

NATO STANDARD

AJP-6

ALLIED JOINT DOCTRINE FOR COMMUNICATION AND INFORMATION SYSTEMS

Edition A Version 1

FEBRUARY 2017



NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

**Published by the
NATO STANDARDIZATION OFFICE
© NATO/OTAN**

INTENTIONALLY BLANK

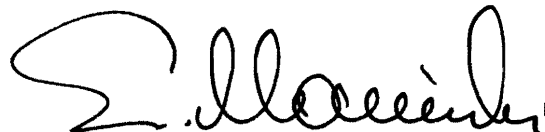
NORTH ATLANTIC TREATY ORGANIZATION

NATO STANDARDIZATION OFFICE

NATO LETTER OF PROMULGATION

28 February 2017

1. The enclosed Allied Joint Publication (AJP)-6 Edition A, Version 1, ALLIED JOINT DOCTRINE FOR COMMUNICATION AND INFORMATION SYSTEMS, which has been approved by the nations in the Military Committee Joint Standardization Board, and is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 2525.
2. AJP-6 Edition A, Version 1, is effective upon receipt and supersedes AJP-6, which shall be destroyed in accordance with local procedures 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 or partner nations, or NATO commands and bodies.
4. This publication shall be handled in accordance with C-M(2002)60.

A handwritten signature in black ink, appearing to read 'Edvardas MAŽEIKIS', with a large, stylized initial 'E'.

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

TABLE OF CONTENTS

Preface	ix
 Chapter I – Overview of Communication and Information Systems	
Introduction	1-1
Communication and Information Systems Terms	1-1
Communication and Information Systems Principles	1-5
Communication and Information Systems in Support of Command and Control	1-16
Overall Structure of Communication and Information Systems	1-17
Interoperability Aspects of Communication and Information Systems	1-22
 Chapter II – Roles and Responsibilities	
Introduction	2-1
Member Nation Responsibilities	2-1
Strategic Level Roles and Responsibilities	2-1
Operational Level Roles and Responsibilities	2-6
 Chapter III – Communication and Information Systems Planning	
Introduction	3-1
Strategic-level Planning	3-1
Operational-level Planning	3-1
Nature of Communication and Information Systems Planning	3-2
CIS Planning Activities	3-4
Other Considerations	3-13
 Chapter IV – Employment of Communication and Information Systems	
Command and Control Environment	4-1
Command Facilities	4-1
Communication and Information Systems	4-2
Exercises	4-4
Predeployment and Deployment Considerations	4-4

Annexes

A	North Atlantic Treaty Organization Architectural Framework Considerations	A-1
B	Joint Consultation, Command and Control Interoperability	B-1
C	Structure and Responsibilities for Spectrum Management in the North Atlantic Treaty Organization	C-1

Lexicon

Part I – Acronyms and Abbreviations	LEX-1
Part II – Terms and Definitions	LEX-3

Reference Documents	REF-1
----------------------------	-------

PREFACE

0001. **Scope.** Allied Joint Publication (AJP)-6 is a “keystone” publication directly subordinate to AJP-01, Allied Joint Doctrine. It provides the overarching doctrinal guidance to integrate communication and information systems (CIS) into Allied joint operations across the range of Allied operations and missions. It describes the characteristics of CIS, the overall structure of CIS, roles and responsibilities for CIS, command and control of CIS, and CIS security (to include cyber defence). It further provides a joint force commander (JFC) with the guidance and information necessary to establish effective CIS in, and for, an Allied joint force.

0002. **Purpose.** This publication has been prepared under the direction of the NATO Standardization Office/Military Committee Joint Standardization Board. It sets forth joint doctrine to govern the activities and performance of NATO forces in operations and provides the doctrinal basis for coordination among NATO, NATO nations, and non-NATO entities. It provides military guidance for the exercise of authority by JFCs and prescribes joint doctrine for operations and training. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the accomplishment of the overall objective.

0003. **Application.** AJP-6 is intended primarily as guidance for NATO forces at the operational level, and provides a useful framework for, operations conducted by a coalition of NATO nations, partners, stakeholders, non-NATO nations, and other organizations.

0004. Allied Administrative Publication-47, Allied Joint Doctrine Development, covers the development of AJP.

INTENTIONALLY BLANK

CHAPTER 1

OVERVIEW OF COMMUNICATION AND INFORMATION SYSTEMS

0101. Introduction

- a. Properly used and protected, modern communication and information systems (CIS) offer the joint force commander (JFC) significant advantages in information sharing, situational awareness, and command and control (C2) execution.
- b. CIS enable the commander to plan, execute, and monitor operations and exercises.
- c. Per Allied Joint Publication (AJP)-3, Allied Joint Doctrine for the Conduct of Operations, centralized planning and decentralised execution are key principles of North Atlantic Treaty Organization (NATO) operations. To enable implementation of these principles, a joint C2 structure that is understood at all levels is required to facilitate the clear, timely, and secure distribution of guidance/orders, situation reports, and coordinating information. Because the structure of a NATO-led force will likely be joint and combined in nature (and may include the characteristics, doctrine, procedures, equipment, and policies of each of the supporting components, host nation, and possibly non-NATO entities¹), contributing capabilities to a coalition should be considered.

0102. Communication and Information Systems Terms

- a. **Communication and information systems** is the collective term for communication systems and information systems [Allied Administrative Publication (AAP)-6, 2014].
- b. **Communication** is the imparting or exchanging of information by speaking, writing, or using some other medium. Communications are the means of sending or receiving information, such as telephone lines or computers (Oxford Dictionary).

¹ Non-NATO entities are defined in AC/35-D/1040-REV6, Supporting Document on Information and Intelligence Sharing with Non-NATO Entities, Annex 1, 21 August 2014. It includes contractors on operations, exercises, and transformational activities; governmental organizations; host nations; international organizations; non-governmental organizations; non-NATO multinational forces; and non-NATO nations.

- c. A **communication system** is an assembly of equipment, methods, and procedures and, if necessary, personnel, organized to accomplish information transfer functions [AAP-06, 2014].
- d. **Information** is knowledge concerning objects (e.g., facts, events, things, processes or ideas, and concepts) that, within a certain context, have a particular meaning. Information may be used in the production of intelligence, situation awareness, or every type of data (e.g., operational, and logistical) which need to be exchanged during a military operation.
- e. **Information management** (IM) is a discipline that directs and supports the handling of information throughout its life-cycle - ensuring it becomes the right information in the right form and of adequate quality to satisfy the demands of an organization.² The IM Plan directs the exchange of information in support of the chain of command by specifically describing how relevant information is to be managed both internally and externally. To ensure effective C2, a high degree of operational information exchange is required - both vertically and horizontally - between increasing varieties of entities. In order to effectively exercise C2 over assigned NATO forces, there must be an effective and appropriate exchange of information between cooperating forces and/or headquarters (HQ). The IM Plan assigns IM responsibilities to specific staff, describes information requirements, and provides command guidance with respect to information currency requirements and information protection needs. The IM Plan prescribes exactly “what” the information needs of the formation are, while the communications plan focuses on “how” the information needs are to be achieved. Coordination of the IM and communications plans ensures that all relevant C2 services required to support of the mission are identified, and adequate planning and provision of C2 services can be achieved. The production of a communications plan must be based upon the early receipt of key IM deliverables including:
 - (1) **Information services requirements.** Information services requirements consolidate the information services required to support the IM Plan. Information services generally fall into one of four categories (data, video, voice, and web) delivered in either secure or non-secure form. Voice services (e.g., radio and telephone) are largely standardized; however, care must be taken when considering video and data services since the technical requirements for delivery vary between services. Information services requirements must also indicate the prioritization of

² For additional information on the information life-cycle, refer to C-M(2007)0118, NATO Information Management Policy, 11 December 2007.

services for use in systems deployment, management, and restoration.

- (2) **Information exchange requirements** (IERs). IERs define the need for information exchange between two or more parties that support a given process. IERs describe the source and destination of the information flow, the content, and usually a number of other information flow characteristics (e.g., format, security classification, releasability, size/volume, performance requirements, and content and context attributes). IERs are pivotal inputs to the CIS planning process. They ensure all relevant C2 services required in support of the mission are identified, and adequate planning and provision of C2 services can be achieved. IERs in the form of orders and reports also reflect the exchange of information products in support of the chain of command. In order to effectively exercise C2 over assigned NATO forces, there must be an effective and appropriate exchange of information between cooperating forces and/or HQs.

- f. In CIS terms, a **system** is an integrated set of functions to support a capability - together with their materiel elements (personnel and other resources). The scope and boundaries, by which a system is described, while never fully or rigidly defined, are usually denoted by a set of related operational support functions and established through one or more capability packages. The implementation of a system (or components thereof) is the contributory elements of a fielded capability [AC/322-D(2008)0031-REV1, NATO CIS Policy to Support Capability Management, version 1.3, 2 April 2009].

- g. An **information system** is an assembly of equipment, methods and procedures and, if necessary, personnel, organized to accomplish information processing functions [AAP-06, 2014].

- h. A **service** is a capability provided to benefit or support communities of users [Military Committee Memorandum (MCM)-0032-2006, NATO Network-Enabled Capability (NNEC) Vision and Concept, 19 April 2006].

- i. An **architecture** is the fundamental organisation of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution [NATO C3 System Architecture Framework, version 3.1].

- j. In a service-oriented architecture, **functions** are defined as independent services with well-defined interfaces. They can be used separately or in

defined sequences [MCM-0038-2005, Development of a NATO Network-Enabled Capability (NNEC)].

- k. **Interoperability** refers to the ability to act together coherently, effectively, and efficiently to achieve Allied tactical, operational, and strategic objectives [AAP-06, 2014]. It also refers to the condition achieved among CIS or items of CIS equipment when information or services can be exchanged directly and satisfactorily between them and/or their users.
- l. **Information assurance** is the protection and defense of information and information systems by ensuring their availability, integrity, and confidentiality [MCM-0032-2006, NATO Network-Enabled Capability (NNEC) Vision and Concept, 19 April 2006].
- m. **CIS security** is an element of information assurance, and consists of the application of security measures for the protection of communication, information, and other electronic systems; and the information that is stored, processed, or transmitted in these systems with respect to availability, integrity, authentication, confidentiality, and non-repudiation. It includes defensive measures to counter cyber attacks and mitigate their effects, preventive CIS security measures, and user awareness as cyber defence.
- n. **NATO Network Enabled Capability**. The Alliance's technical ability to federate the various components of the operational environment, from the strategic level (including NATO HQ) down to the tactical levels, through a networking and information infrastructure [MCM-0038-2005, Development of a NATO Network-Enabled Capability (NNEC)].
- o. **Mission networks** provide a governed single instance of capability, including the CIS, management, processes, and procedures created for the purpose of an operation, exercise, training event, or interoperability verification activity.
- p. A **Federation** is an association of NATO, NATO nations, and non-NATO entities participating in missions, each retaining control of their own capabilities and affairs while accepting and complying with the requirements as laid out in the pre-negotiated and agreed arrangements [MCM-0125-2012, Future Mission Network Concept, 21 November 2012; and C-M(2015)0003, NATO Federated Mission Networking Implementation Plan (NFIP) version 4.0 Volume 1, 21 January 2015].
- q. A **Federation of Systems** is a set of systems connected or related so as to produce results unachievable by the individual systems alone, that is

managed without central authority, being the individual systems independently managed and having a purpose of their own [Euro-Atlantic Partnership Council (AC/322-D(2006)0002-REV1-ADD1)]. It should be noted that the lack of centralized system authority increases the requirement for detailed and sustained coordination between the managers of the individual systems. In particularly dynamic operating environments, the colocation of system management will facilitate continuous interaction and synchronization of efforts.

- r. CIS are **federated** when made up of the aggregation of multiple independent CIS that have different technical, procedural, or security characteristics. These component systems are established and operated independently; however, they follow agreed to standards and protocols for executing the proper operation of the overarching CIS as a whole.
- s. **Federated Mission Networking**³ is the Alliance's approach to unifying coalition networks to provide information exchange services, enable information sharing among mission partners, and guide the establishment of mission network relationships between NATO, NATO nations, and non-NATO entities in which to conduct the full range of operational activities within NATO-led operations.
- t. Services are classified and described using AC/322-N(2012)0092-AS1, Consultation, Command and Control (C3) Classification Taxonomy, 19 June 2012. The **C3 Classification Taxonomy** provides a tool and common language to synchronize and improve life-cycle activities for NATO's C3 capabilities by connecting NATO's strategic concept and political guidance through the levels of ambition expressed in the NATO Defence Planning Process to traditional CIS architecture and design constructs.
- u. **Service management and control (SMC)** enables users to manage, control, and monitor services in all layers of the network-enabled enterprise based on centralized and de-centralized business models, and provides the user with interfaces to implement, enforce, and monitor SMC policies [AC/322-N(2012)0092-AS1, Consultation, Command and Control (C3) Classification Taxonomy, 19 June 2012].

0103. **Communication and Information Systems Principles.** Information is a critical enterprise asset, and supporting CIS and services are essential to the proper conduct of C3. NATO and its Allies rely on the use of CIS to share information

³ For additional information, refer to MCM-0125-2012, Future Mission Network Concept, 21 November 2012; and MCM-0106-2014 (REV 1), NATO Federated Mission Networking Implementation Plan, 14 August 2014.

and function effectively. This reliance on CIS calls for a number of principles that allow NATO and its Allies to harvest the benefits of technology, and also deal with the associated risks and the complexity of exercising information-heavy operations.

- a. **CIS Strategic Principles.** In the context of NATO C3, crisis management, and NATO-led operations, the C3 Board articulated vision is to have mission-wide, secure, resilient, interoperable, valued C3 capabilities and CIS underpinning the NATO Strategic Concept. On this basis, the following strategic principles should be applied:⁴
- (1) Enable seamless flows of information between static and deployable CIS (DCIS) elements for the conduct of operations.
 - (2) Support the shift of focus from delivery of C3 capabilities to information and communications technology services provision.
 - (3) Apply a life-cycle approach.
 - (4) Integrate and satisfy short-, mid-, and long-term C3 requirements for translation into information and communications technology services in a coherent way. Optimize roles and responsibilities, structures, and processes.
 - (5) Emphasize the need for a dialogue between users and requirement holders at all life-cycle phases and particularly during implementation.
 - (6) Address interoperability between C3 capabilities and information and communications technology services provided by nations, and multinational or common funded programmes prior to deployment.
 - (7) Support all information security levels and multiple communities of interest (COIs).
 - (8) Support activities of collective defence in cyberspace.
 - (9) Employ prioritized provisioning according to adopt, buy, or create, whereby priority is given first to adopting what is already owned, followed by buying off-the-shelf, and only creating new as a last resort.

⁴ For additional information, refer to C-M(2014)0016, Alliance C3 Strategy.

- (10) Establish an enterprise architecture discipline.
- b. When employed in a Federated Mission Networking (FMN) environment, mission network CIS should also comply with the following principles: cost effectiveness; maximum reuse; reflect NNEC tenets; reflect C3 taxonomy; incremental approach; support an uncertain future; use network standards; support dynamic federations; and be information centric.⁵ A mission network is established using a flexible and tailored set of non-materiel (i.e., policy, processes, procedures, and standards) and materiel (i.e., static and deployed networks, services, and supporting infrastructures) contributions provided by NATO, NATO nations, and non-NATO entities.
- c. **CIS characteristics.** To satisfy the strategic principles in an efficient and effective manner, CIS should comply with a number of general characteristics. In general, CIS should be:
- (1) **Capable.** CIS should be specified, designed, implemented and operated so that it is able to meet the commander's IERs. To avoid impairing or slowing decision-making processes, care should be taken to ensure sufficient CIS functionality is made available to support the commander's information processes, and that the associated capacity is scaled so it meets the totality of the IERs.
 - (2) **Interoperable.** Effective joint and multinational operations require interoperable CIS that enable the JFC and subordinate commanders to exercise effective C2 between force elements. In ascending order, the levels of standardization are compatibility, interchangeability, and commonality. The same holds for interoperability within a coalition operation. The following facilitate interoperability:
 - (a) Developing joint and coalition force CIS concepts within a NATO-led mission.
 - (b) Harmonizing the information, semantics, and development of data management.
 - (c) Providing and implementing agreed operational, procedural, and technical standards within a NATO-led mission or exercise.

⁵ For additional information, refer to MCM-0106-2014 (REV 1), NATO Federated Mission Networking Implementation Plan, 14 August 2014.

- (d) Delivering information and services to other force elements.⁶ Within a NATO-led coalition with non-NATO entities, the delivery of services and information is dependent on the mission or exercise; defined relationships and the ability of participants to operate CIS and other material and non-material capabilities within the same mission or exercise; and the specific classification and releasability levels.
 - (e) Establishing common training and exercises for NATO, NATO nations, and non-NATO entities.
- (3) **Agile.** Agility ensures that CIS resources can respond dynamically to changes in scales of effort, operational tempo, posture, and outages. It is required to meet changing situations and diversified operations with minimum disruption or delay. For example, while changes in posture (e.g., from peacekeeping to peace enforcement) may result in minor changes to force structure, they could result in a considerably different CIS requirement. Agility is achieved through development and rehearsal of contingency plans (CONPLANS), use of commercial systems and infrastructure, mobile and transportable CIS equipment, freedom of manoeuvre within the electromagnetic environment, reserve capability, standardized processes and services, and making use of alternative means. Agility allows CIS to be readily integrated into plans and operations and supports information exploitation, which is necessary for an organization to rapidly identify changing IERs, business processes, and changes to the operational context.
- (4) **Scalable.** Scalability refers to the ability of CIS to accommodate changes in required size and quality. CIS scalability allows an entity to adapt to a continuum in the size of operations that can be executed using a number of core and augmentation CIS assets. Alliance operations typically follow a number of predefined templates. Scalability provides the flexibility to attend to those varying needs with a single pool of resources. Scalability is also required within a single mission, as operations frequently scale during the deployment and execution phases.
- (5) **Resilient.** Resilience is the ability to recover from unwanted changes and disruptions. CIS resilience is essential to ensure the

⁶ For additional information, refer to AC/322-D(2004)0040, NATO C3 System Interoperability Directive, 13 September 2004.

continuity and the timeliness of the C3 processes. CIS resiliency is achieved through a combination of redundancy and robustness against accidental events and attacks.

- (a) **Redundancy** is the quality of a system with repeated parts or subsystems to provide a backup in case of primary-system failure.
- (b) **Robustness** is the ability of elements, systems, or other units of analysis to withstand a given level of stress, or demand, without suffering degradation or loss of function.

Proper training is required to ensure that redundancy and robustness contribute to overall resilience. Business continuity, including disaster recovery, should be included in the design of CIS. Deliberate practice of disaster recovery procedures must also be included in exercises as part of readiness.

- (6) **Service-oriented.** The C3 Services Taxonomy⁷ establishes a service-oriented approach for NATO CIS, and invites nations and other stakeholders to do the same in order to improve interoperability and reusability, and create efficient employment of CIS. Service orientation is one option for the provision of services in FMN.
- (7) **Autonomous.** Autonomous CIS refers to the ability to operate regardless of the availability, control, and influence of external CIS and any pre-existing logistics and infrastructure (e.g., power and accommodation), and operating actors. CIS autonomy is required to conduct deployed operations, where the availability of communications among different deployment sites is not always guaranteed. Mission command principles are also applied to CIS, which should be provided with the necessary autonomous characteristics to allow the conduct of isolated C3 during wide-area communications outages.
- (8) **Timely.** The Alliance CIS comprises a number of networks and systems with a wide spectrum of required timeliness. Ranging from non-time-critical daily communication (supported by best-effort CIS) to platform and weapon supporting systems (that require real-time CIS), technology should be selected and implemented in a manner

⁷ For additional information on the C3 Services Taxonomy, refer to AC/322-N(2012)0092-AS1, Consultation, Command and Control (C3) Classification Taxonomy, 19 June 2012.

that satisfies individual timeliness requirements in a cost-effective manner.

- (9) **Readiness.** CIS readiness refers to the level of preparation to accommodate an immediate requirement. In general, different NATO and national HQ, units, agencies, and other bodies are made available at different levels of readiness, commensurate with their role in the C3 or mission process. Their respectively allocated CIS should have a similar level of readiness, so they can conduct their function accordingly.
 - (10) **Secure.** Proper CIS security guarantees the required levels of confidentiality, integrity, and availability for services, systems and information, commensurate with the mission requirements. CIS security disciplines, in order to be effective and efficient, need to be an integral part of consultation, mission planning, execution, and assessment, and need to be provided through a balanced combination of design, continued assurance evaluation, and countermeasures.
- d. **CIS Structure.** CIS supports the complete C3 process in NATO and operations where NATO participates, and as such there are a number of different classification approaches for CIS. The most frequent ones are based on provision and location.
- (1) **Provision** looks at the agent that owns and operates the CIS. It is common to distinguish between NATO and nationally-provided CIS. In general, NATO provides full CIS support (*full-provision*) of strategic-level activities of the NATO Enterprise⁸ at the component command level and above, and limited CIS support (*provision-to* or *CIS augmentation*) to multinational static or deployed force structure component-command level HQ. Nations provide for the national elements of the static strategic networks, the core of the multinational HQs and units CIS requirements at component command and below, as well as for the national deployed components.

⁸ Per AC/322-D(2014)0006, The NATO Enterprise Approach for the Delivery of C3 Capabilities and the Provision of ICT Services, 14 July 2014, the NATO Enterprise comprises: the NATO HQ composed of the International Staff and the International Military Staff, and points of presence in national missions and delegations at NATO HQ; the NATO Military Command Structure and points of presence in national representations; the NATO force structure; NATO deployed and embarked HQs; NATO Agencies; NATO educational and training facilities; and points of presence in Nations for interconnection to nations/multinational NATO entities.

- (2) **Location** distinguishes between the static and the deployed environments.
- (a) **Static CIS** is usually provided by the NATO General Communications System (NGCS). The NGCS interconnects and provides local and wide-area connectivity within and between static HQs, NATO Agencies, static training and educational facilities, and points of presence in the nations. Nations provide national extensions to the NGCS when those are required to interconnect national assets in support of the C3 process. The NGCS provides the transmission, transport, and communications access services over which information systems are operated. Those information systems cover the full spectrum of services (i.e., core enterprise to user applications/functional services).⁹
 - (b) **Deployed CIS** consist of a number of building blocks that facilitate CIS combinations tailored to different mission types and sizes during the mission planning cycle.¹⁰ Building blocks include wide-area network (WAN) transmission; core communications services modules; information systems modules comprising core enterprise services of COI services and user applications/functional services;¹¹ distribution networks in different security domains; cross domain gateways; interface-to-nations modules; and end-user equipment. CIS modules are supported by logistics; SMC; transportation; power; chemical, biological, radiological, and nuclear defensive measures; and environmental protection, as required.
- e. **Information Management.** Information is a vital resource for NATO. As such, it should be managed by organizing and controlling information throughout its life-cycle - regardless of the medium and format in which the information is held. The NATO Information Management Policy (NIMP) describes the following key principles of IM:

⁹ There are other CIS (e.g., Air Command and Control System, active layered theatre missile defence, and Battlefield Information Collection and Exploitation System (BICES) that have static and deployable components but do not belong to the NGCS.

¹⁰ For additional information, refer to SH/CCD J6/SM FCIS/394/15-305978, Deployable Communications and Information Systems Concept of Operations (DCIS CONOPS), 28 January 2015.

¹¹ For additional information on the C3 Services Taxonomy, refer to AC/322-N(2012)0092-AS1, Consultation, Command and Control (C3) Classification Taxonomy, 19 June 2012.

- (1) **Information Ownership and Custodianship.** Information should have an originator, clearly defined ownership rights, and custodianship assigned throughout its life-cycle.¹²
- (2) **Leadership and Organizational Structure.** Management of information is a fundamental responsibility that requires executive leadership, top-level involvement, and the creation and maintenance of an effective organizational structure.
- (3) **Information Sharing.** Information sharing allows for the mutual use of information services or capabilities between entities (e.g., operational, medical, logistical, and financial). Information sharing requirements should be published to a COI and specified in IERs. Sharing of information may cross functional and organizational domains, and network boundaries. For example, within a joint force, information may be shared on a common operational picture (COP). To effectively share information, clearly understood rules and regulations on providing (posting), accessing (including classification and releasability), and distributing information should be established, emphasizing the security principle of “need-to-know.” This should be managed to facilitate access, optimize information sharing and re-use, and reduce duplication, all in accordance with security, legal, and privacy obligations.¹³
- (4) **Information Standardization.** Information should have standardized structures and consistent representations to enable interoperability, cooperation, and more effective and efficient processes.
- (5) **Information Assurance.**
 - (a) Information assurance is the protection and defence of information and information systems by ensuring their availability, integrity, and confidentiality. Information assurance requires management processes to ensure the systems and networks employed to manage the critical

¹² For additional information on the information life-cycle, refer to C-M(2007)0118, NATO Information Management Policy (NIMP), 11 December 2007.

¹³ For additional information on information sharing, refer to AC/322-D(2011)0015, NATO Network Enabled Capability Tenets and Principles, 4 July 2011; AC/35-D/2002-REV4, NATO Directive on the Security of Information; C-M(2002)49-COR 11, Security within the North Atlantic Treaty Organization, Enclosure E – Security of Information, 28 May 2014; AC/35-D/1040-REV 6, Supporting Document on Information and Intelligence Sharing with Non-NATO Entities, 21 August 2014; and C-M(2007)0118, NATO Information Management Policy (NIMP), 11 December 2007.

information used by an organization are reliable and secure, and processes are in place to detect and counter malicious activity. Information assurance includes elements of physical security (e.g., personnel and document security) and information security. Communications security and computer security are integral elements of all military CIS operations and should be considered throughout planning and execution. Cyber defence activities are a pivotal element of CIS security - enabling delivery and management of CIS services in response to malicious actions perpetuated through cyberspace. Information should be protected to the correct level, ensuring that valid information is available to authorized users, and preventing valid information from being available to unauthorized persons. The degree of security provided should be consistent with the requirements of CIS users, the vulnerability of transmission media to interception and exploitation, and the reliability and releasability of communications security hardware and software.¹⁴ The three pillars of information assurance are to ensure:

1. **Availability.** Information is accessible and usable upon demand by an authorised individual or entity.
2. **Confidentiality.** Information is not made available or disclosed to unauthorised individuals, entities, or processes.
3. **Integrity.** Information (including data) has not been altered or destroyed in an unauthorised manner.

The combination of these three pillars provides two security by-products: **authentication** and **non-repudiation**.

1. **Authentication.** The act of verifying the claimed identity of an entity.
2. **Non-repudiation.** The measure of assurance to the recipient that shows that information was sent by a particular person or organisation, and to the sender

¹⁴ For additional information on information assurance, refer to AJP-3(B), Allied Joint Doctrine for the Conduct of Operations; and AJP-3.14, Allied Joint Doctrine for Force Protection.

that shows that information has been received by the intended recipient(s).

- (b) Information assurance is represented as consisting of five elements of security: personnel security, physical security, security of information, CIS security (includes cyber defence), and industrial security. The relationship between these elements is depicted in Figure 1.1.¹⁵ For the purposes of this publication, only CIS security (including cyber defence) is defined.¹⁶

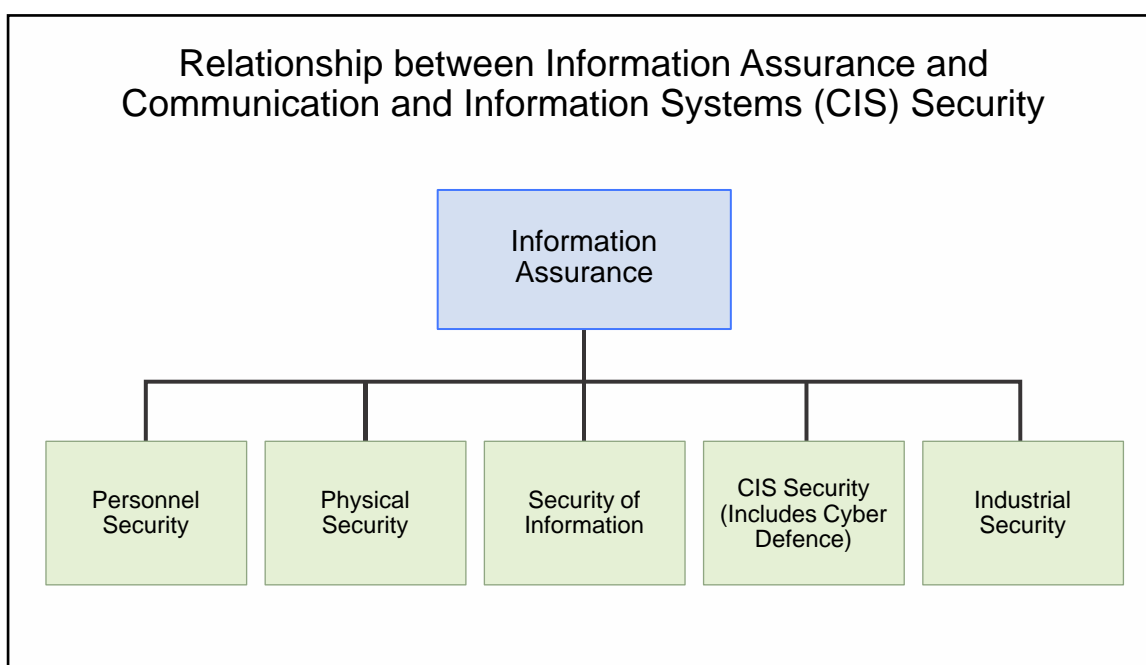


Figure 1.1. Relationship between Information Assurance and Communication and Information Systems (CIS) Security

- (c) **Communication and Information Systems Security (CIS security), including Cyber Defence.** As an element of information assurance, CIS security is the application of security measures for the protection of communication, information, and other electronic systems; and the information that is stored, processed, or transmitted in these systems with respect to availability, integrity, authentication,

¹⁵ For additional information on information assurance, refer to C-M(2002)49-COR11, Security within the North Atlantic Treaty Organisation, 28 May 2014.

¹⁶ For additional information on cyber defence, refer to PO(2014)0358, Enhanced NATO Policy on Cyber Defence, 27 May 2014; MC 0571/1, Military Concept on Cyber Defence; and C-M(2011)0020, NATO Cyber Concept.

confidentiality, and non-repudiation. Cyber defence is defined as the means to achieve and execute defensive measures to counter cyber attacks and mitigate their effects, and thus preserve and restore the security of communication, information, and other electronic systems.¹⁷ According to Enclosure F to C-M(2002)49-COR11, Security within the North Atlantic Treaty Organization, 28 May 2014, cyber defence is included within CIS security.

Acknowledging this, NATO has adopted a comprehensive approach to CIS security (including cyber defence) by integrating equivalent efforts between incident response, preventive CIS security measures, and user awareness to protect static and deployed NATO networks and ensure business continuity or mission assurance for operations. This includes the integration of cyber defence considerations into Alliance operations and missions.

- f. **CIS Prioritization.** Derived from the necessary information inputs and outputs to their processes and activities, all "information consumers" and "information producers" should describe their IERs as a basis for information flow management.¹⁸ CIS discipline requires the identification and prioritization of information flow consistent with the projected rate of activity and scope of operations. Since available CIS may be limited and will have a finite capacity, commanders at all levels should prioritize their information requirements within the IM plan.

- g. **Economy of Communication and Information Systems Employment.** Avoiding unnecessary duplication, carefully defining and managing user requirements, and imposing strict transmission discipline achieves economy of CIS employment. To maximize efficiencies and meet user expectations, requirements should be: developed with user input, clearly stated at the beginning of the planning phase, and adjusted throughout mission or exercise execution. However, an emphasis on economy of CIS employment may reduce the benefit that some CIS may provide. A balance should be found between economy and redundancy of systems. For example, within a NATO-led coalition with non-NATO entities, unity of effort is best generated when partners are able to operate and contribute to a coalition using the CIS with which their forces have been trained and equipped.

¹⁷ For additional information, refer to AC/322-N(2014)0072, Report on Cyber Defence Taxonomy and Definitions.

¹⁸ For additional information on the specification of NATO IERs, refer to Allied Procedural Publication (APP)-15, NATO Information Exchange Requirement Specification Process.

0104. **Communication and Information Systems in Support of Command and Control**

- a. Command is the authority vested in an individual of the armed forces for the direction, coordination, and control of military forces. It is the process by which the commander's will and intentions are impressed upon subordinates to achieve particular objectives. Command encompasses the authority and responsibility to employ forces to fulfil the mission. Control is inherent in command. To control is to regulate forces and functions to execute the commander's intent. To achieve this, the JFC and staff use standardized procedures in conjunction with the available equipment and CIS. Together, they form a system that the commander, staff, and subordinates use to plan, direct, coordinate, and control NATO operations and NATO-led coalition operations with non-NATO entities. CIS J6 (Communications) staff provide advice on the creation of the most effective C2 system, considering the capabilities of the available CIS.
- b. C2 systems must provide commanders with the ability to make and control the implementation of decisions. C2 systems should provide the commander with relevant and timely information required to support the decision-making process, and the staff with sufficient data to effectively manage assigned resources in the achievement of mission objectives. Furthermore, joint C2 CIS architectures must be able to adjust in support of changes to the command support structure.
- c. The scope and scale of the CIS to support C2 is determined by: the C2 structure; the identity and contributions of partner nations; the nature of mission tasks; geographic dispersal; the nature, classification, volume, and level of data and information to be exchanged between each C2 entity; and the application of reachback.
- d. Implications of Reachback
 - (1) Reachback, at the operational level, is the process of obtaining products, services, applications, forces, equipment, and material from organizations that are external to the area of responsibility. Provision of reachback capabilities expands, via virtual means, the capabilities of an operational-level HQ while reducing the footprint of the operational level HQ - without degrading efficient, effective, and timely support to operational level forces.
 - (2) The effectiveness of reachback relies upon provision of robust CIS services that should be deployable, flexible, and sustainable to support the complexity of changing missions in austere or

unpredictable environments. The commander should be aware of CIS capabilities and limitations and should be prepared to allocate these critical resources based on a personal assessment of operational necessity.

- e. A signal support group facilitates CIS management and network control. Activities that are critical to NATO CIS should be fully coordinated with the joint operations centre (JOC).¹⁹
- f. To meet the JFC's C2 requirements, the J6 staff should lead the planning, coordination, and execution of CIS architectures and joint operations area (JOA) CIS, as well as participate in the establishment of strategic guidelines.
- g. J6 staff, in coordination with J2 (Intelligence) military security staff, identify CIS vulnerabilities and develop procedures and capabilities to protect coalition CIS. They develop CIS security plans, support the development of operations security plans, and ensure the readiness of recovery and consequence management plans and procedures to be executed by service providers. Additionally, the J6 staff assesses the impact of adversary activities on coalition CIS and takes part in the production of the joint restricted frequency list (JRFL), under the responsibility of the J3 (Operations) staff. The J6 staff coordinates specialist support relating to protection of friendly CIS. Finally, they coordinate use of the radio frequency (RF) electromagnetic spectrum for a wide array of communications and electronics resources.²⁰ In some nations, electronic warfare (EW) planning and coordination are carried out by the J6 staff.
- h. **Liaison.** CIS coordination and execution is enhanced by exchange of liaison officers to facilitate mutual understanding, unity of purpose, and action.

0105. **Overall Structure of Communication and Information Systems.** The objectives of cooperation in this area are to provide NATO-wide, cost-effective, interoperable, and secure C3 capabilities supported by CIS to ensure high-level political consultation and C2 of military forces. A federation of NATO networks securely connected with national fixed and mobile networks link NATO HQ, all

¹⁹ For additional information on support of a deployed operational-level HQ, refer to MC 0593, Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations, 23 February 2015; and SH/CCD J6/SM FCIS/394/15-305978, Deployable Communications and Information Systems Concept of Operations (DCIS CONOPS), 28 January 2015.

²⁰ For additional information, refer to AJP-3.6(B), Allied Joint Doctrine for Electronic Warfare; AJP-3.10, Allied Joint Doctrine for Information Operations, and ACO Directive 080-083, Allied Command Operations (ACO) Electronic Warfare (EW) Protection of Joint Restricted Frequency List.

HQ of the integrated military command structure, national capitals, national military commands, and NATO nations. The systems also provide for secure connections to facilitate consultation between NATO nations and conduct operations when NATO leads a coalition that includes non-NATO entities.

- a. **Federation.** When different CIS can operate with each other without requiring additional or external measures from those implemented when they were designed, they can be considered integrated systems. NATO has established rules and procedures for the classification, distribution, and foreign release of NATO information, both classified and unclassified. However, sometimes ad-hoc measures must be negotiated with, and accepted by, nations providing units to the joint force. To realize the synergistic benefits of federation (e.g., generating unity of effort and speed of command), federation of NATO CIS and NATO nation CIS within a coalition that includes non-NATO entities may occur at a mission or exercise specific classification and releasability level. FMN provides a way to achieve interoperability and federation.
- b. **Multidimensional Structure.** Each of the specific CIS aggregated to conform to the federated NATO CIS can be characterized according to different dimensions depending on operational, technical, or security aspects. Operationally, CIS may be categorized depending on the specific characteristics of the service or military function for which they were designed. While installed and operated with specific technical and procedural characteristics to support a service or military function, they may differ from the ones used in other services or military functions. In this regard, NATO CIS can be classified as:
 - (1) Static NATO CIS.
 - (2) Deployable NATO CIS.
 - (3) CIS provided by nations in support of NATO operations.
 - (4) CIS provided by partners in support of NATO-led coalition operations that involve non-NATO entities.
- c. **Communication and Information Systems Services.** In line with the Alliance C3 Strategy,²¹ CIS planning, provision, and operation is articulated in terms of services. Services express the functionalities CIS offer to the user, saving him/her from the need to understand or deal with the specific circumstances or characteristics required for the service to be

²¹ For additional information, refer to C-M(2014)0016, Alliance C3 Strategy.

offered. The C3 Services taxonomy²² defines the following services categories:

- (1) **Communications Services.** Communications services interconnect systems and mechanisms for the opaque transfer of selected data between, or among, access points, in accordance with agreed quality parameters and without change in the form or content of the data as sent and received. Communication services are further decomposed into access, transport, and transmission services.
 - (2) **Core Services.** Core services provide generic, COI-independent, technical functionality to implement service-based environments using infrastructure, architectural, and enabling building blocks. Core services provide these building blocks so generic, common capabilities do not have to be implemented by individual applications or other services. Core services are usually decomposed into infrastructure, service-oriented architecture platform, and business support services.
 - (3) **Community of Interest-Specific Services.** COI-specific services provide functionality as required by user communities in support of NATO operations, exercises, and routine activities. COI-specific services may have been previously referred to as "functional services" or "functional area services."
 - (4) **User Applications.** Communications, core, and COI-specific services compose the "technical services" layer of the C3 services taxonomy that represents the collection of services with requirements for software and hardware functionalities that can be reused for different purposes, together with the policies that should control their usage. User applications make use of the technical services to provide a user-facing capability. User applications provide a user front-end that aggregates technical services in support of a given military process.
- d. **Communication and Information Domains.** CIS domains are a way to sub-divide CIS-supporting capabilities attending to some particular criterion. This sub-division facilitates focusing the specification, design, implementation, or operation on specific subsets of the complete CIS. In

²² For additional information on the C3 services taxonomy, refer to AC/322-N(2012)0092-AS1, Consultation, Command and Control (C3) Classification Taxonomy, 19 June 2012.

NATO, domains are used for different purposes; therefore, domain taxonomy is required.

- (1) In the context of NATO joint operations, there are usually three types of main security domains:
 - (a) **NATO Domain.** The security rules and implementation policies for this domain are established by NATO, normally with a permanence character, and apply not only to deployed forces but also to all NATO CIS. They are subject to NATO technical and management policies.
 - (b) **Mission Domain.** These domains are established for a specific mission in time and scope, and incorporate CIS provided by NATO, NATO nations, and non-NATO entities. Mission-specific security and releasability rules and implementation policies are established by the JFC, and are agreed to by all participants. Depending on the situation, mission tasks, and participating partners, a mission domain may or may not have a subsidiary character with regard to NATO domains. A mission domain may be established independent of strict NATO policy in order to federate NATO CIS with CIS provided by partners, to include non-NATO entities, and to enable all partners in an operation to operate as equal peers.
 - (c) **National Domain.** This domain contains those CIS, or equipment, that follow security rules and implementation policies established by a specific nation. They are subject to national technical and management policies.

The three domains listed above may each support multiple network environments that operate at different security and releasability levels.

- (2) Security domains compartmentalize CIS attending to the sensitivity of the information that the CIS domain will process, store, and forward. That information sensitivity dictates the implementation and operation policies that have to be followed in order to be allowed to deal with the level of information sensitivity. In NATO, military networks typically follow a “system-high” approach, meaning that a given security domain can contain all types of information up to the authorised sensitivity level, all users need to be cleared to that level of sensitivity, and the “need-to-know” is not

technically, but administratively, enforced. In order to bring CIS to operation in a given security domain, NATO security accreditation must be granted. Typical NATO security-level domains include: Secret, Confidential, Restricted, Unclassified, and Internet.

- (3) **Mission networks** aim to provide mission-specific information domains. An information domain deals with the CIS and supported information required to conduct a particular mission or function. By spanning multiple security domains (which compartmentalize CIS resources - including the information that is processed, stored, and forwarded in each of them), mission domains facilitate user access to information. Information exchange gateways are the CIS capabilities that securely interconnect two or more security domains, allow the controlled exchange of information, and enable a virtual single information domain into a single mission network. The term domain is used also as a technical term for the installation.

e. **Overall Principles and Responsibilities within North Atlantic Treaty Organization Communication and Information Systems.** The following principles apply within the context of roles, responsibilities, and relationship decisions after consultation between the mission partners.

- (1) NATO policy has established certain overall responsibilities to establish NATO CIS. In this regard, the exchange of information to ensure effective C2 in support of joint and NATO-led coalition operations requires CIS connectivity between:
 - (a) NATO Command Structure, both static and deployed, in support of superior and subordinate HQ at all levels.
 - (b) The HQ of a unit being supported and the supporting unit.
 - (c) Land-, air-, maritime-, and space-based entities as required for mutual support.
- (2) Higher HQ will provide required connectivity to lower HQ. Taking these responsibilities into consideration, the installation, operation, and maintenance of NATO CIS are governed by the following general principles:
 - (a) NATO provides for the extension of unsecure and secure CIS connectivity to the highest level of national or multinational tactical command in a theatre of operations.

- (b) Lead or framework nations and multinational commands provide connectivity and services for multinational or national entities and subordinate formations; however, NATO facilities may be used, if available.
- (c) Nations provide the infrastructure for their own national rear links; however, NATO facilities may be used, if available.

The above principles apply within the context of roles, responsibilities, and relationships decisions after consultation between the mission partners.

- (3) Secure CIS connectivity supporting C2 should be provided to the maximum extent possible, with the NATO Secret (NS) level desired. For NATO-led operations involving non-NATO entities, secure information and data sharing between coalition peers (i.e., NATO and non-NATO entities) involved in a mission should be provided by a separate mission domain - protected at whatever classification level is necessary to accomplish the mission.
- (4) A mission or exercise-specific environment should be established in which all willing participants may choose to contribute material and non-material capabilities to conduct operations as equal peers within the same classification and releasability level. This is accomplished to enhance unity of effort and to enable maximum information and data sharing without impediments to distribution or access (subject to individual national information security policies).

0106. **Interoperability Aspects of Communication and Information Systems**

- a. Interoperability is required to allow the passage of information between different elements of a deployed joint force or, in multinational operations, with NATO, NATO nations, and non-NATO entities. Interoperable CIS allow the commander to exercise operational C2, and permit all elements of the joint force to successfully coordinate their activities in an efficient manner. Further notable aspects of interoperability are:
 - (1) **Interoperability versus Security.** The competing needs of interoperability and security should be actively managed, in compliance with respective NATO directives, particularly on multinational operations. Technical and procedural solutions based on a comprehensive risk analysis should be required. The risk analysis should be detailed, focused on risk mitigation, and identify

the risk owner.²³ Balance between interoperability and security can be reduced, and synergy increased, by employing NATO, NATO nation, and non-NATO entity materiel and non-materiel capabilities within the same classification and releasability level operating environment established for the specific mission or exercise.

- (2) **Joint and Combined Operations.** The requirement for CIS to be interoperable within, and between, joint force components and supporting forces is well established. However, operational trends within NATO-led coalitions, particularly when engaged in peace support, indicate a growing requirement to achieve unity of effort (with some level of material and non-material interoperability) with cooperative partners and stakeholders.
- (3) **Interagency and Public Operations.** The lack of interoperable CIS (i.e., if a federation of NATO CIS and partner-contributed CIS, at a mission specific classification and releasability level, is not practical) and non-material capabilities in such an environment may require the deployment of compatible systems and greater use of liaison officers. Furthermore, establishment of technical, information assurance, security, protection, and data format and semantics standards to which NATO, NATO nations, and non-NATO entities could choose to train and equip would set in place potential increases in CIS technical interoperability and compatibility. Implementation of CIS within a mission or exercise network environment would be further informed and shaped by guidance and direction by commanders and mutual agreements during mission or exercise planning processes.
- (4) **Language.** NATO communication doctrine is based on the use of English and French as the common working language. During multinational or coalition operations, interpreters may be required to overcome language challenges.
- (5) **Doctrine, Tactics, and Procedures.** Agreements such as NATO standardization agreements (STANAGs), memorandums of understanding (MOUs), Allied publications, Allied communications publications (ACPs) as adopted from the Combined Communications Electronics Board, and doctrine will serve as a foundation for interoperability. These agreements and doctrine should cover principles, procedures (e.g., standard message

²³ For additional information on risk analysis, refer to AJP-01(D), Allied Joint Doctrine; and NATO Standardization Agreement 5524, NATO Interoperability Standards and Profiles (NISIP).

formats), and spectrum management. Testing the strength or validity of these should contribute to the aims and objectives of the CIS communities, in concert with operational communities, when utilizing opportunities to exercise in joint, coalition, and combined operations.

- (6) **Verification, Validation, and Testing Activities.** These activities are key to ensure CIS interoperability, and as a prerequisite to efficient information sharing. Materiel and non-materiel interoperability testing, to include CIS, should be conducted as often as possible. These activities should make use of the most recent, proven, and accurate set of testing principles, processes, guidelines, and tools, and should benefit from recent lessons learned to improve mission partner information exchange and interoperability. Processes and procedures for the assessment and assurance of materiel (to include CIS) and non-materiel interoperability between partners to support operations should be established and implemented during the mission or exercise planning phase.
 - (7) **Data Standards, Database Formats, and Information Exchange.** Lack of standardization in CIS procurement and development within NATO and NATO nations has led to implementation of numerous data, database, and waveform formats that hamper interoperability. If at all possible, and in complementary support of NATO and national objectives, a common set of IERs should be adhered to during CIS acquisition and implementation activities. A common set of IERs would facilitate consistent implementation of the agreed-upon standards among NATO and NATO nations. NATO and national J6 staff planners should be aware of NATO-agreed references on interoperability (see references). In some cases, established commercial off-the-shelf software also may be used to maximize interoperability.
- b. The CIS interoperability requirements for a joint force are based on the level of interoperability required for NATO services that must be extended to lower echelons of the joint force (the five "Levels of Interoperability" are listed in Annex B, page B-2, paragraph B002). NATO services are those services employed in the context of NATO C3 systems and, in particular, those provided mainly by NATO-owned CIS. Those services are extended to the joint force by the DCIS. The echelons and units to which the DCIS must extend these services are established by the MC in the minimum military requirements (MMRs). In addition to the MMRs, if NATO services must be extended to other echelons or units, nations providing

these forces must provide the CIS in order for these services to be offered. However, for access to key NATO services regardless of the security domain, access to these services requires that national CIS comply with applicable policy and undergo a NATO certification process.

- c. Specific to the NS security domain, there are three alternative solutions to requiring national CIS comply with NS security domain restrictions in order to exchange information between the NS security domain and a NATO contribution to a mission domain established for those CIS services supporting the joint force, but not following the NS security domain requirements.
 - (1) For movement of information and data from information systems services on the NS WAN to a mission domain information system or user, the exchange must be technically feasible, and requires an appropriate information exchange gateway that guarantees the information is exchanged according to requirements. For communication systems, the common solution is to provide users outside the NS security domain with NATO certified communications terminals that allow end-to-end encryption. While these terminals would be used and controlled according to NS security domain rules, communications should be tunneled through the network that belongs to the mission domain.
 - (2) Establish NATO CIS to support a joint force within a mission specific classification and releasability level (not following NS security domain requirements) to enable direct NATO CIS to partner CIS exchange without tunneling or cross security level movement of information, data, or services.
 - (3) To move information and data from CIS on the NS WAN to a NATO user on NATO CIS within a mission network environment requires an appropriate information exchange gateway that guarantees the information is exchanged according to requirements, while protecting the NS WAN from intrusions.²⁴
- d. **Interoperability in Land Communication and Information Systems**
 - (1) CIS interoperability for land communication and information services often is achieved by procedural solutions. These

²⁴ For additional information, refer to MC 0593, Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations, 23 February 2015.

procedures are based on the rule that higher HQ provide the means for lower echelons to exchange information with them.

- (2) To best leverage technically compatible systems and procedural interoperability belonging to different partners, establishment of a mission specific environment in which all partners share and comply with the same security, protection, information assurance, classification, and releasability rules is recommended, if practical.
- (3) STANAG 5048, The Minimum Scale of Connectivity for Communications and Information Systems for NATO Land Forces, provides the procedural rules for minimum connectivity among different echelons of a land force. Technical interoperability is established in the STANAGs that cover the technical characteristics and required interfaces for tactical area communications systems and combat net radio systems. MC 0593, Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations, 23 February 2015, provides an overarching, framework document encompassing joint strategic and operational levels.
- (4) For land information systems, the Multilateral Interoperability Programme contains technical specifications that facilitate the exchange of data among land C2 systems from different nations. These technical specifications may serve as the basis for defining common implementations of C2 data structures.

e. Interoperability of Maritime Communication and Information Systems

- (1) The planning and execution of operations should be an increasingly joint and multinational effort requiring truly interoperable forces. The goal of interoperability is to efficiently share tactical, operational, and selected administrative knowledge for planning and executing operations. Maritime CIS should have the capacity to support information collection, situation assessment, decision making, and mission execution and control by receiving, correlating, fusing, and disseminating relevant information from multiple sources to the appropriate levels of command.
- (2) Interoperability is a crucial element in supporting the information flow, not only between Alliance force structures, but also with non-NATO entities and other IOs. Ability of maritime forces to operate with respective CIS and non-materiel capabilities within a mission network environment, in addition to national network environments,

should enhance the ability to leverage and use existing technical and procedural interoperability within a coalition force. Benefits apply for interoperability shared with joint partners also operating within the same coalition.

- (3) It is essential that maritime forces meet, at a minimum, an agreed fitting standard for CIS. The CIS fitment at each platform should be robust, secure, reliable, and timely, as well as interoperable, to ensure maritime forces seamlessly integrate into joint operations.
- (4) Interoperability of maritime CIS are addressed in MC 0195/9, NATO Minimum Interoperability Fitting Standards for Communication and Information Systems (CIS) Equipment Onboard Maritime Platforms (or successive revisions); ACP 200 (D) Volume 1, Maritime and Mobile Tactical Wide Area Networking (MTWAN) in the Maritime Environment – Operating Guidance; and ACP 200 (D) Volume 2, Maritime and Mobile Tactical Wide Area Networking (MTWAN) Technical Guidance.

- f. **Interoperability of Air Communication and Information Systems.** The air component of a joint and NATO-led coalition force utilizes a standards-based air C2 system reference architecture. Communications systems are interoperable through radio technical and data link STANAGs. Interoperability of air C2 planning and execution, supporting information exchange systems, and operational processes and data is discussed in AJP-3.3(A), Allied Joint Doctrine for Air and Space Operations, and other air C2 COI documents that frame integrated C2 processes and employment of air C2 systems. The ability of air component forces, to include air assets of other joint Services, to operate with respective CIS and non-materiel capabilities within a mission network environment - in addition to national network environments - should enhance the ability to leverage and use existing technical and procedural interoperability within a coalition force. Benefits apply for interoperability shared with joint partners also operating within the same coalition.

INTENTIONALLY BLANK

CHAPTER 2

ROLES AND RESPONSIBILITIES

0201. **Introduction.** This chapter outlines the strategic and operational CIS-related roles and responsibilities of NATO organizations and commands.

0202. **Member Nation Responsibilities.** Member nations have a responsibility to ensure national capabilities intended to support combined/joint operations are developed in accordance with interoperability standards. The principles of interoperability are discussed in Annex B.

0203. **Strategic Level Roles and Responsibilities**

- a. The North Atlantic Council (NAC) is the principal decision-making body within NATO. It brings together high-level representatives of each NATO nation to discuss policy or operational questions requiring collective decisions. The C3 Board supports NATO C3 by providing guidance and direction, in order to enable information sharing and achieve interoperability. Their role is to:
 - (1) Act as the NATO C3 Senior Policy Committee.
 - (2) Act as NATO's Senior C3 advisory body.
 - (3) Assist the MC in the development of MC advice on C3-related issues.
 - (4) Act as the NATO authority for the development of technical and implementation directives and guidance on CIS security, including cyber defence.
 - (5) Act as the governance body for the NATO Public Key Infrastructure Management Authority.
 - (6) Act as tasking authority for C3 standardisation in accordance with the NATO Standardization Office charter.
 - (7) Act as the governance body for the NATO Information Management Authority.
 - (8) Act as the NATO authority for the C3 enterprise architecture - guiding its development and directing its implementation.

- (9) Act as the coordinating authority for all NATO efforts in pursuit of NATO C3 strategic objectives, to include the NNEC concept.
 - (10) Act as the focal point for NATO Cooperation and Partnership for Peace activities in the field of C3 - establishing policy and coordinating efforts pertinent to these activities.
 - (11) Act as a key forum for promoting C3-related multinational programmes and national adoption of NATO C3 capabilities and their enablers.
 - (12) Maintain and direct a subordinate committee structure that directly contributes to the achievement of NATO's C3 strategic objectives.
- b. Allied Command Operations (ACO) plans, prepares for, and conducts military operations to meet Alliance political objectives. Supreme Allied Commander Europe (SACEUR) is one of the two strategic commanders for NATO and the commanding officer of ACO. SACEUR is responsible to the MC for the overall direction and conduct of NATO military operations. The Supreme Headquarters Allied Powers Europe (SHAPE) Deputy Chief of Staff (DCOS) Plans develops, reviews, and maintains strategic planning for direction and oversight of capability planning, NATO deployable C2 capabilities, and static HQ. The SHAPE DCOS CIS and Cyber Defence (CCD) directs, monitors, and coordinates all ACO CIS and cyber defence functional area activities and staff functions. The SHAPE DCOS CCD is dual-hatted as the Commander, NATO CIS Group (NCISG). Emphasis is on providing direction and guidance to the NCISG for the provision of deployable capabilities during operations and exercises and making contributions to the capability management process for NATO's C2/C3 and information assurance capabilities throughout their life-cycle. Working under the direction of the SHAPE DCOS CCD, the SHAPE J6 directs and provides oversight of all CIS and cyber defence functional area activities provided by the NATO Communications and Information Agency (NCIA) across ACO, at all levels of command, and for all ongoing operations and exercises. See Figure 2.1.

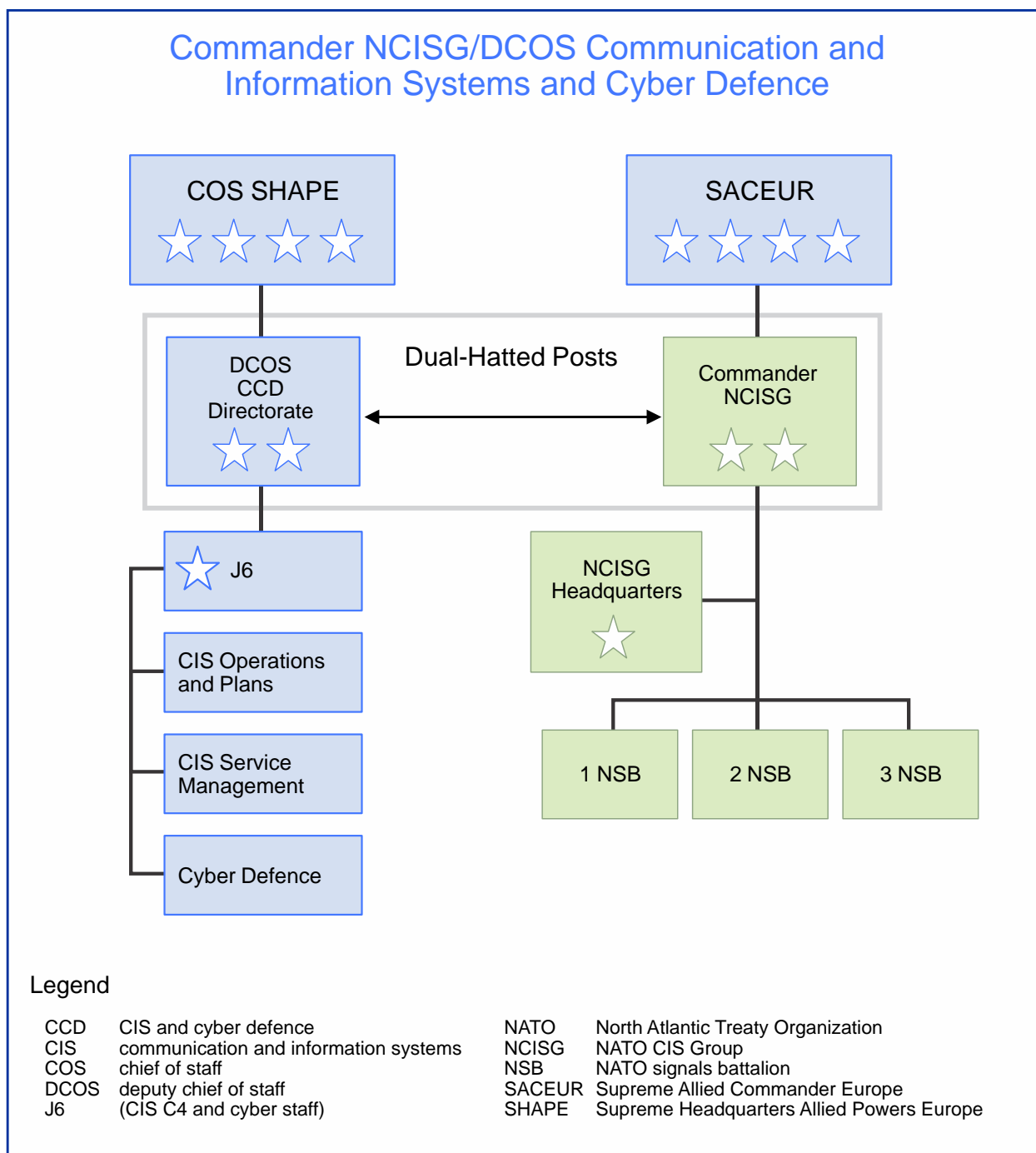


Figure 2.1. Commander NCISG/DCOS Communication and Information Systems and Cyber Defence

- c. Allied Command Transformation (ACT) is NATO's leading agent for change - driving, facilitating, and advocating continuous improvement of Alliance capabilities to maintain and enhance the military relevance and

effectiveness of the Alliance. ACT's strategic objectives include: provide appropriate support to NATO missions and operations; lead NATO military transformation; and improve relationships, interaction, and practical cooperation with partners, nations, and IOs. ACT is organised around four principal functions: strategic thinking; development of capabilities; education, training, and exercises; and co-operation and engagement. These functions are reflected in the composition of ACT which is comprised of the Norfolk HQ and three subordinate entities: the Joint Warfare Centre in Norway; the Joint Force Training Centre in Poland; and the Joint Analysis & Lessons Learned Centre in Portugal. ACT also has a representative at NATO HQ in Brussels and at the Pentagon outside Washington D.C.; an ACT Staff Element at ACO HQ, SHAPE; and a shared Military Partnership Directorate with ACO – also located at SHAPE. Due to the significance that CIS play in today's operational environment, Supreme Allied Commander Transformation established the Command and Control, Deployability, and Sustainability Division, under the guidance of DCOS Capability Development, to lead all transformational efforts related to the provision of CIS capabilities for NATO's operational commanders and national forces.

- d. Detailed responsibilities for providing CIS services within multinational HQ, and between these HQ and subordinate commands, are in accordance with established MOUs or service-level agreements. CIS services within deployed national formations/units and the extension and provision of services to subordinate national elements or parent/national HQ are the responsibility of the nation concerned.
- e. HNs, within whose territory NATO HQ are deployed, usually allow deployed forces to utilize available and appropriate military and civil CIS infrastructure. Automated interfaces between NATO HQ and HN facilities should be established, wherever possible, using NATO standards or NATO-adopted international commercial standards. Details of HN facilities available to deployed NATO HQ will be in accordance with MOUs and detailed technical arrangements agreed to on a case-by-case basis. When NATO HQ are deployed to territories or areas where there is no appropriate military or civil CIS infrastructure available, or nations are unwilling to allow such facilities to be used, SACEUR should provide strategic communication²⁵ links via the most appropriate means.
- f. The **NATO Communications and Information Organisation** is under the authority of the NAC. It was established to meet the collective

²⁵ This "strategic communications" does not refer to the strategic communications (StratCom) in AJP-3.10, Allied Joint Doctrine for Information Operations.

requirements of NATO nations in the fields of capability delivery and service provision related to C3, communications, information, and cyber defence functions.²⁶ It is composed of an Agency Supervisory Board (ASB); and an Executive body composed of a General Manager and staff (i.e., the NCIA).

- (1) The **ASB** is responsible for the organisational governance of the NCIA. Organisational governance is the mechanism by which NATO directs, administers, and controls the NCIA and enables it to accomplish its mission, functions, and tasks. It is the set of rules and best practices through which the ASB pursues the interests of NATO as a whole, as well as individual or groups of NATO nations - ensuring NCIA efficiency, effectiveness, accountability, and transparency. The ASB is the sole entity reporting to the NAC on behalf of the NATO Communications and Information Organisation. It provides strategic direction and guidance to the NCIA and oversees its activities and performance.
- (2) The **NCIA** acts as NATO's principal C3 capability deliverer and CIS service provider to NATO HQ, the NATO Command Structure, and NATO Agencies (including itself), for the full range of its entitled requirements holders and customers. It should be, to the maximum extent feasible, the provider of information technology support to NATO business processes (to include provision of information technology shared services). Its mission is to:
 - (a) Deliver C3 capabilities to its requirements holders, while ensuring their coherence and interoperability in compliance with agreed NATO architectures.
 - (b) Ensure provision of secure CIS services to its customers.
 - (c) Deliver capabilities and provide services (other than C3/CIS) to NATO and NATO nations, as approved by the ASB.

With respect to CIS support to military operations, pre-deployment mission preparation, and exercises, the respective responsibilities between NCIA and NCISG are described in the C2 arrangements between SACEUR and General Manager NCIA.²⁷ SACEUR is

²⁶ For addition information, refer to C-M(2012)0049, Establishment of the New NATO Communications and Information Organisation.

²⁷ For addition information, refer to C-M(2012)0056, Politico-Military Advice on Command and Control Arrangements between SACEUR and the General Manager of the NATO Communications and Information Agency; and MCM-0065-2012, Command and Control (C2) Arrangements between SACEUR

responsible for overall military planning and approval of the results of the CIS operational planning process; definition, development, harmonization, and prioritisation of operational requirements; and development of IERs and their validation. General Manager NCIA is the technical authority and is responsible for creating a technically coherent, stable CIS environment and maintaining an appropriate level of control over technical aspects of in-theatre CIS service provision (including those provided via the NCISG). During most deployed operations, particularly where operations are high intensity or in extremely hostile environments, the NCISG will initially deploy elements of the group to provide in-theatre C2 services for NATO-led forces. This deployment will use NCIA provided DCIS equipment configured to the mission to create a technical extension of the NATO central network. NCIA provides supporting C2 services outside the capability of NCISG - either remotely through deployment of NCIA elements into theatre, by outsourcing, or by some combination of both.

0204. **Operational Level Roles and Responsibilities**

- a. At the operational level, the JFC:
 - (1) Ensures adequate and effective CIS support for the joint C2 structure and directs which system(s) is/are to be the primary executive/operational system for the force.
 - (2) Publishes CIS plans, annexes, and operating instructions to support the assigned mission.
 - (3) Exercises overall management of all CIS supporting the joint force.
 - (4) Reviews and coordinates CIS plans prepared by subordinate commands.
 - (5) Ensures CIS interoperability is achieved within the joint force.
 - (6) Establishes a battlespace spectrum management plan.
 - (7) Ensures adequate procedures are included, in operations and operations planning, to address continuity of Alliance Operations and Missions in case of cyber attacks and serious incidents

and the GM of the NCIA.

threatening mission success, to include business continuity plans and prioritization of disaster recovery activities.

(8) Organizes the C2 of NATO CIS.²⁸

- b. In joint operations, successful CIS integration requires that strict technical and management standards be imposed throughout the network. Integration involves putting together various system components in such a way that the combination of separate systems, capabilities, and functions can operate together effectively without adversely affecting the other elements. The purpose of joint CIS management is to provide centralized control and decentralized execution of the utilization of CIS resources consistent with the JFC's operational requirements and changing priorities. CIS can provide support and technical solutions to implement IM in an organization. In a joint force HQ, the J6 staff normally is responsible for joint CIS services provision - supported by NCISG during planning and by a signal support group when deployed.
- c. In NATO-led coalition operations, successful CIS integration requires that agreed upon technical, management, and policy standards be imposed throughout a federation of mission networks and CIS contributed by NATO, NATO nations, and non-NATO entities alike. Integration involves putting together, as a final item, various components of a system in such a way that the combination of separate systems, capabilities, and functions can operate together effectively without adversely affecting the other elements. The purpose of coalition communications management within a federation of mission networks is to provide centralized control and decentralized execution of the utilization of communication resources consistent with the JFC's operational requirements and changing priorities. CIS can provide support and technical solutions to implement IM in an organization. In a coalition force HQ, the J6 staff normally is responsible for managing communications in concert with management of sovereign CIS resources contributed by partners.

²⁸ In accordance with MC 0593, Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations, 23 February 2015.

INTENTIONALLY BLANK

CHAPTER 3

COMMUNICATION AND INFORMATION SYSTEMS PLANNING

0301. **Introduction.** CIS planning is a component of the NATO planning process, in all of its three levels: strategic, operational, and tactical. All levels of CIS planning must consider participation of committed non-NATO entities.
0302. **Strategic-level Planning.** At the strategic level, planning is conducted in accordance with the Comprehensive Crisis and Operations Management process, as detailed in the ACO Comprehensive Operations Planning Directive (COPD).²⁹
- a. **Strategic Planning Products.** Planning products at the strategic level include SACEUR's Strategic Assessment, military response options, strategic operation plan (OPLAN), and strategic planning directives.
 - b. **Strategic CIS Planning Products.** CIS contribute with the following supporting elements to the strategic-level plan: strategic CIS assessment, strategic CIS estimate, strategic concept of operations (CONOPS) CIS guidance, strategic CIS planning guidance, and CIS support plan (SUPPLAN).
0303. **Operational-level Planning.** Operational-level planning responsibilities are defined at the strategic level, with the planning being directed at the joint command, component command, or multinational component command-level. Operational-level planning steps and activities are described in AJP-5, Allied Joint Doctrine for Operational-Level Planning. AJP-5, in turn, informs and guides the development of planning instruments, including the ACO COPD, and the underlying functional planning guides [e.g., ACO Directive 080-095, Communication and Information Systems (CIS) Planning Directive, 2 July 2014].
- a. **Operational-level Planning Process Steps.** The operational-level planning process (OLPP) consists of the necessary steps to support a JFC and staff in order to develop the operational-level OPLAN - including the conduct of the operational estimate process. The steps also comprise the campaign and operational assessment during execution in order to review or revise the plan, when required. These steps are:
 - (1) Step 1 – Initiation.

²⁹ For additional information, refer to the Allied Command Operations Comprehensive Operations Planning Directive, Interim version 2.0, 4 October 2013.

- (2) Step 2 - Problem and mission analysis.
 - (3) Step 3 – Course of action (COA) development.
 - (4) Step 4 - COA analysis.
 - (5) Step 5 - COA validation and comparison.
 - (6) Step 6 - Commander’s COA decision.
 - (7) Step 7 - Operational-level CONOPS and plan development.
 - (8) Step 8 - Campaign assessment and plan review/revision.
- b. **Operational Planning Products.** AJP-5 describes operational planning products in generic form while the ACO COPD provides greater detail tailored to SHAPE-led operations. Operational planning products include the draft Combined Joint Statement of Requirements, the draft Theatre Capability Statement of Requirements, and the draft Crisis Establishment.
 - c. **Operational CIS planning products.** CIS contributes to the following supporting elements of the operational-level plan: Operational CIS Assessment and Estimate, IERs (Annex Q to operational CONOPS), and CIS Service Matrix (Annex Q to operational OPLAN).

0304. **Nature of Communication and Information Systems Planning**

- a. CIS planning is cyclical and iterative in nature. It is conducted continually, in close synchronization with the J2, J3, and J5 (Plans), to ensure CIS plans are consistent with the overall planning effort. CIS planning supports each step of the OLPP, as well as most³⁰ of the **doctrinal principles** laid-out in AJP-5, including:
 - (1) Definition of objectives.
 - (2) Unity of purpose.
 - (3) Sustainment.
 - (4) Concentration of force.

³⁰ The remaining doctrinal principles, including “initiative” and “maintenance of morale,” are, in general, not directly addressed in the CIS planning cycle, but still enabled by proper CIS.

- (5) Economy of effort.
 - (6) Flexibility.
 - (7) Security.
 - (8) Simplicity in plans and orders.
 - (9) Multinational.
- b. CIS planning is conducted taking into account the following **critical planning factors**:³¹
- (1) Time.
 - (2) Budget.
 - (3) Scale and type of operation.
 - (4) Availability of resources.
 - (5) Capability limitations.
 - (6) Interoperability.
 - (7) CIS security (includes cyber defence).
 - (8) DCIS impact on on-going missions and tasks.
 - (9) DCIS real-life support and force protection.
- c. CIS planning also takes into account the following **additional planning factors** that are used to guide the estimates for NATO CIS:
- (1) The time available for planning, pre-deployment, deployment, redeployment, and reaction to CONPLANS.
 - (2) An understanding of the IERs and information systems and facilities.

³¹ For additional information, refer to ACO Directive 080-095, Communication and Information Systems (CIS) Planning Directive, 2 July 2014.

- (3) The availability of in-service CIS or, if required, commercial CIS, and the ability to respond to urgent operational requirements.
 - (4) Bandwidth and channel availability, particularly on strategic satellite communications bearers and within national communications networks.
 - (5) The availability of, and ability to control and manage, the RF electromagnetic spectrum.
 - (6) The readiness of those required to deploy, operate, and maintain CIS, particularly that which is newly procured.
 - (7) The availability of, and adherence to, international standardization of technical protocols.
 - (8) Architecture of systems to be used (e.g., centralized vs. distributed; local vs. remote; and static vs. mobile).
- d. The **main outcome of the CIS planning process** is the CIS SUPPLAN, which is normally an integral part of the OPLAN developed in support of crisis response planning. Additionally, CIS SUPPLANS or equivalent CIS annexes are developed to detail and augment the contents of advance planning efforts (e.g., a standing defence plan), a CONPLAN, or a generic CONPLAN.
- e. **Roles and responsibilities.** The CIS SUPPLAN is developed by the CIS support entities, namely NCISG and NCIA, with contributions from the operational and subordinate commanders. It contains details about how CIS support is going to be executed at the operational level. SHAPE DCOS CCD is responsible (on behalf of SACEUR) for the overall CIS planning and approval of the CIS SUPPLAN. During development of a CIS SUPPLAN for a NATO-led operation that involves establishment of a federation of mission networks, to include relationships with non-NATO entities, NCISG and NCIA represent NATO Command Structure contributions in the collective development of a CIS SUPPLAN that reflects peer equities of all network contributing mission partners. General Manager NCIA is the technical authority and is responsible for creating a technically coherent, stable CIS environment and maintaining an appropriate level of control over technical aspects of in-theatre CIS service provision (including those provided via the NCISG).
0305. **CIS Planning Activities.** CIS planning comprises a number of activities and tasks that support and inform the overall planning process. The CIS planning

process and the activities associated to each organizational function are available in the Strategic and Operational CIS Task Matrix.³² This matrix can be tailored by the commander to suit the particular needs and complexity of the mission. A summary of tasks is provided here:

a. **Communication and Information Systems Assessment**

- (1) **CIS Estimate.** A CIS estimate provides an assessment of the CIS capabilities required to support the operation against the CIS assets likely to be available, including those in the JOA. After incorporating operational directives, the commander's intent, critical and additional planning factors, and input from participating nations, the SHAPE J6 staff planner formulates the CIS assessment. The CIS assessment consists of the mission analysis, IERs provided by the JFC J6, evaluation of factors, potential solutions, and selected service delivery solutions. The CIS assessment is formulated, in close coordination with NCISG and NCIA, during drafting of the strategic CIS architecture.
- (2) **Information Exchange Requirements.**³³ IERs are pivotal inputs to the CIS planning process. They ensure that all relevant C2 services required in support of the mission are identified, and adequate planning and provision of C2 services can be achieved. IERs in the form of orders, reports etc. also reflect the exchange of information products in support of the chain of command. To ensure effective C2, a high degree of operational information exchange is required both vertically and horizontally, between increasing varieties of entities. In order to effectively exercise C2 over assigned NATO forces, there should be an effective and appropriate exchange of information between cooperating forces and/or HQs. All staff elements provide IERs to J6 staff planners to specify those applications and communication services required and needed for deployment. It is a responsibility of all staff elements, per the IM plan, to provide its specific IERs, with accuracy and in the expected time schedule, as a vital input for the CIS activity. This will also aid in determining the NATO systems with which a connection is necessary. IERs typically include level of classification, voice, data, chat, video teleconferences, web collaboration portals, e-mail, C2, intelligence, logistics, functional area sub-systems, and connection to other networks. Information

³² For additional information on this matrix, refer to ACO Directive 080-095, Communication and Information Systems (CIS) Planning Directive, 2 July 2014.

³³ For additional information on the NATO process for specifying IERs, including managing their configuration, refer to APP-15, NATO Information Exchange Requirement Specification Process.

regarding data format, content, and context relating to the IER elements obtained from all user communities is also critical to determining CIS configuration, capacity, architecture, and implementation policies (security and information assurance). This data, along with an aggregate list of IERs with related NATO, national, and coalition specific operational processes and associated supporting services and activities, can then be translated into the number and type of circuits, the necessary bandwidth, and CIS services to be provided.

- (3) **Information Providing Systems and Facilities.** The SHAPE J6 staff analyzes information-providing systems and facilities (e.g., sensors, command posts, and weapon systems) to define information that might be of interest to certain COIs. This information is published and accessible for the relevant COIs.
 - (4) **Evaluation of Factors.** Subject to NATO provisioning rules, CIS resource status information is included in CIS operational directives, orders, plans, and instructions. J6 staff planners should catalogue the resources committed by participating NATO nations from their analysis of these documents. CIS planning should be based primarily on existing NATO CIS and equipment. If NATO assets are available, the SHAPE J6 staff should, in coordination with NCISG and NCIA, define the CIS strategic architecture. If NATO assets are not available, national assets may be able to fill a requirement. In these cases, a statement of requirements (SOR) is created and submitted to the nations for sourcing. The lead nation (LN) of a particular HQ (e.g., a joint command HQ) assumes responsibility for providing CIS. If NATO does not have units available and the participating nations cannot provide units to meet SOR capabilities, NATO should seek a commercial option.
- b. **Strategic CIS Architecture.** The SHAPE J6 staff should direct NCISG and NCIA to produce a draft strategic CIS architecture at the beginning of the planning process. This draft strategic CIS architecture is based upon the CONOPS and JFC J6 staff input. To overcome strategic CIS architecture shortfalls, contracted, commercial CIS may provide an effective solution.
 - c. **Mission Analysis.** A mission analysis is performed to review the higher authority's direction and guidance, determine the nature of the problem, confirm the results to be achieved, and specify the direction of the CIS and cyber defence aspects regarding the mission. Since each participating nation will bring its own view to the operation, it is essential that a

coherent baseline of understanding be established as a prerequisite of CIS planning. The following points should be covered, as a minimum:

- (1) Situation overview and higher commander's intent.
- (2) Review of limitations.
- (3) Review of assumptions.
- (4) Recommend the commander's initial CIS priorities.
- (5) Identify the main effort and desired end state among the SHAPE J6 planning staff and establish an agreed-upon solution for providing CIS.
- (6) Establish all specified and implied priorities for providing CIS.
- (7) Conduct CIS risk analysis, to include a review of CIS vulnerabilities.
- (8) Review of the threat in cyberspace.

d. **Orientation.** The orientation stage is primarily comprised of the mission analysis results. This analysis should consider the political and military concerns expressed in the initiating directive in relation to all available information. The results of this mission analysis are briefed to the commander and should form the basis for CIS planning guidance. The purpose of this guidance is to focus subordinate planning and ensure appropriate CIS factors are incorporated in the overall plan. This guidance should include direction on CIS aspects of the mission. CIS planning uses mission analysis to orient planning, determine the nature of the problem, and confirm the results to be achieved.

e. **Commander's Planning Guidance and Initial Intent.** The commander establishes a main effort and end state through the statement of intent. The commander's intent drives the development of operational directives, orders, plans, and instructions. SHAPE J6 staff planners should ensure that, in their planning to support the various staff functions, the commander's intent is met. The following points should be covered, as a minimum:

- (1) Identify the basic strategic, operational, and tactical facts.
- (2) Establish the commander's CIS priorities based on an analysis of the CONOPS.

- (3) Identify the main effort and end state.
- (4) Establish agreed conclusions for providing CIS among the J6 planning staff.
- (5) Establish the agreed CIS guidelines among the participating nations.
- (6) Establish all specified and implied requirements for providing CIS.
- (7) Establish the specified and implied time factors for providing CIS. This should include the timeliness of warning orders.

f. **Concept Development**

- (1) Courses of Action and Selected Course of Action
 - (a) CIS service deliveries should flow from the operation's COAs. One CIS service delivery may be enough to cover all extant options, or different CIS service deliveries may have to be identified for each of the commander's options. Each COA should lead to the identification of a number of potential SHAPE J6 staff tasks. Prior to more detailed planning, it is advantageous to develop a broad CIS CONOPS for each potential COA.
 - (b) The choice of the COA drives the content of the CIS input to the CONOPS. The CONOPS expresses the military commander's intention on the use of forces, time, and space to achieve the mission objectives, and attain the end state. For the SHAPE J6 staff planner, this includes how the capabilities of the available CIS resources are synchronized to meet the IERs of the chosen COA.
- (2) CIS assessment follows the mission analysis and corresponds with the mission analysis briefing for the remainder of the staff. The planning process is now focused on concrete action; therefore, this focus is fairly narrow and the level of detail at this stage becomes progressively more important.
- (3) As previously mentioned, if NATO assets are not available, national assets may be able to fill the requirement. In these cases, a SOR is created and submitted to the nations for sourcing during the force

generation conference. If NATO assets are available, the CIS assessment can be determined. The format of the CIS assessment broadly mirrors the strategic evaluation. The SHAPE J6 staff should consider relevant data inputs from all staff branches and functional areas across the JOA for completion of the CIS assessment. It should be emphasized that the CIS focus will change throughout the phases of an operation. While the CIS assessment will differ between the strategic and the operational or tactical level, much of the information required is the same or similar. If NATO has no units available and the nations cannot provide units to meet SOR capabilities, NATO may seek a commercial option.

- (4) CIS assessment criteria and reporting format templates are described in ACO Directive 080-095, Communication and Information Systems (CIS) Planning Directive (chapters 4 and 5 supported by Annexes A, B and C), 2 July 2014. These format templates may be amended, where required.

g. Review of Limitations

- (1) Constraints and restraints on providing CIS may be at the strategic, operational, or tactical level. They may be political, legal, economic, or military in nature. Analysis of the constraints and restraints expressed in the operational directives, orders, plans, and instructions should be an essential early consideration in SHAPE and JFC J6 staff planning.
- (2) CIS resource status information should be included in CIS operational directives, orders, plans, and instructions. This may be expressed in the form of a task organization. SHAPE and JFC J6 staff planners are constrained by the resources committed by the participating nations. The analysis should reveal gaps, overlaps, or duplications in providing CIS. In particular:
 - (a) Availability of assets
 - 1. CIS planning should be based primarily on existing NATO CIS. Systems or equipment already under contract, or subject to pre-planned procurements, could form the basis for later phases depending on lead times for fielding or training.

2. Military, governmental, national, and commercial systems from NATO and non-NATO entities should be considered.
 3. International CIS contributions from NGOs should not be considered as a primary means of communications for military C2; however, they may need to be considered for other purposes (e.g., liaison teams).
 4. For some operations, the local infrastructure may not be available to support NATO CIS.
- (b) Shortfalls can be resolved in a number of ways; firstly, by the employment of NATO-owned CIS resources (e.g., NCISG). Secondly, SACEUR can approach nations for required assets through the force generation process. Finally, assets may be sought through the emergency procurement process. When considering providing assets that may require procuring systems/equipment, the planner should work closely with the J8 (Budget and Finance) staff to ensure support is adequately covered and procurement lead times are considered.
- (c) Personnel
1. SHAPE and JFC J6 staff planners should determine the availability of manpower required to deploy, install, maintain, and operate CIS equipment. They should also ensure that the SHAPE and JFC J6 staffs are correctly manned since the deployment of civilians to a JOA may be constrained. Any identified manpower deficiencies should be referred to J1 (Personnel and Administration) staffs.
 2. Operational requirements might dictate manning level changes to ease transitioning to the operational environment, or for parallel operations.

h. Plan Development

- (1) During plan development, the OPLAN is developed. It is normally the final outcome of planning and is produced in sufficient detail for mission execution. Forces are assigned and all necessary preparations are undertaken for successful execution of the

assigned mission. The OPLAN may be developed at any command level and is formally coordinated and approved by the NAC.

- (2) The OPLAN is comprised of a main body and supporting annexes. The CIS input to the OPLAN is in paragraph 5 of the plan's main body with the detailed architecture in Annex Q, "Communication and Information Systems." However, SHAPE and JFC J6 staff planners should ensure CIS factors are included in the situation, mission, and execution sections, and be aware that CIS requirements might be included in other OPLAN annexes. Coordination is essential to ensure all CIS requirements are met. Strategic CIS are defined as NATO CIS linking users in SHAPE with an operational HQ down to the highest level of national or multinational command. This applies to both inter- and intra-theatre communications. Annex Q follows a standard format that consists of the following five aspects:
 - (a) **NATO Strategic Communications (Strategic CIS).**³⁴ The strategic CIS infrastructure is comprised of the NGCS. The NGCS connects NATO and national defence networks. The strategic CIS infrastructure should provide a flexible, secure, and resilient network among involved NATO HQ. It should have sufficient capacity to provide all essential CIS mission needs. This network is extended to forward-deployed NATO HQ and eligible national/multinational HQ operating in accordance with MC 0593, MC 0195/9, and STANAG 5048.
 - (b) **North Atlantic Treaty Organization Deployable Communication and Information Systems.** The aim of DCIS is to provide communication services, core enterprise services, and COI services for the deployed HQs. NCISG is responsible for the provision of NATO DCIS capabilities as well as CIS operations and exercises planning and control.
 - (c) **National Defence Networks.** National defence networks provide the national communication infrastructure to support national defence requirements. They are nationally owned and operated. There are agreements between NATO and NATO nations regarding provision of NGCS services by national defence networks. NATO can request the use of

³⁴ This "strategic communications" does not refer to the strategic communications (StratCom) in AJP-3.10, Allied Joint Doctrine for Information Operations.

national defence network transmission capacity to support the mission.

- (d) **Tactical Networks.** Tactical networks link national/multinational HQ and equivalent HQ with their lower echelons and are a national/multinational responsibility. Interfaces between NATO strategic and national tactical communications systems are provided where operationally justified. NATO-owned, or provided, satellite links will be used for high command networks and links between HQ and national/multinational HQ or equivalent HQ. Satellite channels are provided from NATO resources or leased from NATO nations. Both means provide essential secure voice and limited data back-up communications.
 - (e) **North Atlantic Treaty Organization Services.** Common NATO services, as found in the C3 Classification Taxonomy, should be provided at the appropriate level. Those services can be provided in a number of security domains (e.g., NS, NATO Unclassified, and mission network environments), as endorsed by SHAPE and agreed to and funded by NATO HQ.
- (3) Once the CIS strategic architecture is defined, paragraph 5 of the OPLAN, along with Annex Q, "Communication and Information Systems," can be developed in coordination with the NCISG and NCIA planning staffs. The OPLAN also details the responsibilities of SHAPE and JFC staff involved in the operation, NCISG, and NCIA. The high level responsibilities are as outlined in Chapter 2.

i. **Plan Review**

- (1) Plan review is the final stage of CIS planning. This stage usually responds to major changes in the operational situation and is synchronized with changes to lower HQ supporting plans.
- (2) All plans have a limited period of validity due to the potential for changes to the circumstances upon which they are based. The purpose of the plan review stage is to ensure a plan remains valid in terms of continuing requirements, policy, and doctrine, and viable in terms of feasibility, suitability, and acceptability. Changes in the situation or the resources available may affect the CIS plan. Therefore, SHAPE J6 staff planners should analyze the scope and scale of any change and identify corresponding CIS changes.

0306. Other Considerations

- a. Each participating non-NATO entity will bring its own perspective to the operation. This makes it essential to establish a coherent baseline of understanding as a prerequisite for CIS planning. Based on their contributions to the mission, role within the coalition organization, and political caveats, non-NATO entities may or may not require communication between the JFC and the higher political and military organizations. Non-NATO entities will bring and contribute their own capabilities, to include CIS, to the extent that their leadership directs. Existing materiel and non-materiel interoperability between NATO, NATO nations, and non-NATO entities will differ according to the extent and currency of interactions with NATO and/or NATO nations. Each non-NATO entity participating in a NATO-led coalition mission will have different CIS capabilities and CIS levels of expertise. These may or may not enable ready interface, integration, and federation with primary NATO C2 and CIS used by a NATO HQ. In some cases, non-NATO entities may request bi-lateral CIS and services support from NATO, a NATO LN, or another mission partner to assist with their mission support objectives.
- b. **Lead Nation.** If the staff of a NATO HQ designated to lead a coalition mission is unable to meet coalition mission CIS coordination requirements with resources on hand, a NATO LN is expected to assist with coordination, creation, or provision of CIS management structures for that specific mission. All Alliance and coalition partners should engage continuously during the mission, or exercise, CIS planning process to facilitate early discovery and mitigation of materiel and non-materiel interoperability issues. Early identification of interoperability issues and conflicting implementation policies is critical to providing the commander and users across a coalition force a baseline of capability they will have to work with to achieve mission objectives at the start of operation execution. Non-technical issues, such as disclosure and releasability policies, have a greater effect on partner interoperability within a coalition than differences between technical aspects of CIS. Differences in doctrine, organization, training materiel, leadership and education, facilities, and personnel skill sets, and implementation policies between NATO, NATO nations, and non-NATO entities requires a robust liaison and collaboration structure at the JFC level to facilitate coordination of collective CIS operations.
- c. **Mission Network Relationships.** The option of allowing non-NATO entity personnel access to NS or NATO Unclassified security domains does not exist within NATO security policy. As a result, the inclusion of non-NATO entities in any NATO-led operation presents the commander

with a coherent C2 planning and execution challenge. To achieve unity of effort and peer-to-peer relationships within and across a coalition force, a commander may require establishment of a mission network in which all partners operate at the same mission-specific classification and releasability level using their respective CIS and C2 capabilities. When establishing a federated mission network, the generation and use of joining, membership, and exit instructions (JMEI) provide a required set of mission specific implementation guidance, policies, and best practices to present and future mission network contributors. Regular and frequent practice in establishing a federation of mission networks during exercises should improve NATO and NATO nation ability to establish and operate using current materiel and non-materiel capabilities in a trusted and secure federated mission network that is complementary and separate from the NATO member-only NS and NATO Unclassified domains. Practicing the establishment of a federated mission environment also contributes to common processes and best practices within NATO organizations that are consistent and coherent regardless of the theater of operations. The NATO Federated Mission Networking Implementation Plan will be the working framework for NATO, NATO nations, and non-NATO entities in an FMN environment.

CHAPTER 4

EMPLOYMENT OF COMMUNICATION AND INFORMATION SYSTEMS

0401. **Command and Control Environment.** NATO C2 services support information collection, situation assessment, decision making, collaboration, C2, and mission planning and execution. Coordinated and coherent C2 within a NATO-led mission is enabled by NATO CIS employed at the strategic and operational levels of command. National forces will provide CIS at the tactical level in support of mission C2. CIS and C2 services are composed of networks and systems able to meet the IERs of the mission commander both vertically and horizontally across the force in terms of functional and geographical scope, capacity, speed, quality, security, and event-specific releasability of information and data if conducting coalition operations with non-NATO entities. NATO CIS supports C2 of a mission or exercise from both static and deployable HQs configured and adapted to meet a unique set of conditions for effective and secure CIS support to a joint or NATO-led coalition force throughout the six phases of NATO operations.³⁵ The six phases of operations are indications and warning; assessment; response options development; planning; execution; and transition. CIS planners from NATO and supporting forces should be engaged and fully integrated in every aspect of horizontal and vertical collaboration during comprehensive preparation of the operational environment and operational design to ensure risks and assumptions regarding CIS support to operations and exercises are included in advance planning products for CONPLANS, standing defence plans, and crisis response planning OPLANS. Planning and preparation for employment of NATO CIS and C2 services is also informed and shaped by high-level NATO operational concepts; NATO policies and architectures; and lessons identified/learned from NATO operations and exercises as compiled in documents such as MC 0593, Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations, 23 February 2015.
0402. **Command Facilities.** A requisite HQ command facility can be static or deployable and may consist of HQ JOCs at the strategic and operational levels supported by national JOCs at the tactical level, as required. A HQ command facility provides the working environment and CIS support for the functional staff areas, base and transportation support, site utilities, personnel support facilities, physical security, and force protection. HQ CIS facilities should have well-trained

³⁵ For additional information regarding planning for future and current NATO tasks, refer to AJP-5, Allied Joint Doctrine for Operational-Level Planning; and ACO COPD Interim version 2.0, 4 October 2013.

personnel and formal procedures in place to be able to constantly monitor and assess CIS status and restore or repair CIS services, when required. SMC covers all layers from communications equipment to business processes. SMC requirements and processes for federated CIS should be thoroughly implemented. See Figure 4.1.

- a. **Static Command Facilities.** These facilities provide support for static HQ which are required to execute C2 of forces, as well as military and political consultation and cooperation for the entire spectrum of NATO's missions. The HQ should accommodate the commanders and their staffs and provide the requisite infrastructure and office equipment, including collocated JOCs, where appropriate.
- b. **Deployable Command Facilities.** These facilities may be established, at the operational and tactical levels, on airborne command and control posts as airborne command centres or as deployable ground and sea-based HQ and JOCs. They enable C2 of combined, joint, and single-Service operations by commanders and their staffs. Size and functional composition of deployable HQ and JOCs should be adaptable to mission, role, and level of command.

0403. **Communication and Information Systems.** Reliable and seamless exchanging and processing of information is essential for military and political decision making. CIS are composed of the following services:

- a. **Information Processing Services.** These services provide the support necessary to accomplish C2. They are further divided into core services and functional services. Core services provide the services common to all users. Functional services provide support for functional and special staff areas. Information processing services consist of data repositories and applications optimized to satisfy the needs of specific staff functions. Both core and functional services rely on information exchange, information assurance, and CIS life-cycle support services.
- b. **Information Exchange Services.** These services provide the core communication network services and the wireless communication transport services needed to access and disseminate information in support of political and military decision making. Information exchange services support the exchange of large quantities of information in diverse formats (e.g., voice, text, still image, video, and data) between geographically dispersed locations in a timely, reliable, and secure manner.

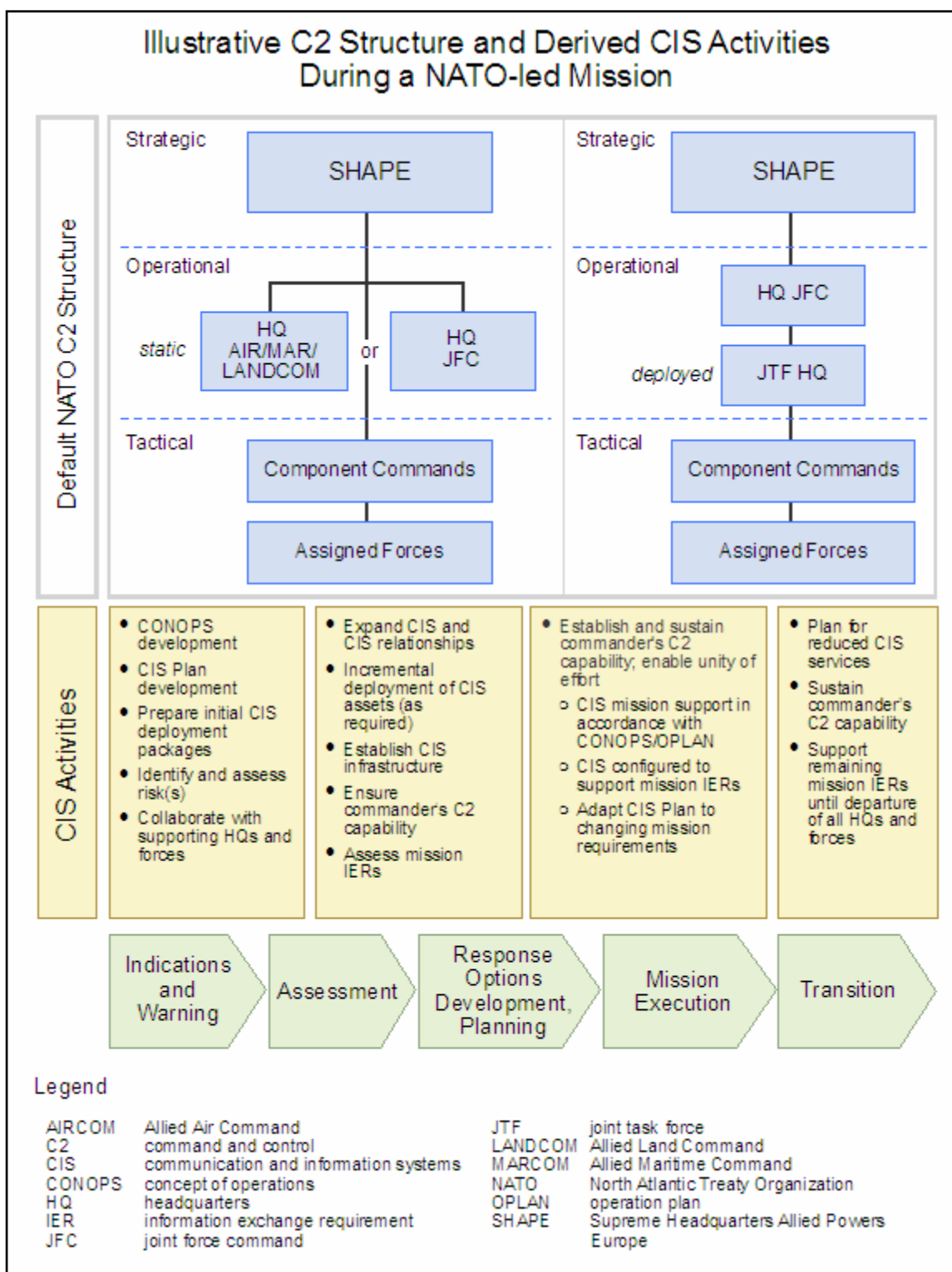


Figure 4.1. Illustrative C2 Structure and Derived CIS Activities During a NATO-led Mission

c. **Electronic Information Assurance Services**

- (1) Electronic information assurance services are required to provide information assurance measures, as part of a balanced set of security measures. To support security objectives, a consistent set of information assurance measures is required for all systems processing both NATO classified and unclassified information.
- (2) The goal of information assurance is to protect the security objectives of information through a variety of procedural, technical, and administrative controls. Information assurance includes a range of measures applied on a routine basis under the auspices of security policy to protect information. The information operations (Info Ops) staff, via the Information Operations Coordination Board and in coordination with others, can provide inputs to aid information assurance.³⁶

0404. **Exercises** are an integral part of education and training. NATO education and training is governed by MC 0458/3, NATO Education, Training, Exercise and Evaluation (ETEE) Policy, 3 September 2014; and managed via Bi-Strategic Command (Bi-SC) 75-2, Education and Training Directive, and Bi-SC 75-3, Collective Training and Exercise Directive. Bi-SC 75-2 introduces the Military Training and Exercise Programme as the management process to match NATO and nations' exercise requirements and opportunities, based on the priorities and intent of the strategic commanders. Bi-SC 75-3 recognizes the CIS support to all exercises, and also defines the purpose and scope of communications exercises. In reality, it is impossible to separate communications from information systems, and those from CIS security, and therefore is better to think of communications exercises as full-CIS events. CIS also play a substantial role in computer-assisted exercises, where CIS technology (including modelling and simulation) plays an additional role to stimulate decision making and training on C2 execution.

0405. **Predeployment and Deployment Considerations**

a. **Predeployment Activities**

- (1) During this time, the JFC is designated and forces are assigned. The NAC initiating directive provides the JFC with guidance to initiate planning. The JFC issues a mission statement and

³⁶ For additional information on the Info Ops staff and Information Operations Coordination Board roles and responsibilities, refer to MC 422/3, NATO Military Policy on Information Operations; and AJP-3.10, Allied Joint Doctrine for Information Operations.

commander's intent. Subsequent to the mission statement and commander's intent, the CONOPS is developed.

- (2) The objective of predeployment activities is to produce a CIS plan to support the commander's intent, mission, and CONOPS and prepare initial CIS deployment packages to provide a CIS deployment package developed to support an OPLAN. This OPLAN may have to consider en-route communications to support initial tactical entry.
- (3) To begin mission analysis and initial planning, the SHAPE and JFC J2, J3, J5, and J6 staffs should clearly understand the command relationships of the joint force.
- (4) This phase of the operation normally relies exclusively on the existing commercial, strategic, and tactical communications infrastructure.
- (5) Establish a battlespace spectrum management (BSM) cell to ensure sufficient spectrum resources are available to support deployment and mission activities. BSM is the practical coordination, consolidation, deconfliction, and allocation of all RF electromagnetic spectrum usage, as well as the identification and resolution of electromagnetic interference (EMI) within the operational environment. It is an integral part of supporting the theater commander in managing the overall operational environment. The BSM cell works with the HN or the organization that assumes responsibility for the RF electromagnetic spectrum. Refer to Annex C for additional information.

b. Deployment Activities

- (1) As the OPLAN is completed and published, CIS are expanded to provide improved information flow between the JFC and component commanders. As the joint forces deploy, CIS assets are extended into the JOA. These assets deploy incrementally in support of the build-up in the operational area. Initial CIS may be insufficient in capacity if not properly planned, coordinated, and employed.
- (2) The objective of CIS deployment activities is to provide for the continuous flow of information between commanders during the initial phases of the operation and establish the CIS infrastructure to support follow-on operations. The primary focus of initial CIS is to support the on-scene commander.

- (3) Available lift assets deploy the initial CIS capability. The initial CIS deployment package provides connectivity as well as the foundation to build the remainder of the network incrementally. CIS support should include reliable, redundant capabilities, in any environment, that ensure the commander is always able to maintain C2 of component and supporting forces.

c. **Redeployment Activities**

- (1) The end of an operation requires a force downsizing phase. Therefore, the SHAPE J6 staff should develop a CIS plan to reduce CIS services and resources accordingly. Throughout the drawdown, information services should continue to meet the operation's IERs for the remaining force elements until final departure.
- (2) Critical redeployment considerations are split between incoming replacement forces and HN coordination.
- (3) A BSM cell should ensure sufficient spectrum resources are retained in order to support redeployment operations. The BSM cell works with the HN or the organization that assumes responsibility for the RF electromagnetic spectrum.

ANNEX A

NORTH ATLANTIC TREATY ORGANIZATION ARCHITECTURAL FRAMEWORK CONSIDERATIONS

- A001. An **architecture** can be captured in a formal description of an instance, or configuration of people, processes, systems and organizations, connected by their interrelationships. An architecture description includes views showing various aspects of the architecture. The views include architectural elements and the relationships between elements as governed by a metamodel.
- A002. **NATO Enterprise.** The initial NATO Enterprise definition includes the NATO HQ (International Staff and International Military Staff), the NATO Command Structure, NATO Agencies, and interfaces to the Nations. An **enterprise architecture** is a formal description of a capability, or a detailed plan of the capability, at the level required to guide its implementation, including a description of the capability components, their interrelationships, and the principles and guidelines governing design and evolution over time. The role of enterprise architecture is to provide decision support for the use of resources (including processes and procedures) in the NATO Enterprise.³⁷ In other words, the architecture defines how resources support the strategy of the NATO Enterprise, and NATO goals and objectives.
- A003. An **architecture framework** is a foundational structure that can be used for the coherent development of a broad range of different architectures. It describes a method for designing the current and the target state of the enterprise in terms of a set of building blocks, and for showing how the building blocks fit together. There are multiple architecture frameworks in use, based on the type and model of the enterprise. Some of the most useful ones include:
- a. The NATO Architecture Framework (NAF).
 - b. Department of Defence Architecture Framework.
 - c. Ministry of Defense Architecture Framework.
 - d. The Open Group Architecture Framework.
 - e. The Zachman Framework.

³⁷ For additional information, refer to C-M(2014)0016, Alliance C3 Strategy.

- A004. The **NAF**³⁸ provides guidance to describe communication and information systems (or C3 systems) through architectures. It provides tools and techniques to design or analyse a system's architecture according to a designated set of roles and principles, using a somewhat holistic approach with architecture, operational, systems, and technical views. NAF defines a standard set of model categories (called "views") that each have a specific purpose. The NAF defines categories of views in terms of the domain they address (e.g., capability, operational, system, services, programme, and technical).
- A005. The use of an architectural framework (e.g., NAF) facilitates the development of military capabilities. It includes:
- a. Identification of capability gaps, with better capability integration.
 - b. Promotion of interoperability across NATO and in NATO Response Force scenarios.
 - c. Increased assurance that customer requirements are satisfied.
 - d. Reduction in risk for C3 capability and information and communications technology services capability.
- A006. An architecture framework provides guidelines on how to model and describe capabilities and supporting systems. In addition to a framework, it is advisable to adopt a common terminology or nomenclature for the building blocks that comprise the architectures to be modeled. As the NATO overarching architecture, the C3 Classification Taxonomy³⁹ provides a tool to harmonise C3 capabilities according to the Strategic Concept⁴⁰ and Political Guidance,⁴¹ through the NATO Defence Planning Process,⁴² to traditional CIS architecture and design constructs.
- A007. The **purpose of the C3 Classification Taxonomy** is to capture concepts from various communities and map them for item classification, integration, and harmonization purposes. The goal is to link political with military ambitions using mission-to-task decomposition, capability hierarchy, statements and codes, operational processes, information products, applications, services and

³⁸ For additional information, refer to AC/322-D(2007)0048, NATO Architecture Framework (NAF).

³⁹ For additional information, refer to AC/322-N(2012)0092-AS1, Consultation, Command and Control (C3) Classification Taxonomy, 19 June 2012.

⁴⁰ PO(2010)0169, NATO Strategic Concept.

⁴¹ C-M(2011)0022, Political Guidance.

⁴² PO(2009)0042, NATO Defence Planning Process (NDPP).

equipment to reference documents, standards, implementation programs, and fielded baselines. See Figure A.1.⁴³

- A008. **Operational Context.** The requirements for future C3 are not purely technical in nature. A framework for CIS services would only address the back-end technology solutions, and would not give any resolution about quality and quantity of services required for a particular mission. The C3 Classification Taxonomy starts with an “operational context.” The operational context describes the environment in which CIS capabilities are defined and used. It connects the strategic concept and political guidance of the Alliance through the NATO Defense Planning Process to the traditional CIS architecture and design constructs.
- A009. The Alliance’s political and military ambitions, the overarching guidance and policies, its level of ambition, and the mission-to-task decomposition are categorized under “missions and operations.” Then the needed capabilities are catalogued, operational (business) processes addressed, and relevant information products incorporated under “**operational capabilities.**” This information provides the organizational framework in which the CIS technology solutions will be deployed in order to achieve success in NATO’s future missions. Being part of the taxonomy could fuel the idea that there is causality in the different layers, and that the classification constitutes a certain hierarchy of data from top to bottom, and eventually into the technical domain. This is not the case. The layers are chosen as a comfortable grouping of datasets. There is a relationship between datasets and layers. Different datasets can be linked directly to all layers of the technical framework and not solely top-down from layer to layer.
- A010. Once the operational context is set, it should be linked to a technical framework of applications, services, and equipment. These “CIS capabilities” span two significant categories: “**user-facing capabilities**” and “**technical services.**” The relationship between these categories, and the separate layers within them, could be regarded as a hierarchical structure, from application down to physical layer.

⁴³ For the current version of this figure, refer to
https://tide.act.nato.int/tidepedia/images/2/2f/C3_Classification_Taxonomy.png

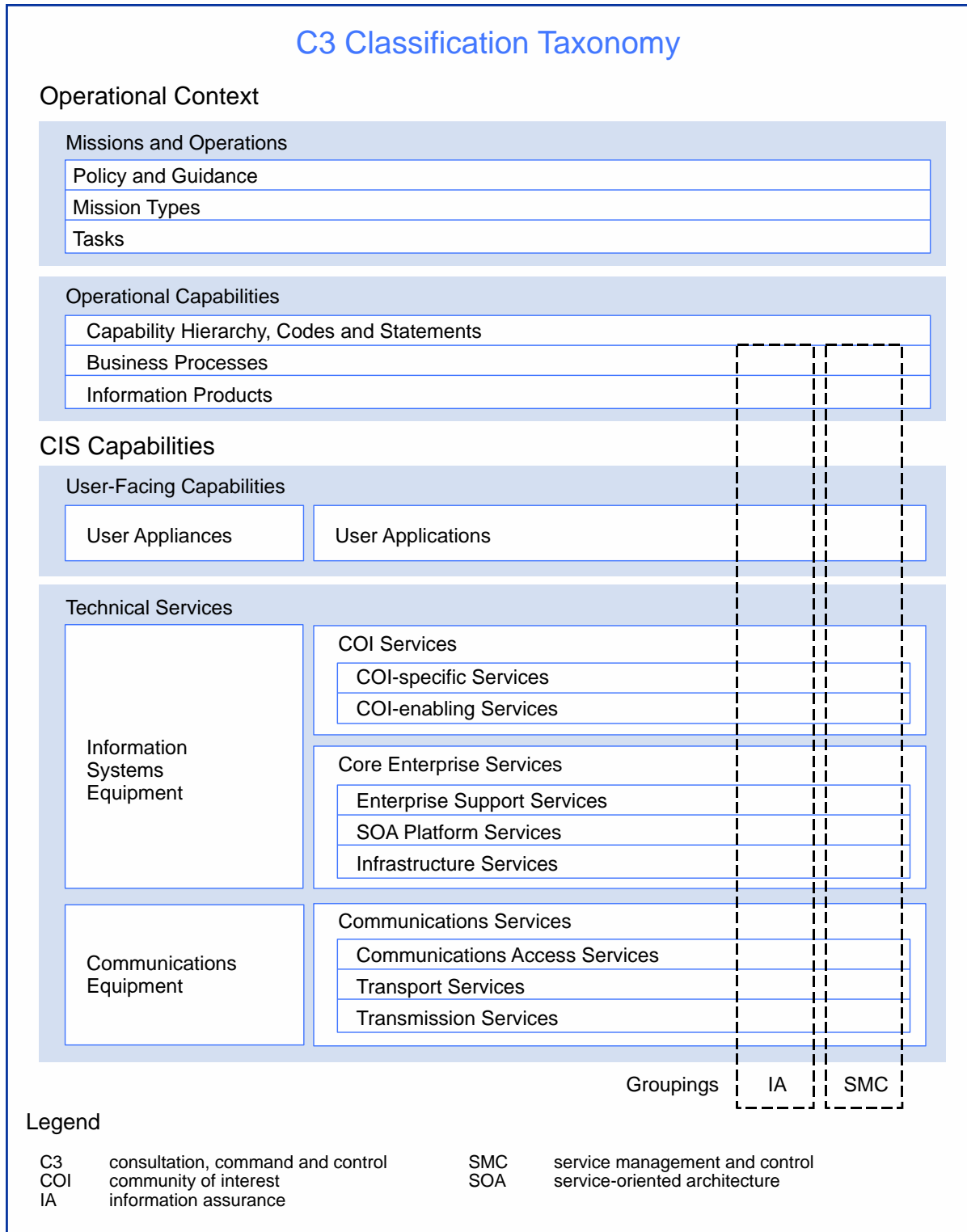


Figure A.1. C3 Classification Taxonomy

- a. **User-facing capabilities** provide an end user with “user applications” to use on “user appliances” to perform particular tasks or operations. User applications are computer software components designed to help a user perform singular or multiple related tasks. They run on user appliances and provide the logical interface between human and automated activities. User applications and their capabilities are defined without reference to particular technologies. These applications are stable and relatively unchanging over time, whereas the services used to implement them could change based on the available technologies and changing business needs. User appliances are instruments or devices for a particular purpose or use, and they provide the physical interface between the operator and the provided suite of user applications.
- b. **Technical Services** provide the foundation for NATO network-enabled capability. **NOTE:** This part of the taxonomy is often referred to as the original technical services framework of the NNEC Feasibility Study, notwithstanding the difference in service classifications. They provide a set of related software and/or hardware functionalities that can be reused for different purposes together with the policies that should control their usage. They should be implemented using a federated model that allows NATO and the Nations to jointly provide a robust and secure platform on top of which the user-facing capabilities can be run. Their requirements are derived from operational needs.

INTENTIONALLY BLANK

ANNEX B

JOINT CONSULTATION, COMMAND AND CONTROL INTEROPERABILITY⁴⁴

B001. Introduction.

- a. The objective of NATO interoperability is the ability to act together at all echelons of command to achieve Allied objectives.
- b. Systems interoperability, including cryptography,⁴⁵ is defined as the ability of systems to provide information and services to, and accept information and services from, other systems and to use the information and services so exchanged. There are three aspects of interoperability:

(1) **Syntactic** (technical) - achieved when two or more systems or components comply with the same specified communication protocols, message formats, and data formats to support an exchange of data.

(2) **Structural** - achieved when two or more systems or components are syntactically interoperable and all have agreed to communicate to produce and/or consume data in a structured exchange with the same information arrangement and granularity.

(3) **Semantic** - achieved when two or more systems or components are syntactically and structurally interoperable and all have the ability to automatically interpret the information exchanged meaningfully and accurately in order to produce useful results as defined by the end users of all systems or components.

Interoperability between systems is achieved and maintained during the development of new or substantially modified systems through: an architectural approach to system design, implementation of agreed standards and products, and application of a rigorous interoperability testing programme.⁴⁶

⁴⁴ For additional information, refer to AC/322-D(2015)0002, Alliance C3 Interoperability Policy, 17 February 2015.

⁴⁵ For additional information on cryptography, refer to B007 and IMSM-0504-2014, ACT Global Approach for Cryptographic Transformation, 19 May 2015 (NATO Unclassified).

⁴⁶ For additional information, refer to AAP-31, NATO Glossary of Communication and Information Systems Terms and Definitions.

- c. CIS interoperability is the ability of different CIS to work together to improve the way the JFC exercises C2 over assigned or attached forces. CIS interoperability is not an absolute condition. NATO CIS will normally be made up of the interconnection of diverse CIS designed with different national criteria that will have to be federated by employing various levels of interoperability (see section B002). Interoperability is difficult to achieve and sustain because of design, security, or national restrictions.

B002. The Levels of Interoperability. NATO interoperability policy defines the levels of interoperability in terms of information systems as follows.⁴⁷

- a. Level 0 – Isolated Interoperability in a Manual Environment. The key feature of level 0 is human intervention to provide interoperability. Systems are isolated from each other and there is a manual gateway (e.g., diskette, memory stick, tape, and hard copy exchange).
- b. Level 1 – Connected Interoperability in a Peer-to-Peer Environment. The key feature of level 1 is physical connectivity providing direct interaction between systems. There is an electronic connection but products must be homogeneous to be exchanged, and data is separated from applications (e.g., frequency modulated voice, tactical data links, and e-mail).
- c. Level 2 – Functional Interoperability in a Distributed Environment. The key feature of level 2 is the ability of independent applications to exchange and use independent data components in a direct or distributed manner among systems. Product exchange may have a heterogeneous nature and basic collaboration is supported (e.g., exchange of annotated imagery or maps).
- d. Level 3 – Domain Interoperability in an Integrated Environment. The key feature of level 3 is a domain perspective that includes domain data models and procedures where data is shared between independent applications that may begin to work together in an integrated fashion. While data is stored in shared databases, applications are still separated from the data. Collaboration can be more sophisticated (e.g., shared COP).
- e. Level 4 – Enterprise Interoperability in a Universal Environment. The key feature of level 4 is a top-level perspective that includes enterprise data models and procedures. Data is seamlessly shared among applications

⁴⁷ For additional information, refer to AC/322-D(2004)0040, NATO C3 System Interoperability Directive, 13 September 2004.

that work together across domains in a universal access environment. Collaboration among users is very advanced (e.g., interactive COP).

B003. The ways of achieving interoperability between two CIS may fall into one, or several, of the following categories:

- a. Technical Standards. These are rule sets that permit CIS to exchange information by establishing appropriate operational procedures, or by changing configurations. They are normally employed when designing, buying, or fielding new equipment. Standards can also be applied to technical or operational procedures.
- b. Operational or Configuration Procedures. These are rule sets that permit CIS to exchange information by establishing appropriate operational procedures, or by changing configurations.
- c. Gateways.⁴⁸ Gateways are communications or computer interfaces that solve the problems of technical or procedural interoperability. There are two main types:
 - (1) Technical Interface Gateways. These change the nature of the data in order to make it exchangeable between different CIS or equipment.
 - (2) Information Exchange Gateways. These serve to connect different security domains in order to check and filter the information that can be exchanged between them.

B004. Whenever it is possible to find procedures or configuration arrangements to enable the interoperability interface, the resulting interoperability will achieve level 3. Gateways, especially those implemented for interconnecting security domains, will achieve up to level 2. If these gateways cover technical interfacing, interoperability may also reach level 3. Finally, whenever interoperability requires manual manipulation of the information between systems (e.g., when implementing the “swivel chair” solution of STANAG 5048), interoperability may stay at level 0.

B005. The achievement of technical interoperability to match a commander’s needs requires significant effort by NATO and involved nations. To be effective, this activity should be conducted well in advance of deployment. When such activity has not taken place, the JFC may be faced with a combination of CIS that

⁴⁸ For additional information on gateways, refer to MC 0593, Minimum Level of Command and Control Service Capabilities in Support of Combined Joint NATO Led Operations, 23 February 2015.

technically cannot support the required interoperability to complete the mission. In these circumstances, the commander will be forced to accept lower capabilities and implement procedural solutions.

B006. For an Allied joint operation, the only way to generate a joint force with the appropriate level of interoperability is to anticipate, as much as possible, the identification, definition, and resolution of possible interoperability shortfalls. The evolution of the C2 structure to support the joint force, during the different phases of the operation, may not be known before carrying out the corresponding planning process. In this way, the interoperability requirements to fulfil the C2 procedures of the joint force may evolve in time to adapt to the changes in the C2 structure during the operation. This means that CIS, during a phase of the operation, may be required to connect with other CIS, and thereafter, be interoperable with it. During the next phase of the operation, the CIS may be required to connect with different CIS with different interoperability requirements.

a. Definition and Identification of Consultation, Command and Control Information Exchange Requirements.

- (1) The definition of the type of information to be exchanged is associated normally with a certain C2 procedure based on mission requirements. When a capability or force has been designed using an architectural approach, this information is defined as IERs within the corresponding operational view. Those requirements should contain the main interoperability elements expected for the capability, expressed in terms of the type of information, security classification, releasability, destination, and characteristics.
- (2) A C3 interoperability⁴⁹ requirement expresses the translation of the operational information of interoperability requirements into the technical requirements that will permit it to be exchanged by CIS. This translation will identify the type of C3 services the operational information requires to be properly exchanged according to the characteristics defined in the operational interoperability requirements (level of interoperability). In this translation process, it is necessary to take into account that C3 services are grouped in layers that form a structured hierarchy. This structure is depicted in the NATO Overarching Architecture. The main characteristic of this structure is that the exchange of C3 services corresponding to higher layers requires having assured previously the exchange of more basic services at the lower layers. The grouping of all C3

⁴⁹ For additional information on C3 interoperability, refer to AC/322-N(2009)0037-REV1, NATO C3 Interoperability Handbook for Expeditionary Operations.

services required to exchange certain information is known as a services interface.

- (3) A final step for defining C3 interoperability requirements is to identify the technical standards required for each C3 service within the services interface. All the technical standards that permit exchange of information by a services interface are grouped to form an interoperability profile.
- (4) Technical standards, in turn, will be expressed initially as services' interfaces, and then in interoperability profiles that group the required standards. Since interoperability requirements are associated with IERs that depend on the C2 structure of the force, and the C2 structure of the force evolves during an operation, IERs may change. This means the associated interoperability requirements may also change. This also assumes the forces, capabilities, or systems meet the defined interoperability requirements within the respective architecture or are included in the MMRs. The aim of the identification phase of the C3 interoperability process, therefore, is to translate operational C3 interoperability requirements to technical C3 interoperability requirements.
- (5) To enable the implementation of the resulting IERs, DCIS services should be provided in an interoperable manner.
- (6) When the composition of the HQ/forces that will carry out a NATO operation is not known, the only solution to identify and define C3 interoperability requirements is utilizing past experience with similar forces in NATO operations and exercises.

b. Resolution of Consultation, Command and Control Interoperability Requirements for Joint Forces.

- (1) Initially, the resolution of C3 interoperability requirements necessitates the appropriate definition of the requirement in technical terms. This definition can be completed whenever the characteristics of systems that are going to exchange services are known. With this prerequisite completed, solutions can be identified and evaluated to permit the exchange of required services.
- (2) This resolution analysis is completed when it is possible to test appropriately its suitability to fulfil the requirement. This testing

should be based on the technical characteristics the C3 interoperability interface is intended to perform.

- (3) In order to analyze and help mitigate mission partner interoperability issues, a number of assurance and validation initiatives or approaches can be followed (e.g., regular force certification interoperability exercises, and the Coalition Interoperability Assurance and Validation Working Group). Lessons learned and best practices, as identified by relevant COIs in support of exercise and missions, should be exploited to resolve these issues.

c. **Timing to Perform the Consultation, Command and Control Interoperability Process in Support of Consultation, Command and Control Interoperability for Joint Operations.**

- (1) For NATO forces that have been identified prior to being generated, the identification and definition of C3 interoperability requirements should start as soon as the identification of forces is known.
- (2) Troop-contributing nations and both national and NATO HQ staffs should identify their C3 interoperability requirements before, or no later than, the first force generation conference.
- (3) No matter how much force planning occurs, the joint force C2 structure will evolve to support the OPLAN. This means the C3 interoperability requirements process must adjust to fulfil changing requirements.

B007. **Cryptography.**⁵⁰ Cryptography is an essential tool in military communications. Cryptography provides a number of information assurance supporting services, including communications confidentiality, integrity, and availability. Other existing and emerging services (e.g., identity management, digital signature, or non-repudiation services) also rely on cryptography. In NATO, cryptography is used at all levels (i.e., from strategic to tactical, and in static and deployed) and for mostly all communication services (e.g., voice, video conference, real- and non-real time data). Cryptography is implemented through hardware and software products, and also should take into consideration crypto-related processes and procedures, policies, and key management (e.g., key generation, distribution, and dissemination). Cryptographic capabilities should support: securing

⁵⁰ For additional information, refer to IMSM-0504-2014, ACT Global Approach for Cryptographic Transformation, 19 May 2015 (NATO Unclassified).

information and information provisioning services; establishing the identity of users; and auditing operations over information and services.

INTENTIONALLY BLANK

ANNEX C

STRUCTURE AND RESPONSIBILITIES FOR SPECTRUM MANAGEMENT IN THE NORTH ATLANTIC TREATY ORGANIZATION

C001. **North Atlantic Treaty Organization Joint Spectrum Management.**

Electromagnetic emissions do not respect national boundaries or operational boundaries within a JOA. Failure to properly manage the RF electromagnetic spectrum within the operational environment could result in loss or degradation of important CIS, weapons, intelligence, surveillance, target acquisition, and reconnaissance systems. BSM is founded on the JFC's intent, and requires practical coordination and proper deconfliction of the RF electromagnetic spectrum within the JOA.

C002. **Spectrum Management in the North Atlantic Treaty Organization.**

Transmission assets should be coordinated at the strategic, operational, and tactical levels by national, international, military, and governmental agencies and staffs. They should also be coordinated with the formation of the emission control plan and its operation. Comprehensive management of the RF electromagnetic spectrum by trained persons ensures the most effective use of the spectrum within the joint force with the least impact of EMI.

C003. **Battlespace Spectrum Management - Introduction**

- a. NATO's ability to access, manage, and control the RF electromagnetic spectrum may be degraded by a variety of factors (e.g., Allies, adversaries, neutral organizations, and the civilian sector all compete within the HN for RF electromagnetic spectrum utilization; the HN may apply restrictions; and there may be limited access to the RF electromagnetic spectrum). To deliver an operational advantage, it is necessary to consider RF electromagnetic spectrum access during every stage of planning and develop plans to create the ability to manoeuvre freely within the RF electromagnetic spectrum. Without effective BSM and timely access to the RF electromagnetic spectrum, the ability to manoeuvre within the operational environment may be severely hampered and result in reduced operational advantage.
- b. In the JOA, spectrum managers should exercise authority over all operational users: military, coalition, and civil elements supporting the mission (e.g., media and IOs/NGOs) to ensure the available and/or

allowable RF electromagnetic spectrum is effectively allotted and/or assigned based on known HN restrictions or limitations.

c. **Principles of Battlespace Spectrum Management.** BSM is founded on the following principles:

- (1) **Sovereignty.** The RF electromagnetic spectrum is a sovereign resource. Therefore, coordination should take place with the HN administration prior to mission execution, if possible.
- (2) **Authority.** BSM authority should be established at the highest level of command (e.g., a joint force HQ) with the goal of forming a federated BSM structure that includes representatives from all staff branches operating in the electromagnetic environment.
- (3) **Deconfliction.** Where necessary, time and space deconfliction, if feasible, should be explored - thereby enabling effective allotment and assignment of the RF electromagnetic spectrum throughout the force.
- (4) **Delegation.** When possible, the authority to permit use of specific frequency bands should be delegated down to the lowest level of command – establishing “centralized control and decentralized execution.”
- (5) **Knowledge of the Electromagnetic Environment.** Sound BSM is dependent on detailed knowledge of the electromagnetic environment within the JOA.
- (6) **Agility.** BSM should be agile and responsive enough to be able to support critical phases of high-tempo operations. This is achieved, in part, by ensuring that spectrum managers, in consultation with the other staff branches, produce CONPLANS for potential alternate COAs.
- (7) **Effective and Efficient Use.** Given that the RF electromagnetic spectrum is an increasingly limited asset, any BSM process should be effective and efficient to maximize its use.

d. **The Battlespace Spectrum Management Function**

- (1) During the planning phase, RF electromagnetic spectrum access should be considered. Participating units should anticipate and identify all RF requirements necessary to support spectrum-

dependent systems. BSM functions, responsibilities, and engagements with the intelligence and operations communities should be identified.

- (2) Managing the operational environment, and hence BSM, is based on interpretation of the JFC's intent, operational priorities, and an intelligence assessment of the electromagnetic environment. Therefore, BSM is subject to J2 and J6 staff guidance and J3 direction.
- (3) The BSM cell within J6 operations should work closely with the J3. The JFC should, through the J6 staff, authorize the BSM staff to undertake the necessary level of spectrum management to ensure that a minimum number of restrictions are applied to friendly forces. Spectrum utilization negotiations with civil and international agencies are also the responsibility of the spectrum manager at the highest appropriate level. The result of successful BSM is a coordinated use of the RF electromagnetic spectrum by the force.

C004. **The Battlespace Spectrum Management Process.** To fulfil the BSM function, spectrum managers follow a defined process comprising a number of stages. The stages that follow the production and maintenance of the BSM plan are described below.

- a. **Maintaining a Spectrum Management Database.** In peacetime, general spectrum plans should contain as much information on RF electromagnetic spectrum administration and usage as possible. There are many sources for this information (e.g., exercises; previous operations; and terrain, chart, and propagation information). These plans are updated regularly. By combining the plans for a number of geographical regions, it is possible to determine core data upon which to build a BSM plan for a proposed JOA. Technical details of emitters of likely coalition partners and their concepts of use may be maintained in a similar fashion.
- b. **Defining the Spectrum Requirement.** Spectrum requirements should be estimated based on likely force composition together with experience from previous operations and exercises. As actual requirements are defined, estimates are refined. When the spectrum manager acts on behalf of the LN of a coalition force, the manager coordinates spectrum requirements across all components of the force. This may include other coalition partners, Allies, and IOs/NGOs. It entails compiling all coalition equipment specifications and force lists. This process is dynamic – as the force composition frequently changes – and continues through all phases of the

operation. This is also the time to consider what functions require protection from electronic countermeasures through inputs in the JRFL.

- c. **Identifying the Available Spectrum.** Accessibility and availability to the RF electromagnetic spectrum entails close liaison with HNs within the JOA and varies depending on the type of operation and entry. For example,
 - (1) When a legitimate friendly administration is in power, frequencies and frequency bands are requested in accordance with established national procedures.
 - (2) If the administration is not friendly, the spectrum manager may be required to manage the entire RF electromagnetic spectrum for the military and all other users.
 - (3) When a forced entry is made into a country and coordination between the spectrum manager and the civil authority is not possible, other methods may be required to determine unused spectrum. Some RF electromagnetic spectrum access may have to be on a non-interference basis. At this stage of the process, rules of engagement governing military RF electromagnetic spectrum use should be promulgated.
- d. **Producing the Battlespace Spectrum Management Plan.** Based on the information obtained above, a BSM plan is produced and forms the start-state for deploying into theatre. It includes frequency allotments and assignments for both communications and non-communications emitters. During all stages of plan development, the spectrum manager should maintain contact with the other staff branches to ensure that OPLAN changes are reflected in the BSM plan. The plan remains dynamic throughout an operation and should be issued on a regular basis to ensure all relevant RF electromagnetic spectrum users are informed.
- e. **Implementing the Battlespace Spectrum Management Plan.** Ideally, implementing the plan requires that the spectrum manager be continuously aware of the state of the RF electromagnetic spectrum throughout the operational environment. It is essential that this information be obtained from as many locations as possible because, in the land environment especially, terrain and propagation characteristics give rise to differing spectrum situations in different locations. This requires a monitoring capability with receivers as widely spread across the JOA as possible.

- f. **Reviewing and Updating the Battlespace Spectrum Management Plan.** As the operation develops, changes to plans and task organizations require changes to the BSM plan. Rules of engagement for the RF electromagnetic spectrum also need regular reviewing and updating.
- g. **Frequency Utilization.** The end product of the entire process is successful management of the RF electromagnetic spectrum in such a manner as to enable and protect friendly force operations, and provide an operational advantage over an adversary.
- h. **Electronic Warfare Integration**
 - (1) The BSM process produces a robust solution only if all active spectrum participants share information. It is essential that the EW community and spectrum manager establish a process to exchange requisite information. This process includes compiling the JRFL through coordination between the J2, J3, and J6 staffs. The JRFL is a management tool used by various operational, intelligence, and support elements to identify the level of protection desired for specific spectrum assets (e.g., nets, frequencies, and bands) in order to preclude those assets from being interfered with by friendly forces conducting EW. The JRFL is a “living” document that is updated regularly during the operation. While led by the J3, responsibility for JRFL compilation rests with the spectrum manager.
 - (2) The J3 specifies functions (e.g., C2 nets, navigation aids, and critical intelligence resources) that are to be protected. The J2 provides frequencies to be guarded while the J6 staff supplies the frequencies for the functions the J3 wants protected. The electronic warfare coordination cell/signals intelligence/electronic warfare operations centre (SEWOC) coordinates EW use of the RF electromagnetic spectrum with J2, J3, and J6 staffs.⁵¹
 - (3) The Info Ops staff, via the Information Operations Coordination Board, can provide advice and inputs for JRFL production and maintenance.⁵²

⁵¹ For additional information on electronic warfare coordination cell/SEWOC roles and responsibilities, refer to AJP-3.6(B), Allied Joint Doctrine for Electronic Warfare; MC 64/10, NATO Electronic Warfare (EW) Policy; MC 515, Concept for the NATO SIGINT & EW Operations Centre (SEWOC); and MC 521, Concept for Resources and Methods to Support an Operational NATO EW Coordination Cell/SIGINT & EW Operations Centre (EWCC/SEWOC).

⁵² For additional information on Info Ops staff and Information Operations Coordination Board roles and responsibilities, refer to MC 422/3, NATO Military Policy on Information Operations; and AJP-3.10, Allied

i. Electromagnetic Interference Resolution

- (1) EMI impedes operations and hinders mission accomplishment by degrading or limiting the effective performance of essential systems that utilize the RF electromagnetic spectrum. The proliferation of spectrum-dependent systems due to the increase of joint and combined operations and coalition support escalates the possibility of EMI incidents.
- (2) Affected users should report all EMI incidents and provide detailed information to analyze and assist with the resolution efforts. EMI should be resolved at the lowest level possible. Hence, spectrum managers possessing monitoring equipment should attempt to identify the source.
- (3) SEWOC support can also be requested to support EMI resolution efforts. Local efforts to resolve EMI incidents should be exhausted. However, when the capability to resolve EMI is not within the local spectrum manager's ability, it should be elevated to the next higher spectrum manager having authority.
- (4) When it is not possible to identify or turn off the offending signal, changing the victim's frequency assignment may be appropriate.
- (5) The timely and accurate identification, reporting, and resolution of EMI are key functions of BSM.

LEXICON

PART I – ACRONYMS AND ABBREVIATIONS

AAP	Allied administrative publication
ACO	Allied Command Operations
ACP	Allied communications publication
ACT	Allied Command Transformation
AJP	Allied joint publication
APP	Allied procedural publication
ASB	Agency Supervisory Board
Bi-SC	Bi-Strategic Command
BICES	Battlefield Information, Collection, Information and Exploitation System
BSM	battlespace spectrum management
C2	command and control
C3	consultation, command and control
CCD	Communication and Information Systems (CIS) and Cyber Defence
CIS	communication and information systems
COA	course of action
COI	community of interest
CONOPS	concept of operations
CONPLAN	contingency plan
COP	common operational picture
COPD	Comprehensive Operations Planning Directive
DCIS	deployable communication and information systems
DCOS	Deputy Chief of Staff
EMI	electromagnetic interference
EW	electronic warfare
FMN	Federated Mission Networking
HN	host nation
HQ	headquarters
IER	information exchange requirement
IM	information management
Info Ops	information operations
IO	international organization

JFC	joint force commander
JOA	joint operations area
JOC	joint operations centre
JRFL	joint restricted frequency list
LN	lead nation
MC	Military Committee
MCM	Military Committee memorandum
MMR	minimum military requirement
MOU	memorandum of understanding
MTWAN	maritime and mobile tactical wide area networking
NAC	North Atlantic Council
NAF	NATO Architecture Framework
NATO	North Atlantic Treaty Organization
NCIA	NATO Communications and Information Agency
NCISG	NATO Communication and Information Systems (CIS) Group
NGCS	NATO General Communications System
NGO	non-governmental organization
NIMP	NATO Information Management Policy
NNEC	NATO Network-Enabled Capability
NS	NATO Secret
OLPP	operational-level planning process
OPLAN	operation plan
RF	radio frequency
SACEUR	Supreme Allied Commander Europe
SEWOC	signals intelligence/electronic warfare operations centre
SHAPE	Supreme Headquarters Allied Powers Europe
SMC	service management and control
SMO	spectrum management office
SOR	statement of requirements
STANAG	NATO standardization agreement
SUPPLAN	support plan
WAN	wide-area network

PART II – TERMS AND DEFINITIONS

commonality

The state achieved when the same doctrine, procedures or equipment are used. (AAP-06)

compatibility

The suitability of products, processes or services for use together under specific conditions to fulfil relevant requirements without causing unacceptable interactions. (AAP-06)

concept of operations

A clear and concise statement of the line of action chosen by a commander in order to accomplish his given mission. (AAP-06)

control

The authority exercised by a commander over part of the activities of subordinate organizations, or other organizations not normally under his command, that encompasses the responsibility for implementing orders or directives. (AAP-06)

coordinating authority

The authority granted to a commander or individual assigned responsibility for coordinating specific functions or activities involving forces of two or more countries or commands, or two or more Services or two or more forces of the same Service. He has the authority to require consultation between the agencies involved or their representatives, but does not have the authority to compel agreement. In case of disagreement between the agencies involved, he should attempt to obtain essential agreement by discussion. In the event he is unable to obtain essential agreement, he shall refer the matter to the appropriate authority. (AAP-06)

electromagnetic interference

Any electromagnetic disturbance, whether intentional or not, which interrupts, obstructs, or otherwise degrades or limits the effective performance of electronic or electrical equipment. (AAP-06)

functional area

The area of responsibility within an organization where specific operational, administrative, or technical functions are performed. (AAP-31)

functional service

A service that provides a capacity to a specific staff function where the information content is closely related to the service. (AAP-31)

host nation

A nation which, by agreement:

- a. receives forces and materiel of NATO or other nations operating on/from or transiting through its territory;
- b. allows materiel and/or NATO organizations to be located on its territory; and/or
- c. provides support for these purposes. (AAP-06)

intelligence

The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity. (AAP-06)

interchangeability

The ability of one product, process or service to be used in place of another to fulfil the same requirements. (AAP-06)

interoperability

The ability to act together coherently, effectively, and efficiently to achieve Allied tactical, operational, and strategic objectives. (AAP-06)

joint operations area

A temporary area defined by the Supreme Allied Commander Europe, in which a designated joint commander plans and executes a specific mission at the operational level of war. A joint operations area and its defining parameters, such as time, scope of the mission and geographical area, are contingency- or mission- specific and are normally associated with combined joint task force operations. (AAP-06)

operation

A sequence of coordinated actions with a defined purpose. (AAP-06)

operations security

The process which gives a military operation or exercise appropriate security, using passive or active means, to deny the enemy knowledge of the dispositions, capabilities and intentions of friendly forces. (AAP-06)

reachback

The process of obtaining products, services, applications, forces, equipment, and material from sources external to the area of responsibility through the use of communication and information systems. (Not NATO Agreed, TTF approval pending)

tactical command

The authority delegated to a commander to assign tasks to forces under his command for the accomplishment of the mission assigned by higher authority. (AAP-06)

REFERENCE DOCUMENTS

AAP-06, NATO Glossary of Terms and Definitions
 AAP-31, NATO Glossary of Communication and Information Systems Terms and Definitions

AC/35-D/1040-REV 6, Supporting Document on Information and Intelligence Sharing with Non-NATO Entities, 21 August 2014
 AC/35-D/2002-REV4, NATO Directive on the Security of Information
 AC/35-D/2004-REV3, Primary Directive on CIS Security
 AC/322-D(2004)0040, NATO C3 System Interoperability Directive, 13 September 2004
 AC/322-D(2007)0048, NATO Architecture Framework (NAF)
 AC/322-D(2008)0031-REV1, NATO CIS Policy to Support Capability Management, version 1.3, 2 April 2009
 AC/322-D(2011)0015, NATO Network Enabled Capability Tenets and Principles, 4 July 2011
 AC/322-D(2014)0006, The NATO Enterprise Approach for the Delivery of C3 Capabilities and the Provision of ICT Services, 14 July 2014
 AC/322-D(2015)0002, Alliance C3 Interoperability Policy, 17 February 2015
 AC/322-N(2009)0037-REV1, NATO C3 Interoperability Handbook for Expeditionary Operations
 AC/322-N(2012)0092-AS1, Consultation, Command and Control (C3) Classification Taxonomy, 19 June 2012
 AC/322-N(2014)0072, Report on Cyber Defence Taxonomy and Definitions

Allied Command Operations Comprehensive Operations Planning Directive (ACO-COPD) Interim version 2.0, 4 October 2013
 ACO Directive 080-083, Allied Command Operations (ACO) Electronic Warfare (EW) Protection of Joint Restricted Frequency List
 ACO Directive 080-095, Communication and Information Systems (CIS) Planning Directive, 2 July 2014

ACP 200 (D) Volume 1, Maritime and Mobile Tactical Wide Area Networking (MTWAN) in the Maritime Environment – Operating Guidance
 ACP 200 (D) Volume 2, Maritime and Mobile Tactical Wide Area Networking (MTWAN) Technical Guidance, March 2015

AJP-01(D), Allied Joint Doctrine
 AJP-3(B), Allied Joint Doctrine for the Conduct of Operations
 AJP-3.3(A), Allied Joint Doctrine for Air and Space Operations
 AJP-3.6(B), Allied Joint Doctrine for Electronic Warfare
 AJP-3.10, Allied Joint Doctrine for Information Operations
 AJP-5, Allied Joint Doctrine for Operational-Level Planning

APP-15, NATO Information Exchange Requirement Specification Process

Bi-SC 75-2, Education and Training Directive, 2 October 2013 (NATO Unclassified)

Bi-SC 75-3, Collective Training and Exercise Directive, 2 October 2013 (NATO Unclassified)

C-M(2002)49-COR11, Security within the North Atlantic Treaty Organization, 28 May 2014

C-M(2007)0118, NATO Information Management Policy (NIMP), 11 December 2007.

C-M(2011)0020, NATO Cyber Concept

C-M(2011)0022, Political Guidance

C-M(2012)0049, Establishment of the New NATO Communications and Information Organisation

C-M(2012)0056, Politico-Military Advice on Command and Control Arrangements between SACEUR and the General Manager of the NATO Communications and Information Agency

C-M(2014)0016, Alliance C3 Strategy

C-M(2014)0061-AS1 - The NATO Enterprise Approach for the Delivery of C3 Capabilities and the provision of ICT Services

C-M(2015)0003, NATO Federated Mission Networking Implementation Plan (NFIP) version 4.0 Volume 1, 21 January 2015

IMSM-0583-2005, Bi-Strategic Command Concept of Deployable Communication and Information Systems (DCIS)

IMSM-0504-2014, ACT Global Approach for Cryptographic Transformation, 19 May 2015 (NATO Unclassified).

MC 64/10, NATO Electronic Warfare (EW) Policy

MC 0195/9, NATO Minimum Interoperability Fitting Standards for Communication and Information Systems (CIS) Equipment Onboard Maritime Platforms

MC 0458/3, NATO Education, Training, Exercise and Evaluation (ETEE) Policy, 3 September 2014

MC 422/3, NATO Military Policy on Information Operations

MC 515, Concept for the NATO SIGINT & EW Operations Centre (SEWOC)

MC 521, Concept for Resources and Methods to Support an Operational NATO EW Coordination Cell/SIGINT & EW Operations Centre (EWCC/SEWOC)

MC 0571/1, Military Concept on Cyber Defence

MC 0593, Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations, 23 February 2015

MCM-0032-2006, NATO Network-Enabled Capability (NNEC) Vision and Concept, 19 April 2006

MCM-0038-2005, Development of a NATO Network-Enabled Capability (NNEC)

MCM-0065-2012, Command and Control (C2) Arrangements between SACEUR and the GM of the NCIA

MCM-0106-2014 (REV 1), NATO Federated Mission Networking Implementation Plan, 14 August 2014

MCM-0125-2012, Future Mission Network Concept, 21 November 2012

PO(2009)0042, NATO Defence Planning Process (NDPP)

PO(2010)0169, NATO Strategic Concept

PO(2014)0358, Enhanced NATO Policy on Cyber Defence, 27 May 2014

SH/CCD J6/SM FCIS/394/15-305978, Deployable Communications and Information Systems Concept of Operations (DCIS CONOPS), 28 January 2015

STANAG 5048, The Minimum Scale of Connectivity for Communications and Information Systems for NATO Land Forces

STANAG 5524, NATO Interoperability Standards and Profiles (NISP)

STANAG 5525, Joint C3 Information Exchange Data Model (JC3IEDM)

STANAG 7149, NATO Message Catalogue (APP-11 Ed D)

INTENTIONALLY BLANK

AJP-6(A)(1)