task or if the dynamic task is a higher priority to supplant existing planned collection.

(1) **Ad hoc tasking of JISR assets.** Ad hoc JISR asset tasking occurs after the release of the endorsed CTL when urgent CRs emerge and there is still time to adjust an already issued order prior to scheduled execution. CM staff must quickly validate and prioritize ad hoc requirements to determine which original task can be cancelled or modified with the least negative effect and then determine how to satisfy the affected requirements at a later stage. If an original JISR task cannot be cancelled or modified, a new CT requiring additional time may need to be created. As changes are made to deliberate and planned tasking, the original requesters must be notified of any modifications or cancellations due to ad hoc priorities. In addition, modifications to deliberate and planned tasking will result in the re-prioritization of federated PED resources. The ad hoc tasking process is to be managed by the CM element holding CRM authority as they will have a greater perspective on the wider impact to the CTL and the most efficient way to collect the information. However, if timeliness is an issue, it is likely that the CM element holding COM authority will process the ad hoc tasking with the awareness that their available assets might not be the most efficient means of collection.

[27] Refer to Bi-Strategic Command (BI-SC) Directive 080-006 Lessons Learned, 23 February 2018, which is relevant to the Joint Intelligence, Surveillance and Reconnaissance.

(2) **Dynamic tasking of JISR assets.**[28] Dynamic JISR asset tasking occurs when the importance and urgency of an emerging CR demands immediate attention and redirection of an already collecting JISR asset.[29] The requester will communicate the requirement to the appropriate CRM staff element for retasking purposes. COM must be alerted in a short notice normally via the ISRR format. The COM element will, in turn, synchronize and integrate the requirement with current operations. The senior intelligence duty officer or equivalent within the ISR operations staff will then make a decision based on agreed operational priorities, environmental and tactical conditions and the availability of capabilities versus the urgency of the task. Should this situation require a decision to be made on the loss of collection occurring against other critical requirements, rapid liaison is required with the CM element to make an informed intelligence gain/loss assessment and inform the potential reattribution of a capability. As with ad hoc tasking, dynamic JISR tasking will also result in the re-prioritization of federated PED resources.

Collect

3.11 The second step in the JISR process consists of the actual gathering of data and information by JISR capabilities and assets. Collection encompasses the detailed scheduling of JISR tasks to available JISR assets and the execution of those tasks by JISR capabilities. JISR assets collect the requested data and information and make it available for further processing. The CM element needs to consider all JISR capabilities to satisfy a valid CR.

3.12 **JISR capabilities.** JISR capabilities provide timely information and intelligence that contribute to a commander's SA and understanding of the operating environment. JISR capabilities can consist of both dedicated and non-dedicated capabilities.

a. **Dedicated JISR capabilities.** Commanders require the right mix of capabilities and assets to respond effectively to changing situations. Because JISR assets have specific and unique capabilities with no single asset able to cover all CRs, commanders and staffs require a realistic appraisal of JISR collection and PED capabilities, and in particular an awareness of their limitations. A JISR capability may be manned or unmanned, operate in air, space and cyberspace, or function on the ground and at or below sea-level. Depending on the threat, each capability can have distinct operational advantages and disadvantages

[28] Types of missions and situations that may require dynamic re-tasking include threat warning, combat search and rescue, personnel recovery, dynamic targeting, dynamic collection, dynamic cross-cues, weather, platform or sensor maintenance issues, troops in contact (TIC), compressed or extended collection time lines, or PED node challenges.

[29] Non-Interference based (NIB) tasking is a method of satisfying a dynamic task without having to seek TCM approval to change an asset's mission or positioning.

when collecting data and information for JISR processing. Some capabilities can easily be re-tasked within the JISR process while others are limited by operational constraints and the sensor technologies they possess. Either way, the JISR process provides the mechanism for executing and maximizing operational use of JISR capabilities in order to meet and satisfy the commander's critical information requirements.

b**.** **Non-dedicated JISR capabilities.** For any operation, there will be a finite number of dedicated JISR capabilities, but there are many more potential ISR capabilities that can be leveraged to gather data and information about the operating environment and fulfill requirements. Although their primary role is not ISR-related, they are capable of collecting and disseminating data and information and producing a result. Commanders and staffs need to consider asset availability in the early stages of planning operations. Many activities that are performed by military units are not considered as part of the JISR process. However, while performing their activities, they have the means to gather information about the operating environment that can serve the same purpose as a dedicated JISR capability (e.g., an aircraft on another tasking or in transit). Implementing a non-dedicated JISR collection capability programme requires close alignment and coordination between the CM element and other operational planners within a component headquarters or joint headquarters.

b. **Non-dedicated ISR capabilities and the JISR process.** Tasking and integrating non-dedicated ISR capabilities into the JISR process requires careful deconfliction against their primary missions. Non-dedicated JISR capabilities may be used in an ad hoc manner augmenting dedicated JISR assets to satisfy intelligence requirements. However, commanders and staffs need to consider the optimal means to process, exploit, and disseminate the collected data by non-dedicated JISR capabilities to effectively integrate their results within the JISR process.

Process

3.13 The third step in the JISR process is the conversion of collected data and information into appropriate, readable and useable formats that enable further exploitation, storage or dissemination. Advances in technology continue to change the way data and information can be processed. Some JISR assets have a near real-time (NRT) data processing capability that can rapidly convert collected data into exploitable results. Multi-source ISR platforms with the exploitation elements associated with the JISR asset can provide early fused intelligence derived from its own collected multi-source intelligence data and information. In other instances, the conversion of the collected data is accomplished manually or is computer-assisted. It is important to align processing capacity and timing factors based on the volume of collected data, information and the time frame specified to meet the requirement. When collected data and information exceed a command's internal capacity to process, contingencies should be in place to share collected data and information with external processing capabilities.

Exploit

3.14 Within this step of the JISR process, processed data is exploited to derive a JISR result. The time required to conduct exploitation activities will vary depending on the characteristics of the collection assets. Some JISR assets accomplish processing and exploitation automatically and nearly simultaneously at the time of the collection, while the data and information derived from other collection assets, conversely, may require a more substantial amount of time and various levels of exploitation. Exploitation is performed by skilled personnel to evaluate and interpret the collected data or information and provide a useful product to answer a requirement.

3.15 Different levels of exploitation exist for each JISR capability or asset. The levels range from a rapid and preliminary assessment of collected JISR data or information up to a more time-consuming and in-depth assessment via reachback capabilities. The different levels of exploitation are dependent on the specifications and characteristics of the JISR asset or capability and its supporting organization and personnel (e.g., physical proximity to the sensor, in-theatre or in reachback locations).

a. **Initial level of exploitation.** The initial level of exploitation is the rapid and preliminary assessment of collected JISR data or information. If the collection cannot satisfy the CR, the CR should be resubmitted for further collection. If the collection satisfies the CR, the exploiter forwards the results immediately to the commander and/or requester, often in NRT, in support of current operations. This type of exploitation is usually conducted by the sensor operator or exploiter associated with the sensor system or collection capability, but can also be undertaken by other exploiters having NRT access to collected sensor data. The JISR results are then transmitted for further exploitation within the JISR process and the intelligence cycle.

b. **Intermediate level of exploitation.** Further exploitation within the JISR process involves a more detailed evaluation of collected data and information in accordance with exploitation tasking that support commanders and staffs during current operations or intelligence production. Capabilities are typically provided by the exploitation elements associated with the JISR assets or capability, but these capabilities may also be located at a reachback exploitation facility. The result can be sent directly to the commander and/or the requester, disseminated to the intelligence community for further processing, or forwarded to the next level of exploitation.

c. **Advanced level of exploitation.** A more in-depth assessment involves using data and information from multiple JISR assets inside a specific intelligence collection discipline or JISR capability and combined with archived information. This level of exploitation often requires tools, processing power, and/or additional specific subject matter expertise. It can be time-consuming and may be conducted in the joint operations area or via reachback capabilities.

Disseminate

3.16 The dissemination step within the JISR process involves the timely provision of JISR results to those who need it, in the requested format, and through the communication means specified by the JISR task. Dissemination, which does not involve a processing step, may involve sending raw data to a requester. Effective dissemination management is needed to ensure requesters have access to the disseminated JISR results that are posted, published, or transmitted to facilitate effective integration and synchronization. In addition to providing an answer to a specific request, JISR results should be systematically shared to support intelligence development and to improve overall SA and understanding of commanders and staffs. Dissemination is to be executed in accordance with classification and releasability guidance and procedures. Subsequent feedback allows elements to amend collection plans to conduct more efficient and relevant collection operations.

Section 3 – Joint intelligence, surveillance and reconnaissance results

3.17 A JISR result is the outcome of the JISR process disseminated to the requester in the requested format. The JISR result usually consists of the data and information that has been exploited by specialists and provides commanders and their staff with specific data and information to address an intelligence requirement. A JISR result can also be information that has been initially processed and identified for immediate forwarding to a specific requester who urgently requires it. JISR results can also contribute to all-source intelligence analysis, used to populate intelligence, operations, targeting and electromagnetic warfare databases, or feed directly into dynamic-battlespace-awareness tools such as a common operating picture. JISR results can consist of various forms including, but are not limited to, real-time or NRT data links directly from a collection platform to requesters; broadcast transmissions from a collection platform to multiple agencies or standard intelligence reporting procedures. JISR results also contribute to all-source analysis (Figure 3.3).

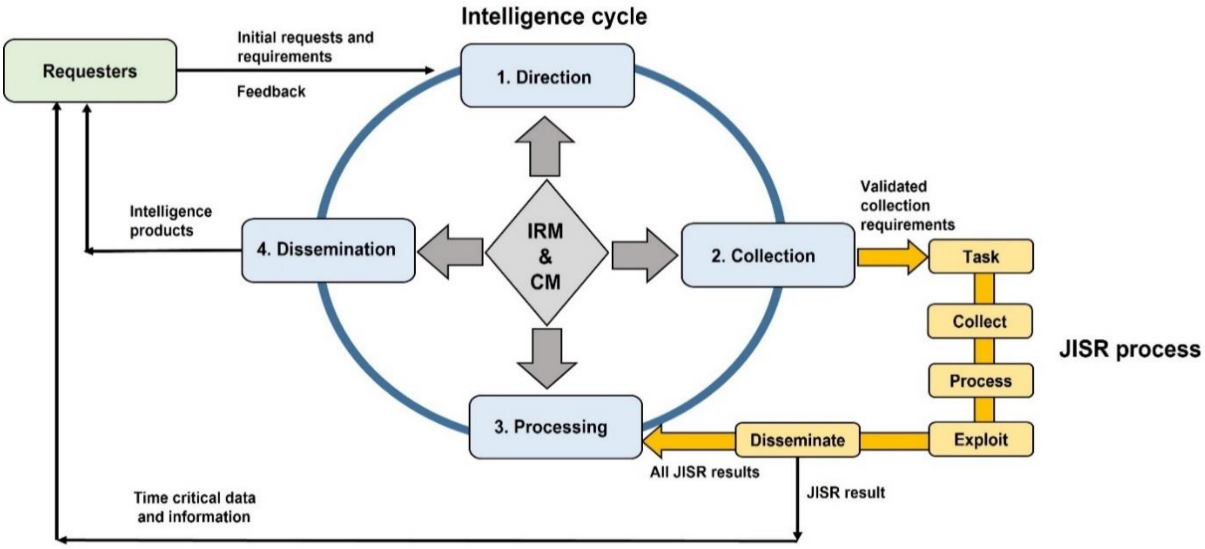

Figure 3.3 – Dissemination of JISR results

3.18 JISR results can be categorized as either a pre-exploited result or an exploited result.

a. **Pre-exploited results.** Pre-exploited results are JISR results that have been provided directly from the sensor without comment or analysis.

b. **Exploited results.** Exploited results are JISR results that have been derived from exploited JISR data and information. Depending on the level of exploitation, the result will consist of information or intelligence. For a supported commander, the exploited results contribute to all-source intelligence analysis during the processing stage of the intelligence cycle.[30]

3.19 JISR reporting can be verbal, textual, or visual and can be transmitted physically or electronically. Standard formats for reporting JISR results include:

a. **Verbal reports.** Personnel verbally communicate what they have seen through visual observation, by screening imagery, or through the exploitation of collected and processed data.

b. **Textual reports.** Personnel prepare written reports that are normally structured or formatted in accordance with NATO reporting standards and formats. Using pre-determined formats and templates enables users to quickly extract only the information requested or required.

c**. Visual reports.** Typically transmitted together with textual reports, visual reports may be automatically produced by the sensor, by supporting computer systems, or by personnel.

(1) **Data-linked or networked NRT data.** Some JISR assets can continuously distribute data via data-links or networks that automatically update linked systems and databases. When JISR systems are unable to pass pre-exploited data, imagery and information, tactical data link messages may be used as a surrogate, providing location, direction, speed and identification for other systems within the network.

(2) **Data analytics.** Data analytical techniques and algorithms help to discover and derive information from collected raw data and may be able to automatically generate JISR results.

3.20 **JISR results and all-source intelligence.** Given the nature of difficult and complex environments, JISR results alone cannot provide the information needed by commanders. JISR results fused with all available data and information from other sources is the best way to provide commanders with sufficient understanding of the operating environment to make informed decisions. Single-source information and single discipline results derived from a specific intelligence discipline may answer

[30] For more information on how JISR results are processed within the intelligence cycle see Allied Intelligence Publication, *Intelligence Processing*, (AIntP-18).

individual and limited requirements (often without any confirmation), but cannot replace all-source intelligence to satisfy the requirement.[31]

Section 4 – Joint intelligence, surveillance and reconnaissance assessment and feedback

3.21 To assess and optimize the JISR process, the CM element implements mechanisms to provide management staff elements the means to systematically monitor the various JISR activities and receive requester feedback on requirements satisfaction once the JISR result has been delivered. Timely assessments and feedback enable JISR personnel to validate or consider ways to improve and adjust the JISR architecture, process, and operations. Timely assessments and feedback should be available on a continuous basis enabling commanders and staffs to address the effectiveness of JISR capabilities in support of operations and missions.

3.22 Assessment measures are the metrics by which performance, efficiency and effectiveness are measured. MOPs and MOEs taken together help decision makers determine whether progress is being made in meeting intelligence requirements.

a. MOPs are used to measure task accomplishment by evaluating if the JISR activities meet a measurable standard.

b. MOEs are used to measure in which degree the JISR results meet the Information/intelligence requirement While MOEs involve a component of subjective evaluation based on objective data, they should be based on observable and measurable indicators. Indicators provide the evidence that a certain condition exists or certain results have or have not been attained.

3.23 Criteria to assess JISR activities and capabilities could include the following questions.

- How well are the collection requirements met?
- How did the mission contribute to answering the intelligence requirement?
- Do the collection requirements need to be adjusted for the next mission? If so, how?
- Should a different JISR capability be considered to satisfy the intelligence requirement? If yes, which one(s)?
- If a collection requirement was partially met, what is required for the collection requirement to be fully met?

[31] All-source intelligence is the deliberate application of two or more intelligence collection disciplines (e.g., human Intelligence and signals Intelligence) or other JISR capabilities seeking to improve the quality of the intelligence product.

- In case of redundant tasking of different JISR capabilities, was the right mix of JISR capabilities tasked to satisfy the intelligence requirement? Was confirmation achieved through the employment of different independent JISR capabilities? If not, what changes are required?

- Did command and control of the JISR activity contribute to satisfying the intelligence requirement? If not, why not?

- Were there other JISR capabilities, which could have been used redundantly for confirmation? If yes, which capabilities?

Chapter 4 – Joint intelligence, surveillance and reconnaissance architecture considerations

Section 1 – Introduction

4.1 The intelligence staff and the operations staff must continuously collaborate to ensure the integration and synchronization of joint intelligence, surveillance and reconnaissance (JISR) into the overall joint operation. However, JISR must be considered more than just a coordinated staff process performed by intelligence and operations staffs. For JISR to be most effective, all staff elements to include: logistics (J4), plans (J5), communications (J6) and the civil-military cooperation (J9) need to be part of the JISR planning process. Having the right capabilities and number of assets coupled with a comprehensive JISR architecture will provide the commander with the agility to respond to a constantly evolving environment.

4.2 A JISR architecture consists of the systems, tools, and information technology connecting taskers, controllers, collectors, exploiters, analysts, databases, applications, and requesters of data, information and results as well as operational data in a joint environment. This architecture enables the harmonization of intelligence and operation functions at all levels and is an essential part of the overall operational architecture and operational design. To that end, the JISR architecture must be integrated with command and control, intelligence and operational capabilities. The quantity and variety of collection capabilities and process, exploit, disseminate (PED) capacities are essential to ensure pervasive and persistent JISR coverage necessary to collect and disseminate required information. In general, having the right mix and numbers of JISR capabilities provides the operational commander with the ability to respond effectively to many different and changing situations.[32]

Section 2 – Interoperability and integration

4.3 **Interoperability.** Network-enabled JISR capabilities are needed to share multi-sensor JISR collection data and multi-intelligence analytical products, support streaming services and enable JISR mission management across operational and intelligence networks. The network must support the exchange of information among the Nations and organizations within the NATO command structure, including both NATO and non-NATO mission partners.

4.4 The architecture must enable interoperability among NATO and national intelligence, surveillance and reconnaissance (ISR) capabilities and support federated processing, exploitation and dissemination activities. The network must support all activities and the task, collect, process, exploit, disseminate (TCPED) steps associated with the JISR process. The NATO architecture is founded upon coalition shared data servers, which provide the ability to store, discover and retrieve exploitable data, imagery, analytical products, streaming services and ISR workflows,

[32] Refer to NATO's *Joint Intelligence, Surveillance, and Reconnaissance Operational Design.*

enabling all TCPED activities. The network must be flexible enough to accommodate national capabilities that are compliant with the STANAG 4559 architecture and accommodate nations that are not compliant with this STANAG.[33] The network must also facilitate the use of web-enabled services for the workflow taskings. ISR networking includes the need for operational networks (mission networks or federated mission networking) and intelligence networks (e.g., battlefield information, collection and exploitation system) to enable interoperability.

a. The JISR architecture needs to be designed to reflect communication networks and services available which have a particular focus on security, bandwidths, stability and quality to share data within a theatre (including headquarters, commands, units and requesters of JISR results), as well as beyond the theatre with reachback locations in NATO and the nations. This is crucial for sharing JISR results in near real-time (NRT), facilitating rapid decision making and dynamic tasking and enabling timely sensor cross-cueing and reachback support including access to archives.[34] In addition, effective JISR requires the capability to store, share and archive JISR results in compliance with technical and operational standards based on NATO-accepted formats and procedures. Information exchange requirements (IERs) for national units and systems as well as IER interfaces and standards must be addressed and in-place early in the planning process.[35]

b. JISR activities are typically conducted on Alliance-common classified networks. When working with partner nations in a NATO operation, JISR activities will need to be conducted on the agreed mission-common classified network. Although there may be NATO and national caveats precluding the sharing of some information at the mission-common level, the systems and processes that are part of the architecture must be interoperable between NATO, NATO nations and partner nations. The joining, membership, and exiting instructions are designed to facilitate rapid and effective deployment of federated mission networks. Operations planning should consider the currently available systems implemented in NATO and their respective capabilities and limitations. The resulting operational orders should reflect these considerations.

c. Appropriate release and transfer mechanisms and information labeling rules will need to be established and implemented. This will require the

development and deployment of appropriate information exchange gateways

[33] See STANAG 4559, Allied Engineering Documentation Publication (AEDP)-17(A) &18(A) &19(A), *NATO Standard ISR Library, Interfaces and Services,* for NATO standards on the exchange of shared ISR data, products and schemas.

[34] The term "cross-cueing" refers to the passing of detection, geolocation and targeting information from one sensor to another by either manual sensor slewing, or by automated sensor cueing. The second or subsequent asset can provide improved visibility and validity of the target, thus increasing confidence in target identification, confirmation of assumptions or other additional detail.

[35] To ensure information can be exchanged between two or more parties supporting a given process, IERs are pivotal inputs to the CIS planning process ensuring that all relevant command and control (C2) services required in support of the mission are identified, and adequate planning and provision of C2 services can be achieved. For more information on IERs, refer to *Allied Joint Doctrine for Communication and Information Systems,* (AJP-6).

and/or cross-compartment and cross-domain guards. JISR will require sufficient quality of communications network services between theatres and reachback sites to ensure acceptable performance. This aspect is crucial to the provision of an efficient NRT capacity to allow timely sensor cross-cueing as well as reachback support. IER considerations impacting national units and systems should be addressed early in the planning process as well as the required interfaces and standards.

4.5 There must be close communication between intelligence staffs, operations staffs and the communications staffs at the initial stage of the operational planning process to ensure the JISR architecture is sufficient and optimally located to enable access to services, applications and databases.

4.6 **Integration with the operation plan.** The concept of operations (CONOPS) or operation plan (OPLAN) will affect the JISR architecture, including organizational responsibilities and relationships, as well as the communications and information systems (CIS) architecture necessary for mission success.

a. The respective portions within the OPLAN and CONOPS will describe the JISR architecture and the CIS structure necessary for JISR activities. These documents will also explain interoperability between JISR-related data resources and the tools used by the relevant commanders, staffs, units and assets. The architecture will be heavily influenced by IERs across the operation and between NATO and national headquarters, units and JISR assets.[36] Defining the JISR architecture in the appropriate planning documents will ensure visibility within the operations, planning and communications communities and will help identify and address potential shortfalls. Considerations for establishing a JISR architecture include:

- geographical location and characteristics of JISR systems and networks;
- asset capabilities, limitations and quantities to include processing, exploitation and dissemination requirements;
- functional services, bandwidth, connectivity, databases and other CIS support requirements at all levels of commands;
- applicable/available standard operating procedures, standard operating instructions and reporting directives including report templates; information security and information management provisions; and
- dissemination of JISR data, information and JISR results.

4.7 Although the basic concept of the JISR architecture is represented in the

OPLAN or CONOPS, further refinement of the architecture will continue for the duration of the operation.

[36] Refer to MC 0593/1, *Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations.*

Section 3 - Architecture design principles

4.8 The architecture design for JISR is based on the following principles.

a. **Integration of capabilities within the architecture.** Each JISR capability or asset should be fully integrated into the JISR architecture. JISR assets must have the ability to be responsive to several command and control entities and contribute to the satisfaction of intelligence requirements. Assigned PED capabilities must be enabled to process and exploit data from theatre JISR assets and share the results with intelligence elements and requesters at any level to allow for fusion and to support decision-making processes.

b**. Data, information and intelligence sharing.** JISR requires the capability to store and share data, information, results and intelligence, which meet established technical and operational standards. These standards are based initially on NATO-accepted formats and procedures. When NATO direction is not available, the adoption of NATO releasable national standards and procedures may be used.

c. **Interconnected/retrievable.** The JISR architecture will connect nations and NATO intelligence entities to networks enabling stakeholders to discover and retrieve JISR results and to draw on shared information and intelligence including raw and/or processed data originating from both NATO and nationally-owned capabilities. The availability of JISR results that are shared via common agreed-upon networks and data portals will allow requesters across the operation the ability to access both current and historical JISR results.

d. **Flexible and robust.** The JISR architecture should be established, practiced, evaluated and designed to be capable of rapid transition to operations. In addition, it needs to be capable of rapid reconfiguration to meet changing information needs throughout the operation. Any JISR architecture must be robust and resilient to be able to function in any type of environment.

e. **Resilient.** The JISR architecture should be designed to operate under degraded and denied conditions (man-made or natural) to support the planning and conduct of operations at all levels for a given operation.

f**. Compatible.** The JISR architecture must be compatible with both current and future technical constraints and standards, notably for sufficient network connectivity and appropriate broadband links.

g**. Centralized control.** The operational-level headquarters will normally direct the overall JISR effort through their delegated collection requirement management and collection operations management functions.

h**. Federated relationships.** An effective architecture must enable the best possible support to ensure adequate and timely decision-making. Therefore, the architecture must allow JISR resources to be managed and employed in a collaborative manner. This requires federated relationships using networked capabilities and collaborative processes to effectively support operations and fulfil the commander's requirements by ensuring persistence and agility under changing conditions.

i. **PED archiving and retrieval.** NATO commands, agencies, and nations need to plan for JISR architecture requirements far in advance of crises and determine the best potential options to match likely scenarios. As a part of the JISR architecture, PED nodes play a crucial role in the JISR process. PED nodes, where collected data and information is processed and exploited and the JISR results disseminated, archived, and if required, retrieved, must be able to meet the commander's requirements and optimize JISR support to users. Reachback solutions and capabilities involving multinational and national JISR centres should also be part of the planning process in preparing for and executing NATO operations.

Intentionally blank

Annex A – Example of joint intelligence, surveillance and reconnaissance support to joint targeting

A.1 This annex illustrates how joint intelligence, surveillance and reconnaissance (JISR) supports NATO's joint targeting mission. Joint targeting activities rely heavily on JISR collection activities and results (Figure A.1). JISR capabilities and results enable each phase of the joint targeting cycle and play a vital role in target development, target engagement and battle damage assessment. Specifically, JISR capabilities enhance intelligence support to targeting activities, such as positive identification, precise coordinate mensuration and collateral damage estimates. Following target engagement, JISR capabilities can support the assessment phase of the joint targeting cycle and post-engagement requirements to include: battle damage assessment; collateral damage assessment; munitions effectiveness assessment and re-engagement recommendations.

A.2 The JISR process supports deliberate targeting and may use multiple JISR capabilities to provide the required support. However, it is possible that, depending on the relative priorities of the tasks, existing JISR capabilities supporting deliberate targeting operations may be re-tasked to support dynamic targeting operations, due to emerging intelligence and operational collection requirements.

a**. JISR support to deliberate targeting.** Targeting organizations develop individual targets to support specific objectives and guidance.[37] Intelligence analysts and target analysts begin target development by searching existing databases and gathering information, as well as identifying intelligence gaps that require JISR support. This search could generate a request for information (RFI), a collection requirement (CR) or an intelligence, surveillance and reconnaissance request (ISRR). Target analysts continue target development, integrating and analyzing new information as it is collected or provided. As the target analyst performs more advanced target development, a follow-on CR for additional JISR support could be required. For example, the target analyst may require an electro-optical image at a higher resolution to meet operational directives for a collateral damage estimation of a high priority or sensitive target.

b. When advanced target development is complete, the target nomination is presented to the joint targeting working group and/or joint targeting coordination board (JTCB). In both cases, these meetings could generate additional requests and requirements (e.g., RFIs, CRs, ISRRs) from board members sending the nominated target back to the originator for further development. Additionally, decisions made at the JTCB could require JISR coverage during target engagement.

[37] Refer to *Allied Joint Doctrine for Joint Targeting,* (AJP 3.9) for detailed information on the targeting process and activities.

c. **JISR support to dynamic targeting**. After the start of an operation, there is typically an increase in the number of essential targets. For this reason, the importance of dynamic targeting should be well understood and JISR assets should be planned from this perspective. Dynamic targets can include both anticipated events (placing JISR assets and strike assets in a specific area in order to identify and engage targets) and unanticipated events (e.g., emerging targets identified by JISR or non-dedicated JISR assets, which meet a high enough priority that diverts other strike assets or generates new strike missions). Dynamic targeting requires detailed JISR planning and management to place appropriate JISR systems in position to collect on approved dynamic targets but also requires rapid JISR exploitation and dissemination in order to enable effective strike operations against the target. The execution of dynamic targets requires the highest priority for tasking, rapid retasking of JISR assets, and the rapid processing, exploitation and dissemination of relevant information to the targeting cell (including partially or unexploited information when relevant). Given the operational significance of dynamic targets, all theatre JISR assets could be used to effectively track, engage and assess these prioritized targets.

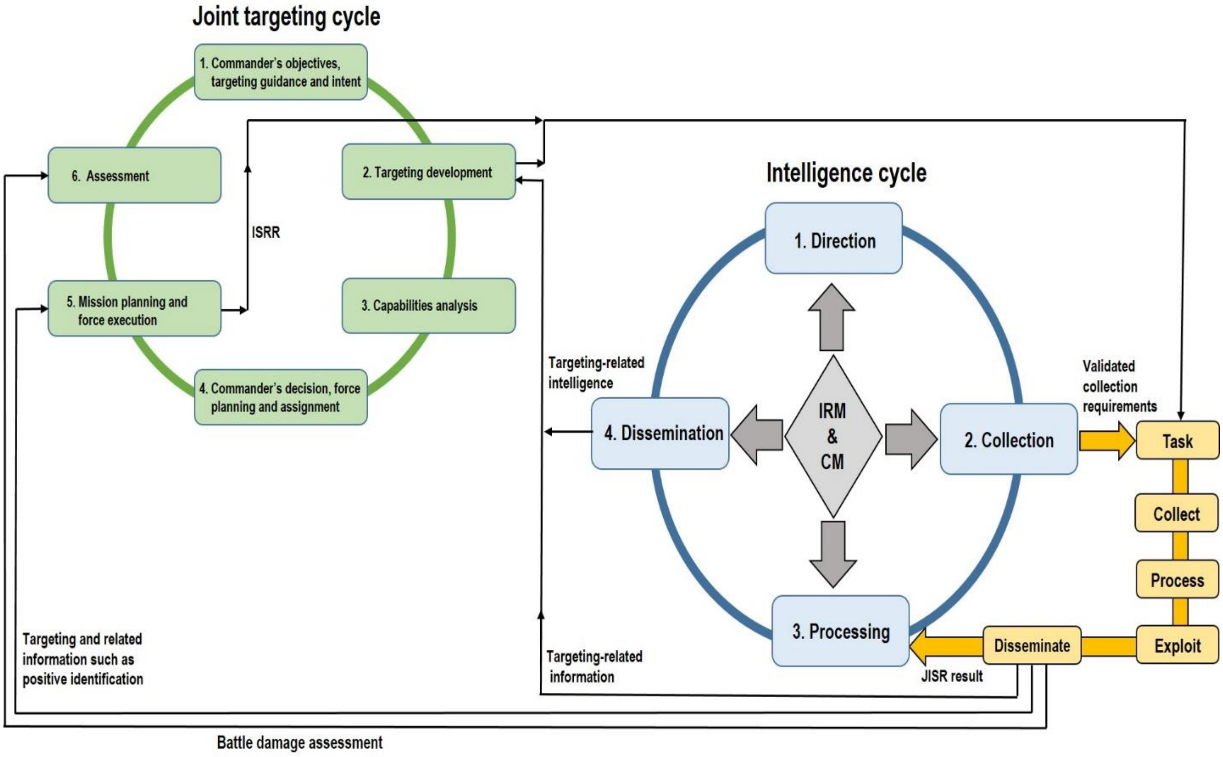
Joint targeting cycle
1. Commander's objectives, targeting guidance and intent
2. Targeting development
3. Capabilities analysis
4. Commander's decision, force planning and assignment
5. Mission planning and force execution
6. Assessment
ISRR
Intelligence cycle
1. Direction
2. Collection
3. Processing
4. Dissemination
IRM & CM
Targeting-related intelligence
Validated collection requirements
Task
Collect
Process
Exploit
Disseminate
JISR result
Targeting-related information
Targeting and related information such as positive identification
Battle damage assessment

Figure A.1 – JISR support to joint targeting

Lexicon

Part 1 – Acronyms and abbreviations

ACINT	acoustic intelligence
AIntP	Allied intelligence publication
AJP	Allied joint publication
CIS	communications and information systems
CJSOR	combined joint statement of requirements
CM	collection management
CMA	collection management authority
COM	collection operations management
CONOPS	concept of operations
CR	collection requirement
CRL	collection requirements list
CRM	collection requirements management
CT	collection task
CTL	collection task list
CXP	collection and exploitation plan
EEI	essential elements of information
HUMINT	human intelligence
ICP	intelligence collection plan
IER	information exchange requirement
IMINT	imagery intelligence
IR	intelligence requirement
IRM	intelligence requirements management
IRM&CM	intelligence requirements management and collection management
ISR	intelligence, surveillance and reconnaissance
ISRR	intelligence, surveillance and reconnaissance request
JCMB	Joint Collection Management Board
JCMWG	Joint Collection Management Working Group
JFC	Joint Force Command
JIPOE	joint intelligence preparation of the operating environment
JISR	joint intelligence, surveillance and reconnaissance
JOA	joint operations area
JTCB	Joint Target Coordination Board
LO	liaison officer
MASINT	measurement and signature intelligence
MC	Military Committee (NATO)
MOE	measure of effectiveness
MOP	measure of performance

NATO	North Atlantic Treaty Organization
NRT	near real-time
OE	operating environment
OPLAN	operation plan
OSINT	open-source intelligence
PED	process, exploit, disseminate
PIR	priority intelligence requirement
RFI	request for information
ROE	rules of engagement
SA	situational awareness
SIGINT	signals intelligence
TCM	theatre collection manager
TCPED	task, collect, process, exploit and disseminate

Part 2 - Terms and definitions

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. (This term and definition modify an existing term and definition and has been processed for NATO Agreed status via terminology tracking file [2011-1237])

collection management (CM)
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. [NATO Agreed]

collection management authority
The authority to develop, establish, validate and prioritize collection requirements; establish asset tasking; and to develop and execute collection, exploitation and dissemination plans and strategies. [This term and definition only applies to this publication]

collection operations management
The direction, scheduling and control of specific collection operations and associated processing, exploitation, asset management and reporting resources.
(This term is a new term and definition and has been processed for NATO Agreed status via terminology tracking file [2019-0356])

collection requirement (CR)
A validated information requirement, for which the requested information is not already available in a repository and therefore needs to be collected through joint intelligence, surveillance and reconnaissance asset tasking or be forwarded as a request to higher or adjacent commands. (NATO Agreed)

collection requirement management
A staff management function that receives all collection requirements and joint intelligence, surveillance and reconnaissance requests and then consolidates and prioritizes those requirements to produce the draft collection task list. (This term is a new term and definition and has been processed for NATO Agreed status via terminology tracking file [2019-0359])

information
Processed data of every description which may be used in the production of intelligence. [NATO Agreed]

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. [NATO Agreed]

intelligence cycle
The sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users. (This term and definition modify an existing term and definition and has been processed for NATO Agreed status via terminology tracking file [2015-0009])

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. [NATO Agreed]

intelligence requirements management (IRM)
The management function that develops, validates and prioritizes intelligence requirements, forwards validated intelligence requirements to the collection management authority and oversees dissemination of the intelligence products. [NATO Agreed]

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, operations or time period. [NATO Agreed]

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

joint intelligence, surveillance and reconnaissance (JISR)
An integrated intelligence and operations set of capabilities, which synchronizes 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. [NATO Agreed]

joint intelligence, surveillance and reconnaissance asset (JISR asset)
An individual, detachment, unit, sensor, or platform that can be tasked by respective authorities to achieve joint intelligence, surveillance and reconnaissance results. (This term is a new term and definition and has been processed for NATO Agreed status via terminology tracking file [2019-0349])

joint intelligence, surveillance and reconnaissance capability (JISR capability)
An asset or set of assets, including supporting organizations, personnel, collectors, systems, supporting infrastructure, processing, exploitation and dissemination processes used to achieve a designated joint intelligence, surveillance and reconnaissance result. [NATO Agreed]

joint intelligence, surveillance and reconnaissance process (JISR process)
A coordination process through which intelligence collection disciplines, collection capabilities and exploitation activities provide data, information and single source intelligence to address an information or intelligence requirement, in a deliberate, ad hoc or dynamic time frame in support of operations planning and execution.
Notes: The joint intelligence, surveillance and reconnaissance (JISR) process consists of five steps: Task, Collect, Process, Exploit and Disseminate, referred to as task, collect, process, exploit and disseminate (TCPED). [NATO Agreed]

joint intelligence, surveillance and reconnaissance result (JISR result)
The outcome of the intelligence, surveillance and reconnaissance process disseminated to the requester in the requested format. (This term is a new term and definition and has been processed for NATO Agreed status via terminology tracking file [2019-0344])

reachback
The process to provide deployed forces with services and capabilities from experts that are external to the theatre of operations. [NATO Agreed]

reconnaissance (RECCE)
A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy adversary, or to secure obtain data concerning the meteorological, hydrographical or geographic characteristics of a particular area. [NATO Agreed]

surveillance
The systematic observation across all domains, places, persons or objects by visual, electronic, photographic or other means. [NATO Agreed]

understanding
The interpretation and comprehension of a particular situation in order to provide the context, insight and foresight required for effective decision-making.
(This term is a new term and definition and has been processed for NATO Agreed status via terminology tracking file [2019-0342])

AJP-2.7(A)(2)