NATO STANDARD

AEDP-02
VOLUME I

NATO INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR) INTEROPERABILITY ARCHITECTURE (NIIA) - ARCHITECTURE DESCRIPTION

Edition B Version 1
JANUARY 2018

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED ENGINEERING DOCUMENTATION PUBLICATION

Published by the
NATO STANDARDIZATION ORGANISATION (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION ORGANISATION (NSO)

NATO LETTER OF PROMULGATION

9 January 2018

1. The enclosed Allied Engineering Documentation Publication AEDP-02, Volume I, Edition B, Version 1, NATO INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (ISR) INTEROPERABILITY ARCHITECTURE (NIIA) - ARCHITECTURE DESCRIPTION, which has been approved by the nations in the NATO AIR FORCE ARMAMENTS GROUP, is promulgated herewith. The agreement of nations to use this publication is recorded in STANREC 4777.

2. AEDP-02, Volume I, Edition B, Version 1, is effective upon receipt and supersedes AEDP-02, Volume I, Edition 1 which shall be destroyed in accordance with the local procedure for the destruction of documents.

3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member nations or NATO commands and bodies.

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

Edvardas MAŽEIKIS
Major General, LTUAF
Director NATO Standardization Agency

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
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 Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

<table>
<tr><td>[nation]</td><td>[detail of reservation]</td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">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 Database for the complete list of existing reservations.</td></tr>
</table>

INTENTIONALLY BLANK

FOREWORD

This document describes the NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA), which defines how NATO and national reconnaissance and surveillance assets within the Joint Capability Group on ISR (JCGISR) area of responsibility will achieve interoperability. The main aim of the NIIA is to outline a top-level architecture which will provide a context and structure for the JCGISR STANAGs and other interoperability initiatives. A complete architecture should include a technical view, a systems view, and an operational view to be complete. However, the systems and operational views are dependent on the specific scenario, the participating nations' systems involved, and the operational view defining how the various systems are actually interconnected. While an armaments group, such as the JCGISR, could theorize hypothetical scenarios and generate the systems and operational views based on those hypothetical scenarios, the NIIA focuses on the technical issues of providing the interconnectivity options between national and NATO-owned systems.

This Allied Engineering Documentation Publication (AEDP) provides the technical and management guidance for implementing the NIIA to support NATO operations. It is divided into three volumes. Volume I provides the introduction and explanation of the technical architecture. Volume II contains guidance for configuration management, test and certification, intra-NIIA dependencies, and terms and definitions. The two volumes are published separately due to the large size of each.

This volume focuses on providing an introduction to the architecture and a description of the philosophy behind the architecture and its key elements. It identifies the specific standards to be implemented and describes how the standards fit together into the architecture. This volume addresses interoperability aspects of multiple intelligence disciplines within a single architecture framework.

In addition to AEDP-02, users of the NIIA should be cognizant of each of the STANAGs incorporated into the architecture. These STANAGs provide the key interface standards needed to provide the systems interoperability. Many of the STANAGs also have separate Implementation Guides for the standard, published as separate AEDPs.

Questions or comments on this document can be provided to either the Secretary of JCGISR or the NIIA Custodian. Correspondence to the Secretary should be addressed to: Secretary, JCGISR; ISR Section, Armament and Aerospace Capabilities Directorate, Defence Investment Division; HQ NATO; B-1110, Brussels, Belgium (telephone: +32-2- 707-4313; telefax: +32-2-707-4103). Correspondence to the Custodian should be addressed to: Custodian, NIIA; SAF/AQIX; 1060 Air Force Pentagon; Washington D.C. 20330-1060; United States (telephone +1 571-256-0129).

TABLE OF CONTENTS

TABLE OF FIGURES

Executive Summary

This document describes the NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA), which defines how NATO and national reconnaissance and surveillance assets within the Joint Capability Group on ISR (JCGISR) area of responsibility will achieve interoperability. The main aim of the NIIA is to outline a top-level architecture which will provide a context and structure for the JCGISR STANAGs and other interoperability initiatives.

The NIIA provides the description of the operational environment, including a number of variations on the basic data flow. This description includes notional task flow descriptions and timelines. It also provides a summary of standards included in the NIIA. Each standard is discussed in terms of its application and use. Other documents relevant to the architecture, including draft standardization agreements (STANAGs), are also specified.

NATO defines interoperability as the ability to act together coherently, effectively, and efficiently to achieve Allied tactical, operational and strategic objectives.[1] The NIIA is focused on technical ISR interoperability, which allows NATO and national systems to communicate with and amongst one another and share data and information. To expand upon NATO's definition of interoperability, different levels of technical interoperability are possible. These include:

- Degree 1: Unstructured Data Exchange. Involves the exchange of human-interpretable unstructured data such as the free text found in operational estimates, analysis and papers.
- Degree 2: Structured Data Exchange. Involves the exchange of human-interpretable structured data intended for manual and/or automated handling, but requires manual compilation, receipt and/or message dispatch.
- Degree 3: Seamless Sharing of Data. Involves the automated sharing of data amongst systems based on a common exchange model.
- Degree 4: Seamless Sharing of Information. An extension of degree 3 to the universal interpretation of information through data processing based on cooperating applications.

It should be noted that the objective of the NIIA is to achieve interoperability at Degree 2, with some specific interfaces achieving Degree 3. Degree 4 can be considered a long-term objective, but lower degrees of interoperability should not be delayed in favour of ultimately achieving a higher degree. Degree 2 interoperability is a significant accomplishment, and will provide a high level of capability to NATO and coalition forces. Higher degrees of interoperability will be addressed once Degree 2 is achieved and demonstrated unless evidence of higher degrees of interoperability are easily

[1] AAP-06. NATO Glossary of Terms and Definitions (English and French). 14 December 2016.

achievable. A continuing issue is the multitude of configuration choices provided by many of the standards, thereby allowing multiple implementations that would not be interoperable with the broader NIIA. It will be important to develop interface profiles that define the specific choices within each standard, thereby ensuring interoperability.

In summary, the ISR architecture is applicable across all levels of NATO and coalition operations, including both Article 5 and non-Article 5 operations. Finally, while the standards are sufficient, there is a large volume of supporting documentation, including configuration management plans, test and certification plans, implementation guidance, and acquisition guidance, that are available to the community. STANAG custodians should consolidate this documentation into a single volume to accompany each standard. The accepted form of this volume is an Allied Engineering Documentation Publication (AEDP). Combining the AEDPs with this document and the standards forms the complete NIIA definition and documentation set.

INTENTIONALLY BLANK

CHAPTER 1 INTRODUCTION

1.1 Overview

1.1.1. This document describes the NATO Intelligence, Surveillance, and Reconnaissance (ISR) Interoperability Architecture (NIIA), which defines how NATO and national reconnaissance and surveillance assets within the Joint Capability Group on ISR (JCGISR) area of responsibility will achieve interoperability. The main aim of the NIIA is to outline a top-level architecture which will provide a context and structure for the JCGISR STANAGs and other interoperability initiatives. The JCGISR has the basic responsibility for interoperability of ISR systems. Specifically, it has the responsibility for specifying standards for ISR assets to achieve interoperability within coalition and NATO environments. The goal of the NIIA is to provide a concept to achieve data exchange interoperability between NATO and national ISR assets.

1.2 Scope

1.2.1. The NIIA builds upon the construct laid down in the NATO Enterprise Architecture (NEA) (see Figure 1), which addresses, as a minimum, the NATO Headquarters, the NATO Command Structure, the NATO Agencies plus other NATO requirement holders and customers entitled to consume information and communication technology services provided by NATO Service Providers.[2] The NEA is defined as the combination of:

a. Business architecture defining business strategy, governance, organisation and key business processes;

b. Information Architecture describing the organisation logical and physical information assets and information management resources;

c. Application Architecture providing a blueprint for the individual services to be deployed, their interactions, and their relationship to the core business processes of the organisation;

d. Technology Architecture describing the infrastructure (software & hardware) capabilities that are required to support the deployment of services.

1.2.2. This document interfaces with the Technology Architecture of the NEA and provides the technical framework to provide interoperability between national and NATO ISR systems and outlines the concepts for the development of an ISR architecture for NATO. The NIIA is focused on promoting interoperability of NATO and national ISR assets among NATO/Coalition nations, which supports NAFAG's focus areas, including: Requirements Harmonisation and Translation Mechanism; Interoperability Through Standardization; Interoperability Through Armaments

[2] C-M(2015)0041-REV1 "NATO Enterprise Architecture Policy," https://tide.act.nato.int

Procurements; Information Exchange; Leverage Civil and Defence Technology & Industry; and Demonstrations.[3]

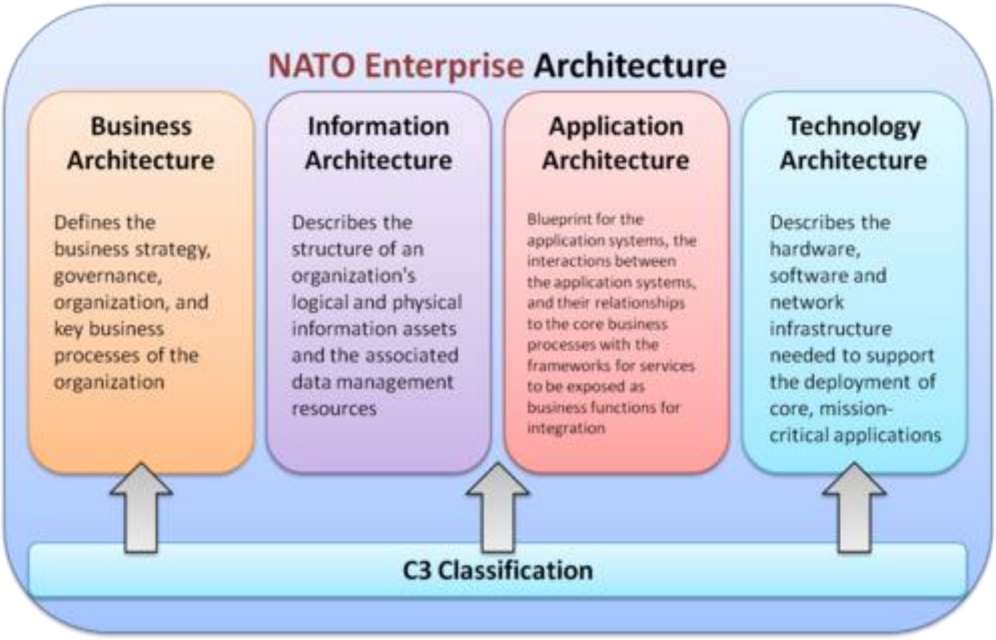

NATO Enterprise Architecture
Business Architecture
Defines the business strategy, governance, organization, and key business processes of the organization
Information Architecture
Describes the structure of an organization's logical and physical information assets and the associated data management resources
Application Architecture
Blueprint for the application systems, the interactions between the application systems, and their relationships to the core business processes with the frameworks for services to be exposed as business functions for integration
Technology Architecture
Describes the hardware, software and network infrastructure needed to support the deployment of core, mission-critical applications
C3 Classification

Figure 1: NATO Enterprise Architecture

1.2.3. The key to successful deployment of interoperable systems is the implementation of the architecture in national and NATO systems, and the test and certification of the implementations to verify interoperability and compliance with the standards. Implementation is an obvious element of interoperability, but one that is often deferred due to resource limits or lack of political will. Test and certification of the implementations is less obvious, but an important step in achieving interoperability. The standards for digital interoperability are complex and often have multiple options. Test and certification ensures that the standards were correctly interpreted and applied, and documents the options chosen in the particular implementation. Failure to test the implementation often results in expensive fixes in the field to make systems work together after deployment. This is more expensive and delays the integration of important systems into operations.

1.2.4. While this document addresses the technical issues of interoperability for ISR systems, issues of security and data sharing policies can still hinder the dissemination and retrieval of ISR data throughout the combat theatre. These issues must be addressed at the senior national levels to ensure that battlefield commanders and combatant forces can access the information they need to execute their missions with the minimum amount of risk to Alliance or Coalition resources.

1.3. Background

[3] AC/224-D(2017)0003 “NAFAG Management Plan,” 3 March 2017.

1.3.1. Technological advances in weaponry and communications continue to drive the need for NATO forces to field responsive ISR assets that possess interoperable capabilities. Rapid and accurate collection, exploitation, and dissemination of relevant information are vital to achieving operational objectives.

1.3.2. The NATO Interoperability Design Study was conducted in the early 1990s to investigate ways to enable interoperability of electronic systems. One of the approaches considered was to mandate that all nations procure and operate the same systems. However, it was emphasised at this time that NATO could not mandate interoperability of national ISR systems, but that interoperability among national systems would be purely voluntary. Instead, NATO developed a number of Standardization Agreements (STANAGs) to allow exchange of data between ISR systems and, eventually, the NIIA, first promulgated in 2005. While the STANAGs and the work of the NAFAG initially focused primarily on Imagery Intelligence (IMINT), the work of the JCGISR and its subordinate All-Source Intelligence Integration Sub-Group has expanded the scope of intelligence disciplines and associated interoperability requirements and documents that compose the NIIA.

1.3.3. The NIIA relies on the interoperability of data, sensors, platforms, and information systems across the ISR Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED) process to produce all-source intelligence.[4] All-source intelligence can include Geospatial Intelligence (GEOINT),[5] Human Intelligence (HUMINT),[6] IMINT, Measurement and Signature Intelligence (MASINT),[7] Open-Source Intelligence (OSINT),[8] and Signals Intelligence (SIGINT).[9]

1.3.4. In order to address the expanding interoperability challenges, the Multi-Sensor Aerospace-ground Joint ISR Interoperability Coalition (MAJIIC), a nine-nation multinational effort that began in 2005, aimed to maximize the military utility of surveillance and reconnaissance resources through the development and evaluation of operational and technical means for interoperability of a wide range of ISR assets. MAJIIC addressed interoperability from operational, architectural, and technical perspectives. MAJIIC's work on architectural and technical interoperability helped refine the NIIA. Areas addressed included developing procedures and technology for

[4] Intelligence produced using all available sources and agencies. AAP-06.

[5] Intelligence derived from the combination of geospatial information, including imagery, with other intelligence data to describe, assess and visually depict geographically referenced activities and features on the earth. AAP-06.

[6] A category of intelligence derived from information collected and provided by human sources. AAP-06.

[7] Intelligence derived from the scientific and technical analysis of data obtained from sensing instruments for the purpose of identifying any distinctive features associated with the source, emitter or sender, to facilitate the latter's measurement and identification. AAP-06.

[8] Intelligence derived from publicly available information, as well as other unclassified information that has limited public distribution or access. AAP-06.

[9] The generic term used to describe communications intelligence and electronic intelligence when there is no requirement to differentiate between these two types of intelligence, or to represent fusion of the two. AAP-06.

sharing ISR data and information, system architecture design principles, collaboration tools and technology, tools for managing coalition ISR assets, defining and developing key data formats and protocols for the various sensor and data types, and common geo-registration and data exploitation tools.[10] MAJIIC (and its follow on MAJIIC2) has since concluded and NATO is in the process of operationalising MAJIIC into NATO-wide technologies and standards.

1.3.5. The need to improve NATO Joint ISR (JISR) became more critical following NATO's Operation UNIFIED PROTECTOR in Libya, where Allies observed a number of shortfalls in NATO's ability to coordinate and deploy Allied ISR capability, including a lack of ISR assets and a dearth of trained experts to interpret the data. At the 2012 Chicago Summit, Allies agreed to provide NATO with an enduring and permanently-available JISR capability. In February 2016 NATO declared Interim Operating Capability for JISR which signified NATO's ability to provide ISR support to the NATO Response Force. Further work in JISR includes integrating Alliance Ground Surveillance (AGS) into NATO and achieving higher levels of interoperability among NATO and national ISR assets.

1.3.6. As acknowledged in the Warsaw Summit Communique, there is an arc of insecurity and instability along NATO's periphery and beyond. The Alliance faces a range of security challenges and threats that originate both from the east and from the south; from state and non-state actors; from military forces and from terrorist, cyber, or hybrid attacks. NATO's ability to understand, track and, ultimately, anticipate, the actions of potential adversaries through ISR capabilities and comprehensive intelligence arrangements is increasingly important, particularly with the increased use of hybrid warfare where a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, are employed in a highly integrated design by state and non-state actors to achieve their objectives.[11]

1.4 Architecture Description

1.4.1. An overall architecture is composed of three principle views: the systems view, the operational view, and the technical view. Figure 2 shows these views and their interrelationships. Within the concept of the NIIA, the systems and operational views define the configuration of systems and the operational linkage, both of which are scenario dependent. Rather than define possible scenarios and potentially constrain the architecture to a configuration that would not be used, the NIIA focuses on the technical view to provide the tools for interoperability, while not constraining it to a specific set of scenarios. The definition of the systems and operational views for a particular architecture are left to the people charged to create the specific operational networks based on the resources available from the Nations.

[10] "NATO Nations Deepen Cooperation on Intelligence, Surveillance, and Reconnaissance", 17 March 2011, http://www.nato.int/cps/en/natohq/news_71562.htm?selectedLocale=en
[11] "Warsaw Summit Communique" 9 July 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm.

1.4.2. Within each of the views, the model provides for greater detail by using sub-views.

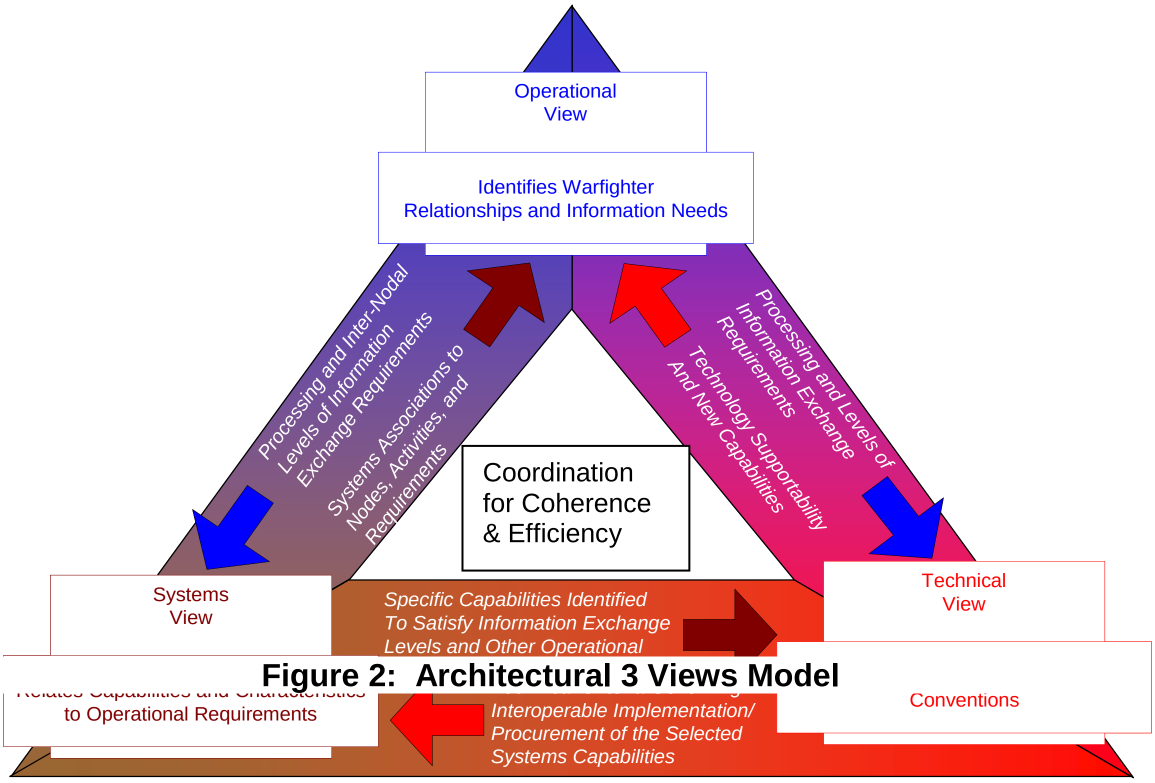


Figure 2: Architectural Views Model

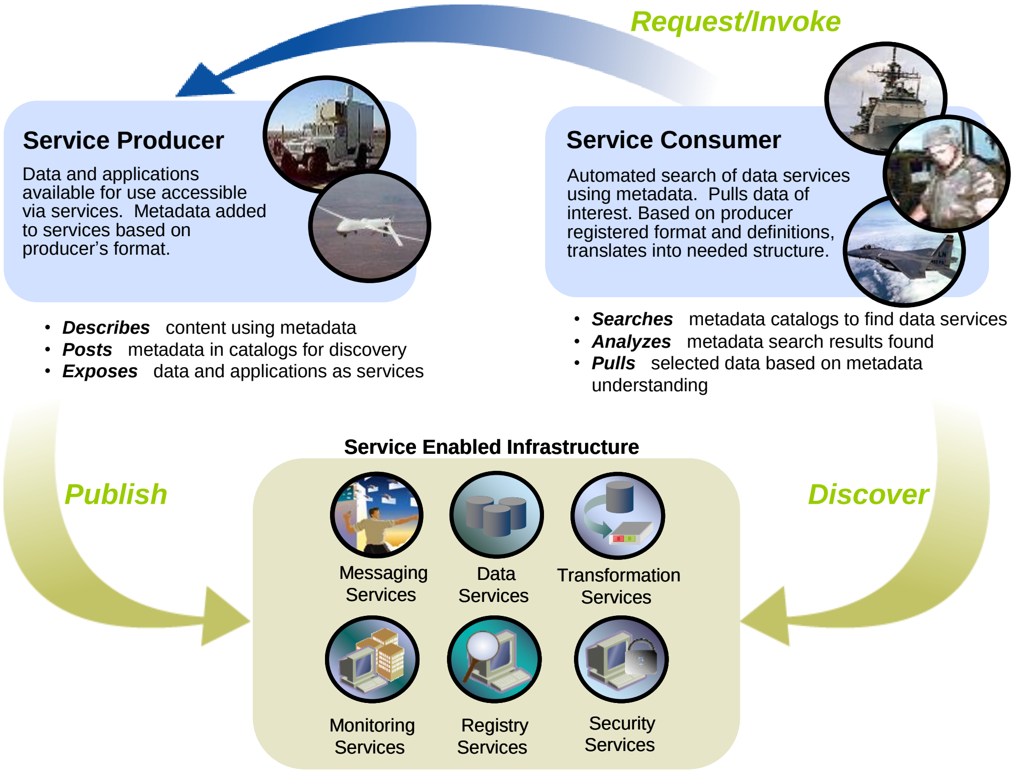
1.5 Service Oriented Architecture (SOA)

1.5.1. Many of the current STANAGs support SOA-type applications and others will need to be modified. A key element of the SOA will be the access to a coalition shared data repository. This set of interfaces provides connectivity for both the ISR data analysts, and to elements of the command and control hierarchy.

1.5.2. SOA allows the registration of services on a network and the access of the services by clients who were able to find them, which groups the network participants into one of two classes: service providers and service consumers. Frequently, a particular network participant could serve both roles, providing services to some and using services provided by others. Particularly when the network is authorized for classified information, the security services will generally be used by all.

1.5.3. Figure 3 provides an overview of the SOA concept. The service providers describe content using metadata, post metadata in catalogues for discovery, and exposes data and applications as services. The service consumers search metadata catalogues to find data services, analyse metadata search results found, and pull selected data based on metadata understanding. In order to enable this exchange, the network must provide services that underpin the applications. These services are collectively called the core enterprise services and fall generally into six categories.

- Messaging Services: These services provide the ability of users to communicate. Common examples include email services and chat (instant messaging).
- Monitoring Services: Services which allow network administrators to track network performance and data movement.
- Data Services: Repositories and applications used to populate and manipulate the data.
- Registry Services: Tools used to locate services and/or data on the network.
- Transformation Services: Tools used to transform data to make it usable in specific applications, such as to translate data from one format to another, language translations, and manipulations required to get data from one network to another (bridges, guards, etc.)
- Security Services: Services provided to ensure the integrity of the network, to both minimize intrusions and manage security markings.



Service Producer

Data and applications available for use accessible via services. Metadata added to services based on producer's format.

- ***Describes*** content using metadata
- ***Posts*** metadata in catalogs for discovery
- ***Exposes*** data and applications as services

Service Consumer

Automated search of data services using metadata. Pulls data of interest. Based on producer registered format and definitions, translates into needed structure.

- ***Searches*** metadata catalogs to find data services
- ***Analyzes*** metadata search results found
- ***Pulls*** selected data based on metadata understanding

Figure 3.1-1; SOA Concepts

Figure 3: SOA Concepts

1.5.4. The NIIA standards tend to fall into the data and registry services groups. Transformation services may enhance data and metadata harmonisation and alignment. There are also some attributes of the security services in various NIIA standards, but the basic network security remains the responsibility of the network administrator. For example, most of the data formats contain security markings for the information contained in the file, but the network security guards provide the services for checking and transferring the files within the larger scope of the architecture.

1.5.5. Depending on which connectivity is being addressed – the two nodes being connected and the information required to move in both directions – a different subset of the STANAGs and other standards is used. For example, to retrieve a frame of imagery, STANAG 4559 protocols may be used to query a database and request a particular frame, and typically STANAG 4545 is used to format the image for transmission to the requestor. In addition, the actual connectivity is over communications channels that may use Transmission Control Protocol/Internet Protocol (TCP/IP), Ethernet, and/or any of the many other communications standards.

1.5.6. It should be noted that a capability is more than just new equipment or materiel. This underlying philosophy is best described through a series of requirements that support an overall capability:

- Doctrine - Strategic to Tactical, including Joint
- Organization - Unit structures to operate and sustain capability
- Training - Individual to unit training to employ the capability
- Materiel - All required materiel items, including related spares, repair parts, and support equipment, necessary to equip, operate, maintain, and support the capability
- Leadership - Professional military education for the joint commander and staff officers who will use the capability
- Personnel - Adjustments to Peacetime Establishment, Conflict Establishment, and Combined Joint Status of Requirements to take advantage of capability
- Facilities - Real property consisting of buildings, structures, utilities, pavement, or land
- Interoperability - All the issues related to interoperability and connectivity of information systems and security domains

1.5.7. While the NIIA is principally a technical architecture and does not address many of these elements, the JCGISR recognises that coordination with organizations regarding the other elements of the capability is critical to the success of the architecture. Implementing the elements of the NIIA supports the materiel and interoperability elements of the Doctrine, Organization, Training Materiel, Leadership, Personnel, Facilities, and Interoperability (DOTMLPFI) construct; and proper coordination helps ensure appropriate implementation of the other elements.

1.6 NIIA’s Relationship to NATO’s Intelligence and JISR Cycles

1.6.1. Allied Joint Doctrine for JISR, AJP-2.7, establishes Allied joint doctrine to guide commanders, staffs, and forces engaged in JISR operations within the NATO Alliance. AJP-2.7 documents the principles, fundamentals, and essential staff procedures necessary to successfully plan, direct and execute JISR operations that ensure timely and effective decision making. AJP-2.7 provides the framework for coordinating and tasking JISR capabilities to ensure that JISR results are disseminated to the right person, at the right time, in the right format, in direct support of current and future operations and the operational planning process.

1.6.2. The role of the NIIA in this relationship is to provide the technical foundation that enables the movement of the information along the intelligence and operations cycles. In order for the JISR information to flow through the cycles, interoperability standards must be established and agreed amongst the nations. The NIIA documents those interoperability standards agreements and allows for future technological advances.

1.6.3. Figure 4 illustrates the basic JISR concept and its relationship to the Intelligence and Operations Cycles. The JISR process, driven by the needs of the requester, is designed to satisfy intelligence and information requirements and to assist in the conduct of operations. Requesters, commanders and their staffs, create intelligence requirements based on information gaps that need to be fulfilled for the successful completion of NATO operations. These requests are coordinated via a Collection Task List (CTL) and tasked to JISR capabilities to provide data, information, or single-source intelligence (JISR results) necessary to satisfy the commanders' requests.

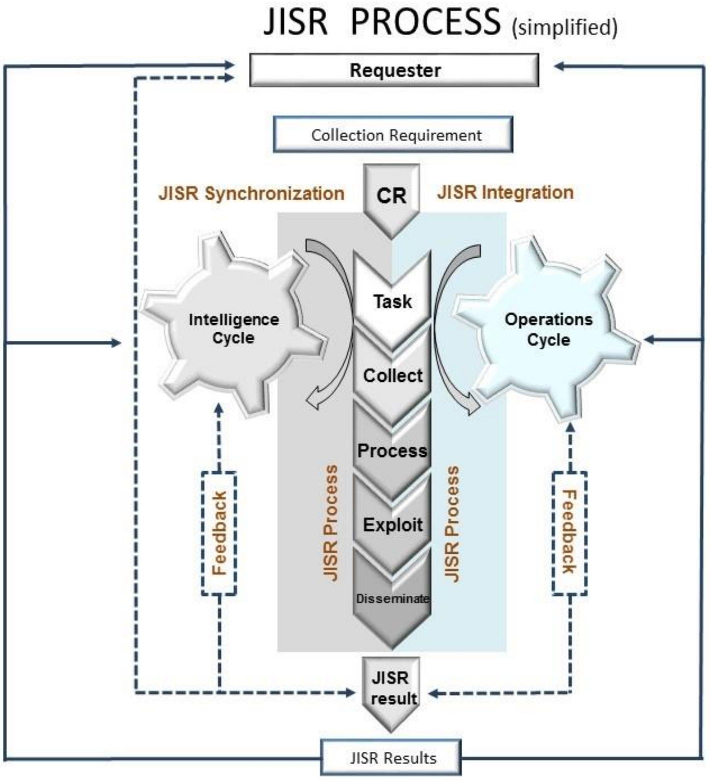


Figure 4: Relationship of the JISR Process to the Intelligence & Operations Cycles[12]

1.7 NIIA Scope and Process

1.7.1. The NIIA describes the structure of components and their relationships to NATO ISR systems in order to provide the minimum information for the interoperability of NATO JISR systems. As systems become more and more complex, system interoperability can compound in complexity. An interoperable interface's complexity is driven by the military requirement. Trying to achieve interoperability of complex systems without an overarching architecture is impossible.

1.7.2. The NIIA also encompasses a net-centric information architecture. In a net-centric environment, producers and users of information are all interlinked, enabling

[12] AJP-2.7, "Allied Joint Doctrine for Joint Intelligence, Surveillance, and Reconnaissance," Edition A, Version 1, July 2016.

secure access to distributed databases to ensure redundancy and rapid posting of perishable data. Once ISR information/data is posted, users can establish customized profiles to: 1) automatically push data to appropriate users, and/or 2) execute a “smart pull” to automatically request (or be alerted to) relevant data.

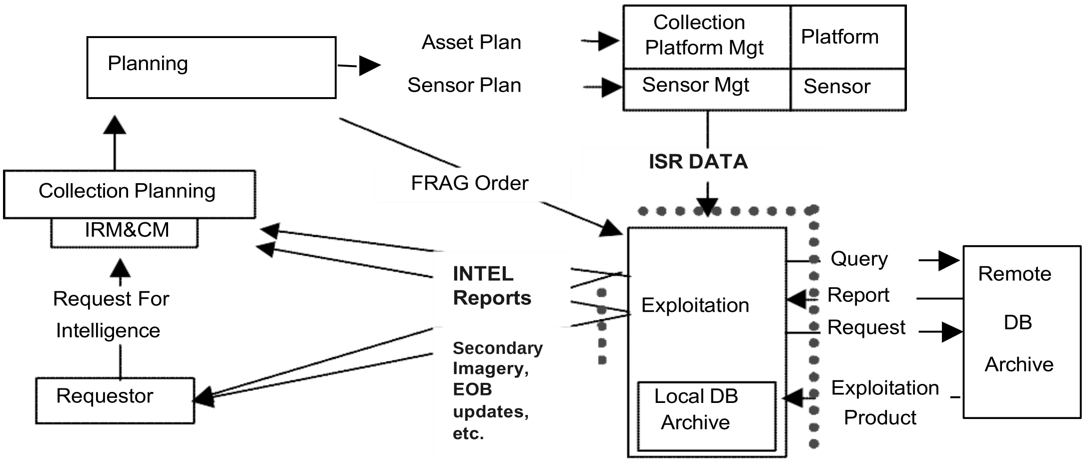


Figure 5: NIIA Scope and Process

1.7.3. Benefits of increased NATO JISR interoperability includes:

a. Improved quality of intelligence through data fusion
b. Improved availability of intelligence at all levels of command
c. Improved accessibility to all areas of terrain
d. Improved dissemination capacity
e. Improved timeliness of information & intelligence
f. Improved area of coverage, revisit rate, endurance and time of coverage; and
g. Improved flexibility of operation and increased redundancy in the event of attrition

CHAPTER 2 CURRENT SITUATION

2.1 NATO is an alliance of nations formed by a multinational agreement, thus it has no real authority to mandate requirements for national procurements. Therefore, it is a commitment on behalf of each nation to be interoperable with NATO systems and systems from other NATO nations. Each nation will need to assess the benefit of interoperability against the cost of compliance. Nations may opt for different degrees of interoperability based on their assessment. The JCGISR's responsibility is to ensure that the tools to provide interoperability at any degree are in place. NATO-owned JISR systems include NATO Early Warning & Control (NAEW&C) aircraft and Alliance Ground Surveillance (AGS). In addition, many nationally-owned ISR systems are made available to NATO.

2.2. The JISR process is a framework through which a single collection requirement is satisfied by a JISR asset following five sequential steps: Task, Collect, Process, Exploit and Disseminate (TCPED). These steps apply at all levels of command, across components, for any type of mission, and in all operational environments. The JISR process provides commanders with specific intelligence discipline data and information to address an operational or intelligence collection requirement. The JISR process supports both current operational needs and ultimately, the production of multi-source intelligence.[13]

2.3. Figure 6 is a notional diagram depicting how the JISR process is integrated with two management staff functions: Intelligence Requirements Management and Collection Management (IRM&CM). CM is divided into two processes: Collection Requirements Management (CRM) and Collection Operations Management (COM). The IRM&CM develops and prioritizes the information and intelligence requirements that drive JISR tasking. Deliberate JISR tasking is the typical mechanism to develop, coordinate and assign JISR tasks to JISR assets. It guarantees sufficient time for mission integration, mission planning, mission tasking and mission preparation. Deliberate JISR tasking can be accomplished directly for the dedicated JISR assets. It occurs also when there is sufficient lead-time for Collection Requirements (CRs) to be incorporated into a Collection Requirements List (CRL) and finally in a Collection Task List (CTL) which is approved at the Joint Coordination and Monitoring 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 the Nations provide tactical control of ISR assets to the commander. This occurs when the development of CRs and JISR tasks are synchronized with other relevant staff rhythms and integrated for mission tasking. Deliberate tasking involves all related functions of IRM&CM as depicted in Figure 6.

[13] AJP-2.7

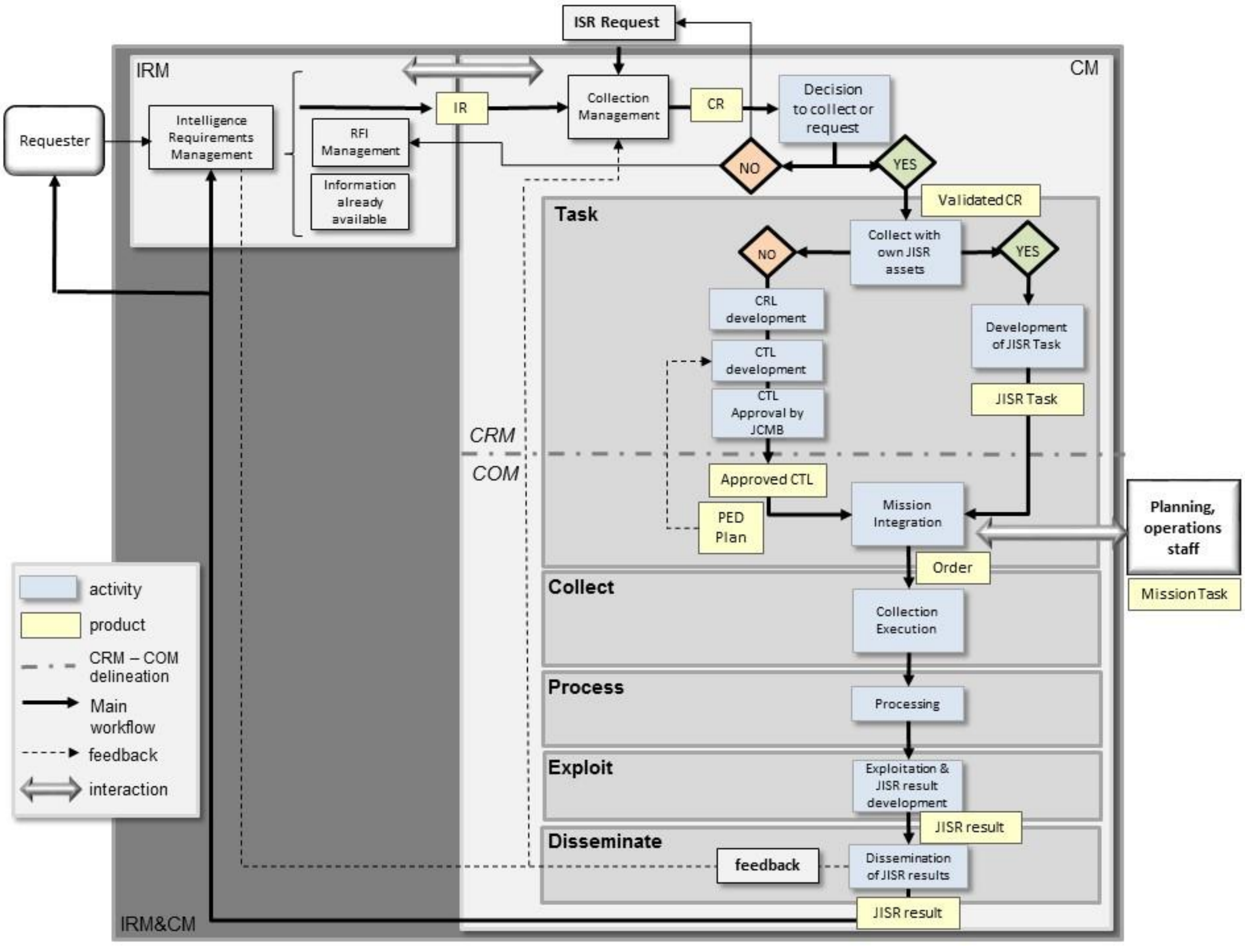
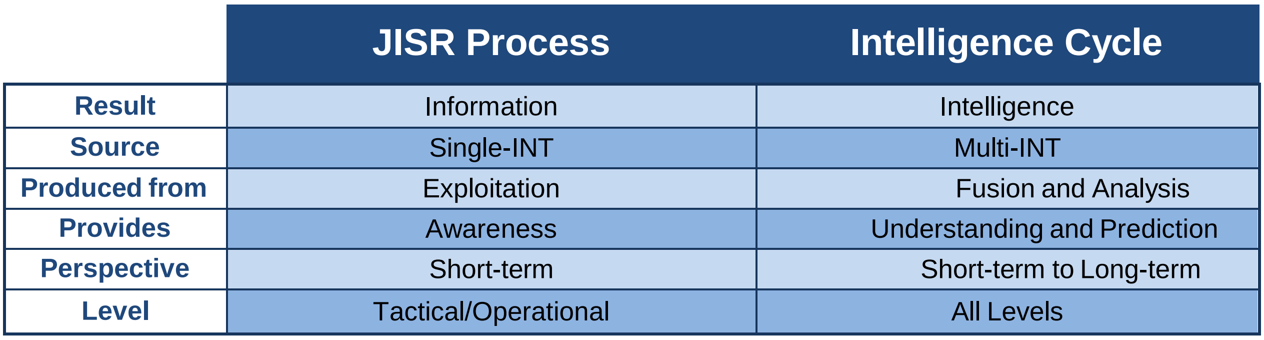


Figure 6: Deliberate JISR Tasking Process[14]

2.4. A key difference between the Intelligence Cycle and the JISR Process, as identified in AJP 2.7, is the product. The JISR Process produces single-source intelligence products and information. Some of this information and intelligence is in response to short-term operational requirements, supporting situational awareness. This information is also the input to the Intelligence Cycle's Processing step. This step takes information and intelligence from all sources to produce a multi-source intelligence product to address the commander's intelligence requirements. Both processes support operations at all levels of commend, with the time scale dependent on the requirements of that level of command. Figure 7 illustrates the key differences AJP 2.7 identifies that distinguish the JISR Process from the Intelligence Cycle.[15]

[14] AJP 2.7
[15] AJP 2.7



	JISR Process	Intelligence Cycle
Result	Information	Intelligence
Source	Single-INT	Multi-INT
Produced from	Exploitation	Fusion and Analysis
Provides	Awareness	Understanding and Prediction
Perspective	Short-term	Short-term to Long-term
Level	Tactical/Operational	All Levels

Figure 7: Differences between the JISR Process and the Intelligence Cycle[16]

[16] AJP 2.7

Chapter 3 NIIA ARCHITECTURE

3.1 Architecture Description

3.1.1. The original NIIA architecture was relatively simple, reflecting the technologies available at the time. With advances in technology and concepts of operations, the architecture has become more complex and complete. The key functional flow that is addressed by the NIIA can be divided into two parts. The first part is the input side of the data flow from the sensor into the exploitation function. The second part is the dissemination side of the process, providing the products of the ISR process to users. While the requirement for full interoperability on the sensor side is of less priority – with national policies often precluding the sharing of direct sensor data, the need to standardize the data is still very important as it lends itself to the ability to share the data more fully later in the processes.

3.1.2. While Figure 8 provides the connectivity and identifies the use of each standard in the functional flow of the ISR data, it does not provide a complete picture of the connectivity of each interface. The interfaces between the airborne segment and the ground segment (or another airborne segment) and the ground segment outputs are defined as the critical interfaces for coalition interoperability. The outputs of the sensor systems are provided via either Data Link,[17] Streaming Services, or Data Storage devices with the defined interface and the format of the transmitted or stored data defined by one of the data type standards. This “raw” data can be routed directly into a STANAG 4559 implementation and provided to the exploitation function where it is converted into ISR products. These products can consist of classical geospatial products (reports, maps, intelligence preparation of the battlefield, assessments, etc.) or they can be products such as support to time-sensitive targeting.

[17] Open Systems Interconnection (OSI) model defines data link as the carrier and is equivalent to OSI Layers 1-3 (Physical, Data Link, and Network) which are mainly hardware/software packages that provide the infrastructure. OSI Layer 4 (Transport) are the protocols that leverage the infrastructure to deliver data.

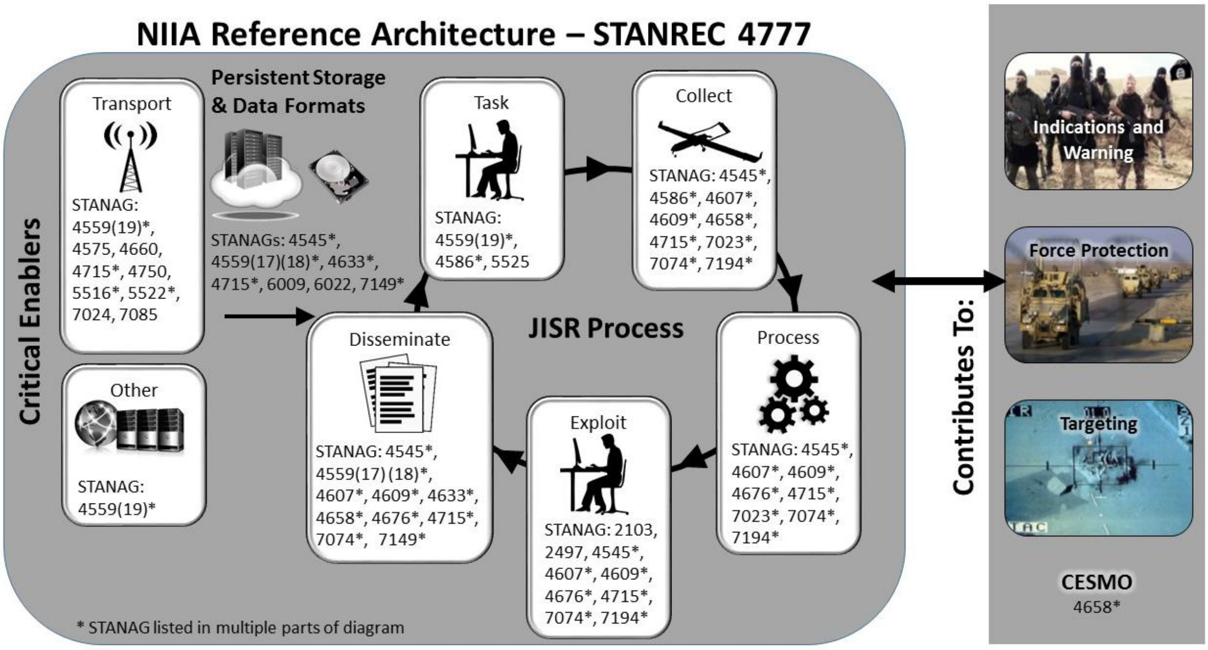

NIIA Reference Architecture – STANREC 4777
Critical Enablers
Transport
STANAG: 4559(19)*, 4575, 4660, 4715*, 4750, 5516*, 5522*, 7024, 7085
Other
STANAG: 4559(19)*
Persistent Storage & Data Formats
STANAGs: 4545*, 4559(17)(18)*, 4633*, 4715*, 6009, 6022, 7149*
Task
STANAG: 4559(19)*, 4586*, 5525
Collect
STANAG: 4545*, 4586*, 4607*, 4609*, 4658*, 4715*, 7023*, 7074*, 7194*
JISR Process
Process
STANAG: 4545*, 4607*, 4609*, 4676*, 4715*, 7023*, 7074*, 7194*
Exploit
STANAG: 2103, 2497, 4545*, 4607*, 4609*, 4676*, 4715*, 7074*, 7194*
Disseminate
STANAG: 4545*, 4559(17) (18)*, 4607*, 4609*, 4633*, 4658*, 4676*, 4715*, 7074*, 7149*
* STANAG listed in multiple parts of diagram
Contributes To:
Indications and Warning
Force Protection
Targeting
CESMO
4658*

Figure 8: NIIA Architecture with Key STANAGs

3.2. Interface Standardization

3.2.1. The key to defining any interface is the use of standards. Without standards, interfaces tend to be defined on an ad hoc basis producing stove-piped solutions that are not interoperable. In order to provide a complete JISR architecture, the NIIA implements both NATO STANAGs and some international standards based on recognized international standards bodies, such as the International Organization for Standardization (ISO) and the International Telecommunications Union (ITU). The STANAGs are developed by various NATO organizations under the Conference of National Armaments Directors (CNAD), Consultation, Command, and Control Board (C3B), and administered by the NATO Standardisation Organization (NSO). The standards adopted from other international standards are managed within that respective organization. However, since most of these other organizations do not address military requirements, a profile of the international standard is often required. The profile defines the application to the military situation, including particular parameters to be used and additional elements (such as security fields) that will be required.

3.3 Architecture Services

3.3.1. As noted above, a key to future operations will be the implementation of a SOA architecture. This type of architecture provides for the connectivity to allow user applications access to the data required to complete the function at hand without excessive user interaction. The applications can access data from a broad range of sources across the network. Many of the current applications that use the NIIA can be applied to a SOA structure.

3.3.2. Integrating ISR sensors into the SOA structure will require employment of Internet Protocol (IP)-enabled ISR Data Links. Sensors on the collection platform and the platform's ISR Data Link Terminal communicate via an IP router. This router receives packetized data from the sensors and forwards it to the ISR data link terminal encapsulated in Data Link Layer frames. At the opposite end of the radio link, the ISR data link terminal forwards the encapsulated IP packets to a second router which strips off the Data Link Layer framing if necessary and forwards the IP packets to exploitation systems, STANAG 4559-compliant ISR Libraries, and other ISR Libraries. Users can access the data via dedicated circuits or via a NATO communications network. This approach, which is illustrated in Figure 9, follows the NATO Architecture Framework (NAF), the NATO Interoperability Standards and Profiles (NISP), and extends the NATO Enterprise Architecture all the way to/from the real time collection mission and/or a disadvantaged user.

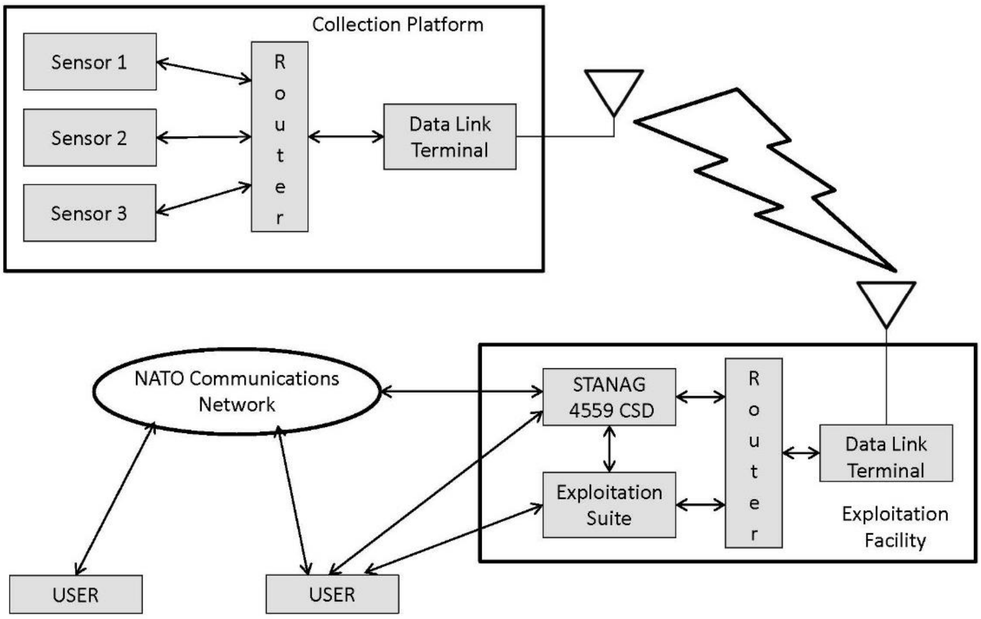


Figure 9: NATO Architecture Framework

3.3.3. All of the profiles identified in Edition 3 of STANAG 7085 are capable of transporting IP packets in the manner described above. Other links may be upgraded to function in the same way. These links include LINK-16/22 and the associated J-Series messages, as well as the Improved Data Modem (IDM) and STANAG 4660.

3.4 Metadata

3.4.1. A key element of JISR is metadata: 'data about data'. Metadata articulate a context for information resources of interest, which can be of manifold type and characteristic, such as plain documents, structured reports, services and schema definitions, sensor data and measurements, imagery, exploitation products, and geographical overlays.

3.4.2. Metadata should accompany all ISR data and products in order to support and enhance:

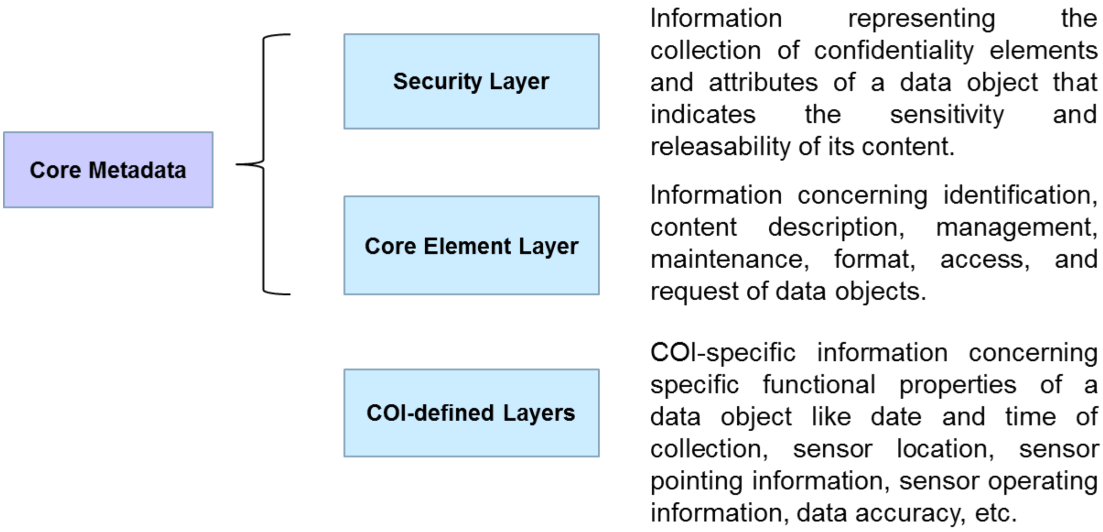
(1) Confidentiality and releasability marking,
(2) Dissemination, Archival, Search and Retrieval (DSAR), and
(3) Processing, Exploitation, and Dissemination (PED), including geospatial refinement.

3.4.3. Metadata can be organized and provided through dedicated metadata catalogues or registries, be embedded in the information resources themselves, or both.

3.4.4. Any data or service repository (library, storage) is normally associated with a metadata catalogue or registry, which serves the purpose of enabling metadata based search and assessment of the characteristics, usability and utility of stored information resources, and retrieving data, as needed, from the storage location. When stored and made accessible through ISR libraries, the published ISR data and products can be searched for through structured queries in the associated ISR library catalogue metadata cards, which usually provide a comprehensive, descriptive set of metadata for each library holding. Typical library catalogue specifications used within NATO are STANAG 4559 NATO Standard ISR Library Interface (NSILI), the Battlefield Information Collection and Exploitation System (BICES) Central Card Catalogue, or the NATO Core Metadata Specification.[18]

3.4.5. The NATO Core Metadata Specification (NCMS) denotes a simple delineation of three main metadata layers: a security layer, a core element layer, and COI-defined layers, as depicted in Figure 10.

[18] AC/332-D(2014)0010, “NATO Core Metadata Specification (NCMS).” 14 January 2015.



Information representing the collection of confidentiality elements and attributes of a data object that indicates the sensitivity and releasability of its content.

Information concerning identification, content description, management, maintenance, format, access, and request of data objects.

COI-specific information concerning specific functional properties of a data object like date and time of collection, sensor location, sensor pointing information, sensor operating information, data accuracy, etc.

Figure 10: Three Metadata Layers

3.4.6. The NCMS itself only deals with what it calls ‘Core Metadata’, and leaves the definition of Communities of Interest (COI) specific metadata to the individual COIs. The core metadata are essentially descriptive metadata about individual instances of application data (data objects), i.e. the actual data content and its sensitivity; a useful description of those metadata would be ‘data about data content’. The core metadata relate to such fundamental organizational and operational aspects like information security and releasability and how a data object is identified, described, managed, maintained, formatted, accessed, requested, or organizationally related to the operational Order of Battle (ORBAT).

3.4.7. A more specialized means of metadata application are metadata registries, as exemplified by the NATO Metadata Registry and Repository (NMRR).[19] The NMRR contains information that describes the structure, format, and definitions of data. In particular, the NMRR provides a consistent, controlled and reliable means to store, manage and access eXtensible Markup Language (XML) artefacts, including metadata and data specifications; and enables controlled registration, discovery and access to XML artefacts (e.g. XML, XSD), data specifications, allowable value lists, and service descriptions (e.g. WSDL). As such, it provides a mechanism for centralized configuration management, quality management and change control of the registered specifications and propagation of specification changes to the software applications affected. The NMRR supports the NCMS as the specification for its metadata cards.

3.4.8. In the NMRR, the term metadata has a twofold meaning, first the usual discovery, mostly descriptive metadata, and secondly, as structural metadata about the design and specification of actual data structures. A useful description of those structural metadata would be ‘data about the containers of data’, i.e. schema and service definitions, data base tables and records, data models, data formats, and message structures.

[19] “NATO Metadata Registry and Repository.” https://nmrr.ncia.nato.int/home.htm

3.4.9. Finally, the COI-defined metadata layers are dealing with the more functional aspects of COI application data, e.g. to provide auxiliary parametric data in support of further processing and exploitation of the source data; a useful description of those COI-defined metadata would be ‘data about data context’. They provide particularities of the data collection and put the data in a geographic, temporal and environmental context. Auxiliary parametric data enable further quantitative processing and advanced exploitation and concern such specific functional properties such as date and time of collection, sensor location, sensor pointing information, sensor operating information, and/or measurement accuracy.

3.4.10. Auxiliary parametric data are generally embedded and tightly entangled with the application data they are supporting. Normally, COI-specific applications need to be applied to utilize these specific parameters and establish the products to be delivered. Many of the ISR STANAGs contain a comprehensive set of embedded parametric metadata, to include STANAG 7023, STANAG 4609, or STANAG 4633. Some STANAGs also provide particular extensions in order to provide more comprehensive sets of auxiliary parametric metadata, such as STANAG 4545 SENSRB. Parametric metadata are normally not included as part of a library metadata card, which mainly focuses on general product information, or only selectively to inform about certain possibilities to further process the source data.

3.4.11. As the volumes of archived data and imagery grow to enormous volumes, metadata is becoming even more critical. Without consistent metadata, a consumer cannot efficiently search and retrieve the data that contain the characteristics and content necessary to support a required task or mission. The timely and consistent capture of metadata is fundamental to the quality of any data resource as a whole.

3.5 Geospatial Aspects of ISR

3.5.1. One important element of metadata is geolocation information. Geolocation information is needed in many contexts, such as geo-referencing or rectifying raw imagery, determining the location and error ellipse of intercepted signals, or delivering modern, high-accuracy ordinance on specific targets. Geolocation information should be provided as accurately and precisely as possible. As accuracy and precision are driven to a great extent by sensor design and capability, measures of uncertainty should accompany all geolocation metadata, such as information on random and systematic errors involved in location, pointing and timing measurements. If such information is missing, geolocation should generally be considered uncertain and derived coordinates should only be used for situational awareness.

3.5.2. Geolocation from imagery and other intelligence sources is a complex process and many factors are to be considered. One factor is that geolocation precision is also dependent on metadata precision. Therefore, metadata formats should enable transport of metadata at least one order of magnitude higher than the precision of the underlying sensor. Another factor for imagery is that the geolocation process normally involves projecting the look direction vector defined by the metadata to a surface model. Unanticipated or uncompensated elevation deviations can cause the intersection of the look direction vector with the surface model to error greatly. Whenever possible, designated ground control points or information should be used with all imagery in order to enhance the reliability of derived ground coordinates. Many of the MASINT sensors that produce image-like products function in the same manner as conventional imagery.

3.5.3. In addition to more rapid solutions to the target coordinates, the geometric diversity of the platforms also generally provides more precise coordinates. The MASINT sensors that produce Electronic Warfare/Signals Intelligence (EWSI[20])-like data are constrained in the same manner as the EWSI sensors.

3.5.4. A significant variation from the geospatial requirements is in the HUMINT community. The location of the target is a prime parameter in the IMINT, MASINT, and EWSI. Most data repositories for these data types are geographically-based, allowing for rapid searches for relevant data covering a specified area. Time is usually the second most important search criteria. For HUMINT, however, the most critical parameter is the human source, including the assessed reliability of the source. The actual location of where the source provided the information (e.g. café, private residence, library, street) is of minimal value. As such, HUMINT data repositories are usually organized by (source) individuals. Geospatial considerations are either part of the reported information if a location is of importance to the content of the information (e.g. the location and time that an individual could be found) or the location of the meeting is included as collateral information.

3.6 Coordination with Other Bodies

3.6.1. The NIIA is intended to be the basis of NATO ISR Interoperability. This concept requires coordination of the architecture with numerous organizations both within and external to NATO. Although most of the organizations are not concerned about the entire architecture, they all have interests and functional roles in some elements of the architecture. The following NATO organizations have ISR responsibilities that directly impact the architecture:

- BICES ISR WG. The BICES ISR Working Group aims to operationalize multinational ISR capabilities exploiting MAJIIC ISR technologies and national capabilities, with the goal to implement the full TCPED process on BICES system through building a standardized multinational global ISR construct.
- Bilateral Strategic Commands (Bi-SCs). Allied Command Operations (ACO) and Allied Command Transformation (ACT) serve as NATO's strategic commands with responsibility to develop and articulate requirements for the NATO Command Structure (NCS) and NATO Force Structure (NFS) which rely

[20] The Electronic Warfare and Signals Intelligence domains are defined in MC64 and MC101 respectively and are closely related. Both may provide actionable information from the electromagnetic spectrum.

on the capabilities of the NIIA.

- C3 Board (C3B). The C3B is the responsible agency for developing and managing command, control, and consultation development within NATO. This mandate includes communications links, C3 architectures, network security, spectrum management, encryption, electromagnetic compatibility, and many other topics that affect the NIIA community. The C3B is a parallel body to the Conference of National Armaments Directors (CNAD) and has a large subordinate structure to manage its diverse mandate.
- Federated Mission Networking (FMN). A key contribution to NATO's Connected Forces Initiative, FMN enables a rapid instantiation of mission networks by federating NATO organizations, NATO Nations and Mission Partner capabilities, thereby enhancing interoperability and information sharing.
- Joint Intelligence Working Group (JINTWG). This group is the parent organization for the JISRP and is responsible for the doctrine and Concept of Operations (CONOPS) for NATO operations.
- JISR Panel (JISP). This group is responsible for the operational aspects of ISR. Reporting through the Military Committee's Joint Standards Board, they have numerous standards under their purview including the tasking and reporting standards. They are also responsible for JISR concepts, and tactics, techniques, and procedures.
- JISR Project Group (JISR PG). The JISR Project Group was constituted under the new NATO Defence Planning Process (NDPP) to manage the delivery of ISR capabilities to operational forces. It is led by the JISR Capability Area Manager (CAM) and has the mandate to coordinate the work of groups and agencies working ISR issues throughout NATO, regardless of the normal reporting channels.
- Military Intelligence Committee (MIC – formerly the NATO Intelligence Board). This senior level committee approves the policies and concepts of operations for all intelligence matters in NATO. Consistency between the architecture and the associated policies and concepts is critical to long term implementation and operational success.
- NATO Communications and Information Agency (NCIA). NCIA's mission is to strengthen the Alliance through connecting its forces. NCIA delivers secure, coherent, cost effective and interoperable communications and information systems and services in support of C3 and enabling ISR capabilities, for NATO, where and when required.
- NATO Electronic Warfare Advisory Committee (NEWAC). The NEWAC is responsible for overseeing the development of NATO's electronic warfare policy, doctrine, and command and control concepts as well as monitoring electronic warfare support to NATO operations. The NEWAC is composed of representatives of each NATO Ally and of the Strategic Commands.
- There are also many non-NATO Organizations that have a role in the development of standards and policies that affect the NIIA. Examples include: ISO, International Civil Aviation Organization (ICAO), ITU, and Defence Geospatial Information Working Group (DGIWG).

Chapter 4 NATO STANDARDIZATION AGREEMENTS (STANAGs) /ALLIED PUBLICATIONS (APs)

4.1. The NIIA consists of three volumes and a number of other STANAGs and associated Allied Publications (APs). This document serves as the overarching guidance for the entire architecture, while each STANAG or AP provides more specific details for an element of the architecture. The STANAGs and APs are organized by number. To better understand where each STANAG fits in the NIIA, please refer to Figure 8. The summaries below are intended only as introductions for each document. Full details on the purpose and applicability of the document are included in the text of each individual STANAG or AP.

4.1.1. STANAGs 2103 and 2497 - Warning and Reporting and Hazard Prediction of Chemical, Biological, Radiological and Nuclear (CBRN) Incidents (2103 - Operators Manual and 2497 - Reference Manual)

The purpose of these STANAGs are to prescribe the procedures, information requirements and functional specifications for CBRN messaging that will contribute to the Warning and Reporting function. They include guidance for assessing and reporting CBRN threats, incidents and the resulting contamination. The culmination and reporting of this data and, ultimately, information includes sensor reporting, prediction and warning of hazard areas from CBRN incidents, contributing to the evaluation of CBRN information to complete the Common Operating Picture (COP), the transmission of advanced hazard warning of potential CBRN or Toxic Industrial Material (TIM) exposure and the exchange of relevant reports with Allied forces, including civil authorities and agencies.

In particular, STANAG 2103 specifies the operational view of the manual portion of the CBRN Warning and Reporting and Hazard Prediction function with respect to simplified and detailed procedures while STANAG 2497 is primarily for automated CBRN Command Information Systems (CIS). It will be used by system designers and software engineers, acquisition program managers, system architecture instructors for the operational users, and a variety of persons engaged in research and development activities. Additionally, STANAG 2497 provides reference material that support STANAG 2103 but it is not used on a daily basis by the warfighter.

4.1.2. STANAG 3377 - Air Reconnaissance Intelligence Report Forms

STANAG 3377 describes a set of formats for reporting and presenting intelligence information derived from air reconnaissance and airborne sensor imagery. They are intended to be used by the reporting agency to inform the tasking, requesting and interested agencies of the results of air reconnaissance missions. It covers specialised reports for time-critical reporting as well as formats for more routine reporting. Six different reports are currently described including in-flight reporting, reconnaissance exploitation reporting as well as reports for more specialised imagery such as Radar-based imagery. This is an older standard and currently the described formats are based on structured-text reporting mainly intended for human interpretation.

In the future it is likely that this standard will be updated to incorporate more modern technologies that are better suited to digital transmission and easier machine-to-machine use, storage and discovery. It may also be updated to include formats beyond the current scope of imagery.

4.1.3. STANAG 3596 - Air Reconnaissance Requesting and Target Reporting Guide

STANAG 3596 provides a common reference for the requesting, planning and reporting of intelligence from air reconnaissance. It describes a set of target categories (e.g. Airfields, Port installations) as well as a common set of characteristics or Essential Elements of Information (EEI) about each of those targets. It describes a simple nomenclature for both requesting information about, as well as reporting on: new targets, change detection, planning, and damage assessment. In doing so, it allows the tasking authority to specify which EEI are to be reported on a given tasking, and it allows the response to describe those EEI in a way that will be understood.

Elements of this standard (particularly the target category list) are used in a number of other NIIA standards. In the future it is likely that much of the content of this standard will be merged with STANAG 3920 as part of an effort to update and simplify the set of extant standards.

4.1.4. STANAG 3920 - Handbook for Air Reconnaissance Tasking and Reporting - ATP-47

STANAG 3920 brings together a broad set of information associated with the planning, tasking and reporting of air reconnaissance (but not technical data like imagery data formats). In addition, the standard contains reference data for use by the imagery analysts. It contains an overview of air reconnaissance, the reconnaissance cycle, types of air reconnaissance as well as considerations for requesting, tasking, planning, reporting, and battle damage assessment. It also includes guidance on a number of related standards, several of which are also included in the NIIA. There is a lengthy section in this document intended to provide details on each nations' reconnaissance systems, but many nations have not provided up-to-date information.

In the future it is likely that much of the content of STANAG 3596 will be merged into this one as part of an effort to simplify the set of extant standards. At the same time much of the content of this standard is likely to be updated to reflect wider changes.

4.1.5. STANAG 4545 - NATO Secondary Imagery Format (NSIF)

STANAG 4545 provides implementation guidance for the NATO Secondary Imagery Format (NSIF). NSIF is designed for the distribution, storage, and interchange of secondary imagery products (not designed for downloading raw products from a primary sensor). The document is identical to the U.S. National Imagery Transfer Format 2.1 (NITF 2.1) to ensure compatibility. This document allows multiple nations to be able to work together with imagery and its associated metadata. AEDP-04, the NSIF Implementation Guide, explains how to use the standard and provides information not necessary for a baseline file but that may be used to enhance the file. The Basic Imagery Interchange Format (BIIF), an international standard for imagery, developed in coordination with the ISO, is compatible with NSIF but with more flexibility for the larger international imagery community.

NSIF was developed with the use of extensions to enhance the standard's applicability, which are added to each file to allow for additional metadata that the baseline standard does not cover. Support Data Extensions (SDEs) include two types of extensions: the Tagged Record Extension (TRE) and the Data Extension Segment (DES). There are many groups of extensions, most importantly geospatial, aircraft, or commercial extensions. The list of NATO-approved SDEs are a subset of those approved for NITF 2.1. Future work will involve adopting changes to NITF 2.1 that will allow multiple geographical entity standards.

4.1.6. STANAG 4559 NATO Standard ISR Library Interfaces and Services

STANAG 4559 promotes interoperability of NATO ISR library interfaces and services for the exchange of shared ISR data, products and schemas. The STANAG is implemented when standard ISR library interfaces and services are incorporated into the Nations' systems in accordance with the requirements of one or more of AEDP-17, AEDP-18 and AEDP-19.

4.1.6.1. AEDP-17 - NATO Standard ISR Library Interface

The aim of AEDP-17 is to promote interoperability for the exchange of static NATO ISR products (like imagery, video, geospatial information, reports, metadata and other information). This AEDP specifies common software interfaces to be implemented and exists for all NATO interoperable library systems. The interfaces are based on CORBA or web service technology and provide electronic search and retrieval capabilities for distributed users to find products from distributed libraries in support of, but not limited to, rapid mission planning and operation, strategic analysis, and intelligent battlefield preparation. The AEDP provides means to support backward and forward compatibility.

This AEDP is part of STANAG 4559 which also contains AEDP-18 and AEDP-19.

4.1.6.2. AEDP-18 - NATO Standard ISR Streaming Services

The aim of AEDP-18 is to promote interoperability for the exchange of NATO ISR streaming data and products (like motion imagery or ground moving target indicator streams). The NATO Standard ISR Streaming Services provide standard interfaces for querying and accessing ISR streaming data and products through suitable applications maintained by NATO and NATO Nations.

AEDP-18 describes the Coalition Shared Dataserver (CSD) Stream Server and its interfaces. The CSD Stream Server is responsible for streaming data, i.e. data generated by sensors and which is periodically updated. The CSD Stream Server allows a sensor to declare that a stream is available and to provide periodic metadata updates, allows an exploitation system to query for recorded and live streaming data, and it allows an exploitation system to request the replay of recorded streaming data, or the relay of live streaming data. One CSD Stream Server may connect to other distributed CSD Stream Servers to provide a coherent coalition enterprise view, using metadata replication.

This AEDP is part of STANAG 4559 which also contains AEDP-17 and AEDP-19.

4.1.6.3. AEDP-19 - NATO Standard ISR Workflow Architecture

The aim of AEDP-19 is to promote interoperability for the exchange of NATO ISR process elements. The NATO Standard ISR Workflow Architecture provides standard interfaces for enabling JISR processes and exchanging JISR workflow elements through suitable applications maintained by NATO and NATO Nations.

The workflow architecture covered by this AEDP-19 covers the ISR enterprise wide sharing and management of:

- Intelligence Collection Plans,
- Requests for information and requests for ISR asset,
- Tasking of organic ISR assets,
- Linkage of collected and exploited products to requests, tasks and intelligence requirements, and
- ISR ORBAT including configuration information.

This AEDP is part of STANAG 4559 which also contains AEDP-17 and AEDP-18.

4.1.7. STANAG 4575 - NATO Advanced Data Storage Interface (NADSI)

STANAG 4575 defines the interface for Advanced Data Storage Technology (ADST) recording systems such as magnetic disks, disk arrays, Solid State Disk (SSD) or custom solid state memory. Its use makes it possible to connect any STANAG 4575-compliant Removable Memory Module (RMM) to any STANAG 4575-compliant ground system and transfer the data from the RMM to the ground system via a direct physical connection. It is a “Data Download Standard” interface that allows download of ISR data without requiring a specific technology or internal memory format. STANAG 4575 defines the physical interface as Ethernet and the command protocol to be Internet Small Computer Systems Interface (iSCSI). It supports legacy use of fibre-channel physical interface.

AEDP-06 is a companion document to STANAG 4575 that provides the detailed technical information for implementation of the STANAG and also provides implementation guidance and lessons learned from previous developments. This information is divided into discrete annexes: electrical and command protocol, file structure definition, and physical interface and connectors. The annexes provide the technical requirements, implementation guidelines, and specific technical details needed for implementation of the interface. Objectives for continuing improvement are to define the message interface in terms of a consistent and complete data model, capturing conceptual, logical, and physical details of the required information exchanges and the internal relationships among data elements. This data model definition, when mapped to widely-used data models within SOA, will lower the initial investment required for NATO Unmanned Aerial Systems (UAS) to implement the standard.

4.1.8. STANAG 4586 - UAV Control System (UCS) Architecture

The aim of STANAG 4586 is to promote interoperability among NATO Unmanned Aerial Systems (UAS), particularly among UAS Control Stations (UCS). This interoperability significantly enhances the war fighting capability of NATO forces, by increasing flexibility and efficiency in meeting mission objectives through sharing of assets and common utilization of information generated from Unmanned Aircraft (UA). STANAG 4586 addresses the interoperability requirement through two means: reference to existing NATO standards for mission information exchange, and definition of a Command and Control (C2) message set for directing the operation of the UA and its mission payloads. The C2 interface is defined in AEP-84. Associated Standards Related Documents (SRDs) are identified using the format AEP-84 and include guidance for implementation and conformance evaluation/validation.

Objectives for continuing improvement to AEP-84 are to define the message interface in terms of a consistent and complete data model, capturing conceptual, logical, and physical details of the required information exchanges and the internal relationships among data elements. This data model definition, when mapped to widely-used data models within Service Oriented Architectures (SOA), will lower the initial investment required for NATO UAS to implement the standard.

4.1.9. STANAG 4607 - NATO Ground Moving Target Indication (GMTI) Format

STANAG 4607 defines the data content and format for the products of GMTI radar systems and provides the mechanism to relay tasking requests back to the sensor system. The format is scalable to allow all types of radar systems to use the format and tailor the data flow to the capabilities of the sensor and the available communications channels. Smaller systems can use the basic capabilities of the format to transmit only moving target reports. Larger, more capable systems can use the same format for the moving target reports, and also provide High Range Resolution (HRR) data and other products of extended processing of the radar returns. The format is also designed to be encapsulated in other types of data files, allowing users with multiple data types to use the GMTI format for the GMTI data, and the other STANAGs for imagery, graphics, and/or text data, all within a common data stream. Extensions are being used to address gaps: the Releasability Extension, which would provide for consistency with other STANAGs in handling releasability designations, and the Target Centroid Extension, which would provide additional environmental data for large maritime and land-based multi-return target reports.

AEDP-07, the NATO GMTI Format Implementation Guide, provides both content and procedural advice for managing the STANAG's development, including a Register of Controlled Extensions and practical advice (derived from implementers' experience and agreed upon by the community) that goes beyond the technical specifications in the standard itself.

4.1.9. STANAG 4609 - NATO Digital Motion Imagery Standard

STANAG 4609, along with its associated AEDP-08, provides guidance for consistent implementation of Motion Imagery Standards to achieve interoperability in both the communication and functional use of Motion Imagery Data. STANAG 4609 documents the structure for data, which includes formats, encodings and containers, and the content of data, which includes common and application-specific information that populates these structures. The structure is based on commercial standards from Standards Development Organizations (SDO) and non-commercial standards developed to support governing organizations' specific activities. The content is principally based on non-commercial standards that support capability-based needs. Together the structure and content constitute motion imagery data that meets conformance to STANAG 4609.

4.1.10. STANAG 4633 - NATO Common ELINT/ESM Reporting Format

STANAG 4633, along with its associated AEDP-14, establishes a NATO common format for reporting Electronic Intelligence (ELINT) information. This flexible format enables reporting of information in three different formats, to include a basic information format, a detailed information format for parametric information, and an expanded parametric information format. Once implemented this format will streamline the input of this information and enhance the interoperability of NATO databases and sensor systems.

4.1.11. STANAG 4658 – Cooperative Electronic Support Measure Operations (CESMO)

STANAG 4658 exists to enable the warfighter to rapidly share and receive Electromagnetic Spectrum (EMS) threat information. Use of the EMS by modern systems such as Integrated Air Defence Systems (IADS), Low Probability of Intercept (LPI) radars, and digitally modulated communications systems poses a steadily increasing threat to today's warfighters.

Cooperative Electronic Support Measures Operations (CESMO) enables rapid coordination and fusion of data from EMS sensors, across an agile tactical network. STANAG 4658 defines a standardised message set to enable CESMO. This enhances the survivability of coalition forces and enables the efficient exploitation of the electromagnetic spectrum. Military benefits include contributions to Time Sensitive Targeting (TST), updates to the Theatre Specific Electronic Order of Battle (TS-EOB), and contributions to the JISR enterprise.

STANAG 4658 is associated with AEDP-13. AEDP-13 defines messages for sharing:

- Platform and collection equipment status
- Participant position reporting
- Sensor Line of Bearing (LOB) intercepts and locations of emitters including amplifying information such as identity (NATO Spot Number), affiliation, confidence, and emission parametric information.

4.1.12. STANAG 4660 - NATO Interoperable Command and Control Data Link (IC2DL)

STANAG 4660 is the response to the lack of line of sight datalink solution available on the shelf dedicated to the command and control of the tactical UAV (Unmanned Aerial Vehicle), MALE (Medium Altitude Long endurance) UAV, HALE (High Altitude Long Endurance) UAV and UCAV (Unmanned Air Combat Vehicle). STANAG 4660 defined the technical requirements for an interoperable command and control line of sight datalink for UAVs. AEP-77 provides additional details to define a standard Line Of Sight (LOS) IC2DL for Unmanned Systems that will facilitate and support NATO interoperability between heterogeneous unmanned systems.

The waveform is designed to comply with the NATO harmonized requirements (network capability, interface, data-rate, range) but take also into account airworthiness and frequency regulations constraints. Future improvements to STANAG 4660 will include the introduction of communication security capability and enhanced performance.

4.1.13. STANAG 4676 - NATO Tracking Data Standard (NITS)

STANAG 4676, and its associated AEDP-12, defines the format and content of track from a variety of ISR sources to enable the exchange of track data. This includes the ability to manage continuous and persistent tracks as sensors come online or go offline. STANAG 4676 also provides a core set of data descriptors that could be extracted or expressed from many forms of intel as tracks. Stubs are provided that will form the entry or touchpoint for different forms of data inputs (e.g. radar, ELINT, SIGINT); data can then be communicated as tracks in the context of another medium such as a single motion imagery frame or raster image. The result is a common format for tracks that is fusible with other tracks, exchangeable between systems (producers and consumers), and which is still able to communicate enough contextual information (images, object information) to aid the analyst in forensic examination and exploitation.

STANAG 4676 at present supports ground-based tracking and will be expanded to cover other forms of tracking such as airborne and space. In addition, the standard will harmonize other NATO ISR inputs to allow more types of tracks to be correlated with quantitative confidence levels, as well as to facilitate other aspects of military operations. The issues of binary encoding and track lineage/pedigree will be resolved before taking up more input types.

4.1.14. STANAG 4715 - NATO Biometrics Data, Interchange, Watch Listing, and Reporting Standard

STANAG 4715 was developed to provide a baseline for NATO national biometric systems to meet interoperability requirements through automated and seamless exchange of biometric data across disparate systems. Biometric data is uniquely identifiable information about a person such as fingerprints, facial image or iris image. This information is a powerful tool in the defence against terrorism by reducing the ability of the enemy to remain anonymous. Biometric collection devices and Automated Biometric Identification Systems (ABIS) deployed by member nations around the globe provide the means for sharing biometric information with other member nations. STANAG 4715 identifies a standardized data format for sharing biometric data for watchlisting and reporting. Future revisions to the STANAG will include additions to account for technological advancements in other biometric modalities such as speaker recognition and Deoxyribonucleic Acid (DNA) matching.

The STANAG 4715 supporting documents include the AEDP-15 to specify and define the biometric submission and response transactions. These transactions are well defined in a manner that the systems can determine how to match, store and share data. The Integrated Data Dictionary (IDD) also accompanies STANAG 4715 and provides definitions, defines values and cardinality and is the source of all data elements available for use in a biometric transaction.

4.1.15. STANREC 4750 - Advanced Data Storage Technology (ADST) Memory Systems Sanitization Guide

STANREC 4750 provides the recommendations for Removable Memory Module (RMM) sanitization in the associated AEDP-03. AEDP-03 is based on RMM use in ISR systems and implementation of the RMM using advanced memory devices. Technical details were coordinated with the U.S. National Institute of Standards and Technologies (NIST) and ISO documents.

AEDP-03 was developed as a companion document to STANAG 4575, the NATO Advanced Data Storage Interface (NADSI). AEDP-03 provides sanitization procedures and defines sanitization levels for storage media used in ISR acquisition and ground support systems. Sanitization is the process that makes the data unrecoverable from the media by any known means, and provides the technical basis for declassification. Declassification is the administrative process of certifying that no classified information exists on the media. Declassification policies, directives, and guidance are found in the NATO information security documents referenced in AEDP-03. AEDP-03 procedures are applicable to RMM which incorporate FLASH Solid State memory, and RAID/Magnetic Disk data storage systems that are used to store ISR data. AEDP-03 provides guidelines and two distinct procedures for sanitization and reuse of non-volatile solid state, and high density magnetic disks/RAID memory elements for the ISR user community. Sanitization times for these technologies, which incorporate large storage capacities, can be very long and AEDP-03 provides streamlined procedures that can greatly reduce this time.

4.1.16. STANAG 5516 - Tactical Data Exchange- Link 16

STANAG 5516 provides guidelines on how to ensure interoperable use of Link 16 Tactical Data Links (TDLs) to disseminate information. Link 16 employs the Joint Tactical Information Distribution System (JTIDS) and Multifunctional Information Distribution System (MIDS) data link terminals. Link 16 is a frequency-hopping, jam-resistant, high capacity data link. Operating on the principle of Time Division Multiple Access (TDMA), 128 time slots per second are allocated among participating JTIDS Units (JUs), time slots are organised into multiple functional Network Participation Groups (NPGs). Link 16 includes elements of Link 11/Link 11B (STANAG 5511) and Link 4A/Link 4C, while providing many new or improved capabilities, including voice. Link 16 is used for exchange of near-real-time tactical data among joined units. Link 16 provides nodelessness, improved security, increased data rate (throughput), increased volume and granularity of information exchange, reduced data terminal size, digitised secure voice capability, relative navigation, and Precise Participant location and Identification (PPLI). Link 16 is primarily an anti-air warfare tactical data link, although it supports all environment types. It supports a single network with a large number of units spread across multiple frequencies.

4.1.17. STANAG 5522 - Tactical Data Exchange-Link 22 NATO Improved Link Eleven (NILE)

STANAG 5522 specifies the Link 22 tactical message standard, which enhanced data exchange and provides a new, layered communications architecture to replace Link 11 (STANAG 5511). Link 22 is a NATO secure radio system that provides Beyond Line-of-Sight (BLOS) communications and is primarily used in the maritime environment. It interconnects air, surface, subsurface and ground-based tactical data systems, and is used for the exchange of tactical data among military units. It is designed to complement and interoperate with Link 16. Link 22's communications security (COMSEC) is provided by an integral encryption/decryption device inside the Link 22 system, called the Link-Level COMSEC (LLC). It uses the same electronic chip used by Link 16 and detects attempts to disrupt the network. The Data Link

Processing (DLP) is connected to, or is part of, the Tactical Data System (TDS), also known as Host System, which processes the received tactical messages and generates tactical messages for transmission in accordance with the unit's national requirements.

4.1.18. STANAG 5525 - Joint C3 Information Exchange Data Model (JC3IEDM)

STANAG 5525 addresses international interoperability of Command and Control Information Systems (C2IS) at all levels from corps to battalion, or lowest appropriate level, in order to support multinational (including NATO), combined and joint operations and the advancement of digitization in the international arena. Communities of Interest (COIs) have large amounts of data in different formats and use different technologies, resulting in different interpretation of information. Uncoordinated stovepipes of data within the NATO Enterprise, the Alliance and mission partners impede data sharing between systems and therefore have a high impact mission execution. STANAG 5525 covers the Multilateral Interoperability Programme (MIP) Joint Consultation Command & Control Information Exchange Data Model (JC3IEDM), which is an information exchange data model that provides a unified information structure and serves as a coherent basis for C2IS development and information exchange mechanisms. The model is a product of the analysis of a wide spectrum of allied information exchange requirements.

The JC3IEDM is evolving under a new initiative, the MIP Information Model (MIM), which enables better use of technology using a state-of-the-art modelling approach and offers greater flexibility with the generation of diverse exchange specifications. This model is the object of a parallel standardisation initiative, known as NATO Information Model (NIM), and provides further robustness and rigour with regard to readability, modularity, extensibility, semantic strictness, and model consistency - it represents a valuable contribution to service design for Federated Mission Networking.

4.1.19. STANAG 6009 - NATO Emitter Database (NEDB)

STANAG 6009 defines the NATO Emitter Database (NEDB) as the sole common NATO database for the exchange of parametric and related information on electromagnetic emitters. It also establishes the NATO Spot Number (NSN) system for verbally or electronically referring to and reporting emitters in NATO channels. The NATO Emitter Database Advisory Group (NEDBAG) will be the forum for the discussion and approval of changes, upgrades and the future development of the NEDB. noting that any matters of policy affecting the NEDB must be approved by the NATO Electronic Warfare Advisory Committee (NEWAC).

4.1.20. STANAG 6022 - Adoption of a Standard Gridded Data Meteorological Message (MET-GM)

STANAG 6022 defines a meteorological message for gridded meteorological data and to standardise the number of information digits and their meanings. The format can be used to pass data sets varying from coarse resolution, single-parameter data through to very high resolution, multi-parameter data depending upon specific data requirements and communications capabilities. The format may also be used to pass observed data from the field back to meteorological centres or higher headquarters. This enables users to receive gridded meteorological data for operational use in artillery fire control systems, CBRN Automated Warning, Reporting and Prediction Software, and various computer-based Battlefield (or Tactical) Decision Aids (BDAs).

4.1.21. STANAG 7023 - NATO Primary Imagery Format

STANAG 7023 defines a standard data format and transport architecture for the transfer of primary imagery between collection systems and exploitation systems. STANAG 7023 primary imagery is normally raw unexploited imagery, which typically includes lots of low level information about the sensor and the platform. It is not normally shared beyond the first exploitation system to receive it, instead being converted into alternative formats for further distribution.

STANAG 7023 defines a flexible self-describing format which includes specification of the data format methodology, the data content, the logical data format encoding, the transport architecture and the structure of the data packets. It can support mixed live streaming of multiple (up to 64) different and varied sensor sources as well as the auxiliary data needed to describe those sensors, the format of the data coming off them, and the properties of the collection platform itself. The standard can also ‘wrap’ (encapsulate) some other formats within the NIIA including STANAGs 4607 and 4609. STANAG 7023’s associated guide is AEDP-09. Historically it has been most widely used in fast jet reconnaissance and targeting pods, though other types of ISR collection systems have also used it. This standard is stable and mature and no significant changes are currently planned for the future.

4.1.22. STANAG 7024 - NATO Imagery Air Reconnaissance Tape Recorder Standard

WARNING: This is a legacy standard, and it is not expected that any new air reconnaissance systems will specify STANAG 7024 tape recorder standards.

STANAG 7024 details a number of standard cassette and data formats for several different types of cassette tapes. This allows data recorded on one machine to be replayed on another that conforms to the same relevant part of this standard. Originally developed at a time when magnetic tape was a leading recording technology, STANAG 7024 formats are now only likely to be seen in legacy equipment. The standard described four separate physical tape formats, with the data format on the tape being either STANAG 7023 format or analogue data. There is an associated guide to this standard, AEDP-11, which contains advice on tape handling and storage.

No changes to this standard are expected in foreseeable future and use of this standard is rapidly declining. New systems which still require a physical method of data transfer should look to use STANAG 4575 which provides a more appropriate and modern interface. The status of this STANAG is to be reviewed in 2020, which may result in its removal from the NIIA.

4.1.23. STANAG 7074 - Digital Geographic Information Exchange Standard (DIGEST)

WARNING: This is a legacy standard and is no longer actively maintained.

STANAG 7074 enables the transfer of Digital Geographic Information between geographic information systems, and formed the baseline for both system developers and national geospatial data production activities. DIGEST was designed as a comprehensive 'suite of standards' capable of supporting the exchange of digital geographic raster, matrix and vector data among producers and users. Since the early 1990s, DIGEST-compliant datasets were produced and exchanged by numerous nations on CD-ROM to support a variety of military and civilian applications. The standard addresses data structures (spatial and metadata), feature and attribute coding schemes, format, exchange media and administrative procedures. This includes sections on how to incorporate geographic data into other data formats, most notably STANAG 4545.

DGIWG is currently working on a new generation of data standards, supported by network protocols and geospatial web services that will facilitate a broader sharing and use of geospatial information across the defence and civil sectors. While DIGEST is still widely used there are no plans to revise or amend any of the standards which form the DIGEST. The DIGEST standards, or parts of, that are required by specific communities to support legacy implementations may be extracted and managed separately by that community in consultation with the DGIWG.

4.1.24. STANAG 7085 - Interoperable Data Links for ISR Systems (NR)

STANAG 7085 removes the limits to interoperability that arise through the use of dedicated, proprietary data links to support ISR sensor systems. STANAG 7085’s solution is to describe a limited number of interoperable data link profiles. Each profile describes a unique combination of all data link waveform parameters with exception of a small set of variable mission parameters including forward link and return link centre frequency, pseudo-noise code, fallback timeout interval (time interval between loss of link and attempting to reinstate the link using fallback parameters), and COMSEC key indices. Current profiles are based on either the U.S. Standard Common Data Link (STD-CDL) or the European Telecommunications Standards Institute (ETSI) Digital Video Broadcast – Digital Satellite News Gathering (DVB-DSNG) Based Data Link (DSDL) Systems. STANAG 7085 profiles provide data rates from 200 Kb/s and 274.176 Mb/s to support a wide range of ISR missions. All current profiles are capable of conveying Internet Protocol (IP) packetized payloads. AEDP-10 contains implementation guidance for STANAG 7085 as well as security classification guidance, and test and certification guidance.

Future improvements to STANAG 7085 will include the addition of more frequency efficient waveforms based on the U.S. Bandwidth Efficient CDL (BE-CDL) and the ETSI Second Generation Digital Video Broadcast (DVB-S2). In addition, future editions will seek to incorporate recent advances in diplexer design as well as recommendations for remote video terminal operation and operation in severe multipath environments.

4.1.25. STANAG 7149 - APP-11 NATO Message Catalogue

STANAG 7149 provides users, system developers and Message Text Format (MTF) managers with the library of NATO messages, the instructions for their use and the associated XML schemas for each message. The use of formatted messages, as contained in the catalogue, is mandatory for all NATO forces exchanging character-orientated messages. All messages are bearer agnostic and can be sent in either of two protocols, simple text suitable for teletype, legacy systems, low bandwidth environment and cyber security or as XML instances. Protocols can be switched, using suitable software, during the transmission process, with no loss of data; it can be particularly beneficial to use plain text in low bandwidth environments or to traverse security gateways which may block XML.

As the compendium of formatted messages, APP-11 is referenced by many other strategic, operational and tactical publications where there is a need to exchange character oriented messages. Direction from the NSO is that message formats contained in other APs should be migrated to APP-11. A new edition of APP-11 is produced every three years with annual versions to accommodate new and updated messages. As new character-based technologies emerge and are adopted by NATO, APP-11 will be updated in accordance with the current edition of ADatP-3.

4.1.26. STANAG 7194 - NATO Imagery Interpretation Rating Scale (NIIRS)

STANAG 7194 promotes interoperability for the exchange of data between JISR collection management activities, imagery exploitation, and imagery capabilities. The NIIRS allows for the evaluation of imagery quality for all kinds of imagery, applicable for still and motion imagery for the different technical sensors types and use of a consistent measure for such evaluations. The NIIRS consists of 10 graduated levels, from 0 (poor quality) to 9 (high quality), with several interpretation tasks or criteria for each level. The NIIRS defines the levels of image interpretability by the types of tasks an analyst can perform with imagery of a given rating level. In general, ratings that are applied to an image are the average of individual assessments from various locations in the image. In particular, if an image has significant variation in resolution, dynamic range, or noise level, average values should be determined carefully to ensure an accurate representation of the overall image. In addition, if a characteristic is clearly visible at one level, but the next level is not achievable, an intermediate rating, based on the analyst’s judgment, using a single decimal value between the integer values can be applied (e.g. NIIRS 7.5). Nations must apply and use the NIIRS tables and the assigned values in this publication when submitting imagery collection requests;

exploiting and analysing the collected imagery; and archiving imagery products. This NIIRS standard does not apply to full motion video.

4.2. Other Documents

4.2.1. Many other documents are useful for participants in the ISR community. These include Military Committee (MC) documents, other STANAGs and Allied publications, draft STANAGs and commercial standards. Note that the Allied Joint Publication (AJP) series of documents provides most of the policy and doctrinal references. The AJP series uses a numbering system where the first digit corresponds to the J-function code (e.g. 2 for intelligence, 3 for operations)

- ATP-26 – Air Reconnaissance Intelligence Reporting Nomenclature – ATP-26 is not produced as a formal published text. It is a hyperlinked software application that allows analysts of intelligence sensors to identify objects of interest in a consistent manner. It breaks potential targets into gross categories (bridges, buildings, vehicles, etc.) and then allows the analyst to select specific features of the object to refine the description to a precise, consistent identification of the objects.

- Ethernet – Ethernet is the most common wired networking protocol in the world. Computer interfaces and cabling are readily available in most parts of the world as well. Ethernet supports data transfers up to 1 GB per second and is scalable to adapt to the network characteristics. While the standard has not been adopted as a NATO STANAG, the commercial standard is recognized and adopted in the NATO C2 Architecture.

- MC 0515 – SEWOC Implementation Concept – This document defines the concepts of operation for the SIGINT EW Operations Centre (SEWOC). This centre is the focus of analysis of SIGINT and EW information. The centre can be established at almost any echelon of command.

- MC 0596 – NATO IMINT Policy – This document informs senior commanders how their intelligence staff should work to support their decision-making and provide a principal reference document for intelligence specialists an explanation of NATO IMINT functions. This doctrine will expand on the NATO Imagery Intelligence Policy.

- MC 0582 – NATO Joint ISR Concept – The Joint ISR Concept defines how the intelligence function fits within the larger context of the ISR support to operations. It integrates the J-2 with J-3, J-5, and J-6 functions of the headquarters.

- STANAG 2190 – Allied Joint Intelligence, Counter-Intelligence, and Security Doctrine (AJP-2) – AJP-2 is the capstone document for defining the policies and doctrine for the intelligence, counter-intelligence, and security forces in NATO.

- STANAG 2191 – Intelligence Procedures (AJP-2.1) – AJP-2.1 provides the top level procedures for intelligence operations in NATO.

- STANAG 2490 – Allied Doctrine for Joint Operations (AJP-3) – AJP-3 is the top level capstone document which defines operations in NATO.

- STANAG 4716 - NATO Standardization of MASINT Reporting – This draft document provides a single, common format for reporting intelligence from MASINT sensors. Because of the wide variety of sensors contained in the MASINT discipline, a common report must be flexible. The standard structure provides a set of common metadata for all sensors that are included in the beginning of the format, and then optional specific metadata that provides the data elements for each type of sensor.

- STANAG 4774 – Confidentiality Label Syntax – This draft document provides common XML-based formats and syntax for security policies and confidentiality metadata. Information objects and data assets can be labelled to support access and release decisions in a manner that is understandable to all coalition partners. It provides the semantics for a common security policy based on agreed NATO Security Policy and supporting directives.

- STANAG 4778 – AdatP-4778 Metadata Binding Mechanism – This draft document provides methodology for associating metadata to data.

- STANAG 4789 - Sensor Integration Standard for NATO JISR Operations – This draft STANAG provides the technical details for developing a capability that provides for the integration of a wide variety of intelligence standards. It provides for the rapid linkage of sensors into a common reporting network, and the automatic polling and reporting of sensor data. The data can then be displayed on a common display. STANAG 4789 is based on Open Geospatial Consortium (OGC) standards that are referenced as the authoritative documents.

- STANAG 7107 – Reconnaissance and Surveillance Support to Allied Joint Operations (AJP-2.7) – AJP-2.7 is a recent addition to the AJP series, converting a previous Allied Tactical Publication (ATP-61) into part of the Allied Joint doctrine. The document provides the procedural aspects of the ISR support to operations. Planned updates to the document will include a better alignment with the Joint ISR Concept (MC 0582, see above).

- Study on NATO Implementation of the Improved Data Modem (IDM) – This study is examining the potential of using the commercial Improved Data Modem protocol as a NATO standard. IDM is a low cost alternative to the Link-16 tactical data link and is used by many nations, particularly for ELINT and ESM information. If used in conjunction with Link-16, a conversion and linkage node is required to connect the two separate networks.

- TCP/IP – The Transmission Control Protocol/Internet Protocol (TCP/IP) consists of a suite of standards to manage data transfer over the Internet or private networks. The suite of standards is defined in numerous commercial standards and there is a wealth of information available both on the Internet and in published books. This suite consists of the following protocols, among others: File Transfer Protocol (FTP), the protocol most often used to download files from the Internet; Telnet, which enables connection to mainframe computers over the Internet; Hyper Text Transfer Protocol (HTTP), which delivers Web pages; and Simple Mail Transfer Protocol (SMTP), which is used to send email messages.

- UDP – The User Datagram Protocol is a much simpler version of the Transmission Control Protocol. Used with IP, UDP provides for the transfer of data form one computer to another, but does not include the complexity to ensure that all packets of the data are received or that they are received in the correct order. Users of UDP provide these services at the application level and thus save on transmission overhead. The only additional provisions provided by UDP over the basic IP protocol are data check-summing and multiplexing by port number. Users requiring additional transfer protocol capabilities should use TCP.

AEDP-02 Volume I (B)(1)