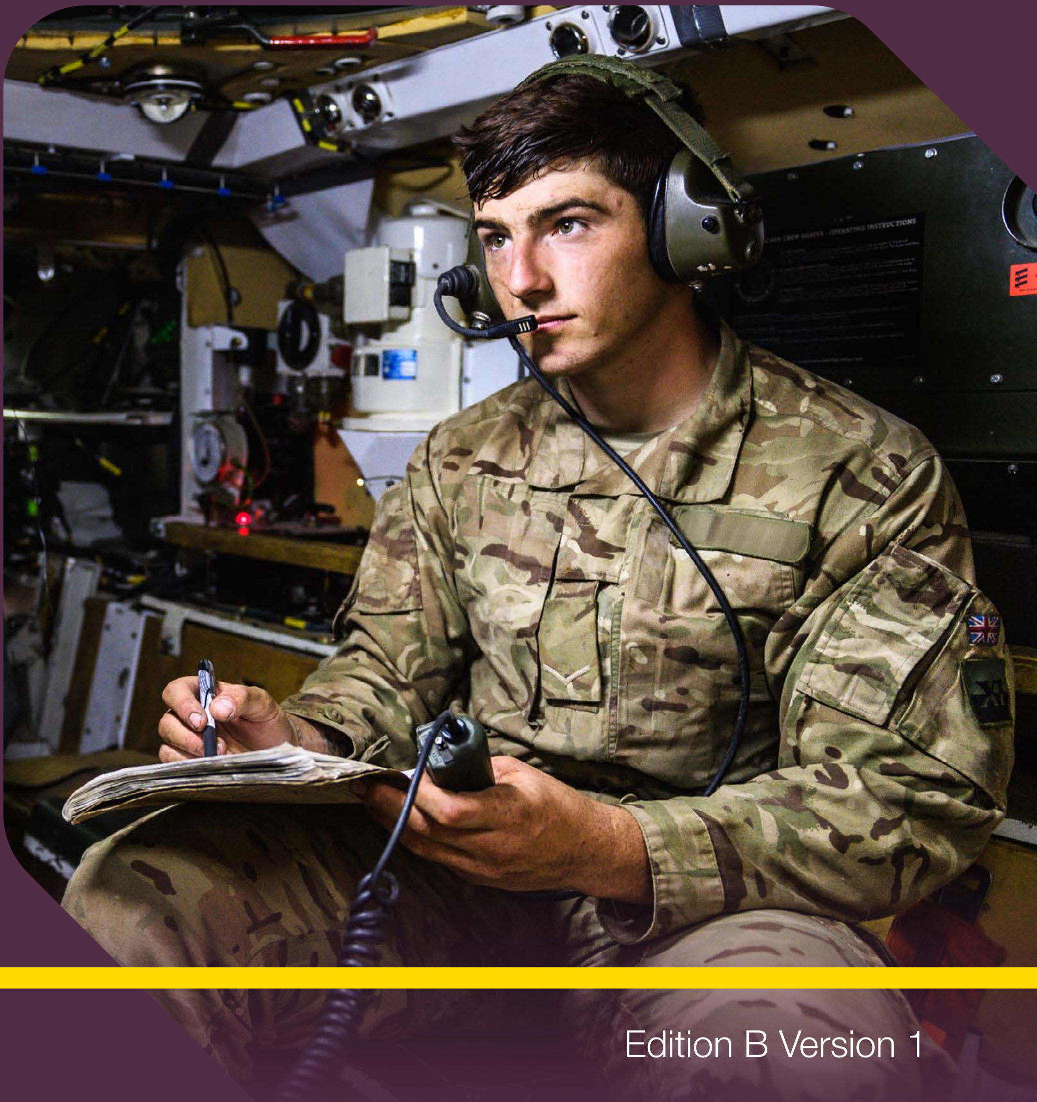
Ministry
of Defence

NATO
OTAN

Allied Joint Publication-6

Allied Joint Doctrine for Communication and Information Systems



Edition B Version 1

NATO STANDARD

AJP-6

ALLIED JOINT DOCTRINE FOR COMMUNICATION AND INFORMATION SYSTEMS

Edition B Version 1

with UK national elements

April 2024

NORTH ATLANTIC TREATY ORGANIZATION
ALLIED JOINT PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

Intentionally blank

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

5 April 2024

1. The enclosed Allied Joint Publication AJP-6, Edition B, Version 1, ALLIED JOINT PUBLICATION FOR COMMUNICATION AND INFORMATION SYSTEMS, which has been approved by the nations in the Military Committee Joint Standardization Board, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 2525.

2. AJP-6, Edition B, Version 1, is effective upon receipt and supersedes AJP-6, Edition A, Version 1, which shall be destroyed in accordance with the local procedure for the destruction of documents.

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

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

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

Intentionally blank

Allied Joint Publication-6

Allied Joint Doctrine for Communication and Information Systems

Allied Joint Publication-6 (AJP-6), Edition B, Version 1, dated April 2024, is promulgated in the UK in June 2024 with UK national elements as directed by the Chiefs of Staff

Director Development, Concepts and Doctrine Centre

Conditions of release

Authorisation

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

Copyright

If contacting Defence Intellectual Property Rights for authority to release outside of the UK government and MOD, the Patent Officer should be informed of any third party copyright within the publication.

Crown copyright and Merchandise Licensing, Defence Intellectual Property Rights, Central Legal Services, MOD Abbey Wood South, Poplar 2 #2214, Bristol, BS34 8JH. Email: DIPR-CC@mod.gov.uk

Distribution

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

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

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

Adopting NATO doctrine

The UK places NATO at the heart of its defence. In doing so the UK should strive to achieve maximum coherence and interoperability with, and between, our closest allies and partners. Where possible the UK will adopt NATO doctrine (Allied joint publications) rather than producing national doctrine (joint doctrine publications). Where it cannot, the UK will ensure it remains compatible. As a result the UK doctrine architecture comprises:

- NATO Allied joint publications distributed in the UK for use on coalition operations as appropriate;
- NATO Allied joint publications promulgated as UK national joint doctrine; and
- UK joint doctrine publications promulgated as UK national joint doctrine.

Where an Allied joint publication is promulgated as UK national doctrine, the cover will carry both the MOD and NATO emblems. These publications may contain UK national element additions, which explain a particular UK approach, clarify a UK definition, or aid understanding. These additions will be clearly identified as boxes with the UK flag icon. All photos and captions are also UK national additions. The original NATO text will not be modified. The UK additions take precedence where terms and processes differ.

Intentionally blank

Record of reservations

Chapter	Record of reservation by nations
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

Intentionally blank

Record of specific reservations

[nation]	[detail of reservation]
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

Intentionally blank

Summary of changes

Record of summary of changes for ALLIED JOINT PUBLICATION (AJP)-6 Edition B, Version 1
• Structured to include: Context, Scope, Purpose, Application, Structure and Linkages to provide overarching doctrinal guidance to integrate communication and information systems (CIS).
• Restructures contents to reflect Strategic, Operational, and Tactical-level roles and responsibilities.
• Harmonized document content with applicable related AJPs, to include AJP-6.1 (in development) and ensure consistency.
• Reduces redundancies and improves continuity between AJP-01 Allied Joint Doctrine, AJP-3 Allied Joint Doctrine, and AJP-5 Allied Joint Doctrine for the Planning of Operations.
• Introduces data centric security model.
• Updates references to NATO Command Structure and NATO Force structure.
• Updates communications and information operations as a part of cyberspace operations.
• Updates overall communications and information systems in support of operations.
• Adds section on tactical-level roles and responsibilities.
• Moves appropriate information from Annex A-North Atlantic Treaty Organization Architectural Framework Considerations, Annex B-Joint Consultation, Command and Control Interoperability, and Annex C-Structure and responsibilities for Spectrum Management in North Atlantic Treaty Organization to main document
• Deletes obsolete Annex A, Annex B, and Annex C
• Adds annex for alignment points with AJP-3, AJP-5 and AJP-6 for planning phases and operations stages.

Intentionally blank

Related documents

Reference

- NSO(JOINT)0741(2019) AJOD, Reporting of the 39th military Committee Standardization Board Allied Joint Operations Doctrine Working Group Meeting, dated 19 June 19.
- *Allied Joint Doctrine Campaign Plan* (AJDCP) 2019-2023, Edition1/19, 16 January 2019.
- ACT/JFD/JDLL/TT-2069/Ser:NU0414 *Request for feedback questionnaire to AJP-6 review*, dated 18 November 2019.
- AAP-47(C), *Allied Joint Doctrine Development*, dated 19 February 2019
- ACT/JFD/JDLL/TT-3011/SER: NU0161 *Virtual Data Fusion Workshop*, dated 15 October 2020.
- ACT/JFD/JDLL/TT-3329/SER:NU 0182 *Corrigendum to the Convening Order for the Data Fusion Workshop of AJP-6 Allied Joint Publication for Communication and Information Systems*.
- ACT/JFD/JDLL/TT-3744/SER: NU0381 dated 24 March 2021, STANAG 2525 – AJP-6(A) Allied Joint Doctrine for Communication and Information Systems
- *Federated Mission Networking (FMN) Management Directive*, Ver 2.0, 9 November 2018.

NATO Military Strategy

- C-M(2002)49-REV1, *Security within the North Atlantic Treaty Organization*, 20 Nov 2020.
- C-M(2007)0118, *NATO Information Management Policy* (NIMP), 28 January 2008.
- C-M(2011)0020, *Concept on NATO's Cyber Defence*, 09 March 2011.
- PO(2023)0036-FINAL (INV), Political Guidance for Defence Planning, 15 February 2023.
- C-M(2012)0049-ADD1, *Addendum to the Charter of the NATO C&I Organisation for AIRC2 and BMD Programmes*, 8 June 2015.
- C-M(2012)0056-AS1, *Politico-Military Advice on Command and Control Arrangements between SACEUR and the General Manager of the NATO Communications and Information Agency*, 2 July 2012.
- C-M(2018)0037-AS1, *Alliance Consultation, Command and Control Strategy*, 24 July 2018.
- C-M(2014)0061-AS1 - *The NATO Enterprise Approach for the Delivery of C3 Capabilities and the provision of ICT Services*, 24 November 2014.

- C-M(2015)0003-AS1, *NATO Federated Mission Networking Implementation Plan* (NFIP), 30 January 2015.
- MCM-0053-2019 (INV), *NATO Joint Military Operations in an Urban Environment*, 11 March 2019.
- MC 0640 (Final) (INV), *Minimum Level of Communications and Information Systems Capabilities at Land Tactical Level*, 24 July 2019.
- MC 0074/4(Final) (INV), *Military Committee Policy for Communications Security for NATO*, 22 May 2019.
- MC 64/11(Final), *NATO Electronic Warfare Policy*, 20 August 2018.
- MC 0195/12(Final) (INV), *NATO Minimum Interoperability Fitting Standards for Communication and Information Systems (CIS) Capabilities On-Board Maritime Platforms*, 07 February 2023.
- MC 0458/4(FINAL) (INV), *NATO Education, Training, Exercise and Evaluation (ETEE) Policy*, 3 January 2023.
- MC 0422/6(Final) (INV), *NATO Military Policy on Information Operations*, 21 November 2019.
- MC 0515/1, *Concept for the NATO SIGINT & EW Operations Centre* (SEWOC), 23 August 2010.
- MC 0521(Final), *Concept for Resources and Methods to Support an Operational NATO EW Coordination Cell / SIGINT & EW Operations Centre* (EWCC/SEWOC), 16 December 2005 .
- MC 0593/1(Final), *Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations*, 12 July 2017.
- MC 0648 (Final), *Military Committee Federated Mission Networking (FMN) Governance Directive*, 6 October 2017.
- IMSM-0583-2005, *Bi-SC Concept of Deployable Communication and Information Systems (DCIS)*, 14 November 2005.
- IMSWM-0391-2014, ACT Global Approach for Cryptographic Transformation, 24 September 2014.
- MCM-0065-2012, *Command and Control (C2) Arrangements between SACEUR and the General Manager (GM) of the NATO Communications and Information (C&I) Agency*, 19 June 2012.
- MCM-0106-2014 (REV1), *NATO Federated Mission Networking Implementation Plan*, 26 November 2014.
- MCM-0125-2012, *Future Mission Network (FMN) Concept*, 21 November 2012.
- MC 0628(Final), *NATO Military Policy on Strategic Communications*, 26 July 2017.
- MC 0665(Final), *Vision and Strategy on Cyberspace as a Domain of Operations*, 12 June 2018.

- IMSM-0222-2018, *High Level Taxonomy of Cyberspace Operations*, dated 22 June 2018.
- MC 0400/4, *NATO's Military Strategy Comprehensive Defence and Shared Response*, 22 May 2019.
- PO(2022)0200-REV9-AS1, *NATO Strategic Concept*, 28 June 22.
- PO(2022)0405 (INV), *NATO'S Digital Transformation Vision*, 07 October 2022.

Allied Command Documents

- AC/35-D/1040-REV6, *Supporting Document on Information and Intelligence Sharing with Non-NATO Entities*, 21 August 2014.
- AC/35-D/2002-REV5, *NATO Directive on the Security of NATO Classified Information*, 25 November 2020.
- AC/35-D/2004-REV3, *Primary Directive on CIS Security*, 15 November 2013.
- AC/322-D(2015)0009-AS1, *NATO Architecture Framework (NAF) v3*, 26 June 2015.
- AC/322-D(2008)0031-REV1-AS2, *NATO CIS Policy to Support Capability Management*, 3 February 2016.
- AC/322-D(2011)0015, *NATO Network Enabled Capability Tenets and Principles*, 4 July 2011.
- AC/322-D(2015)0014-REV4-AS1 (INV), *The NATO Enterprise Approach for the Delivery of C3 Capabilities and the Provision of ICT Services*, 6 July 2023.
- C-M(2015)0041-REV2, *Alliance Consultation, Command and Control Policy*, 20 December 2018.
- AC/322-D(2021)0017, *C3 Taxonomy Baseline 5.0*, dated 30 August 21.
- AC/322-D(2010)0036-REV1, *NATO Cryptographic Interoperability Strategy*, 16 May 2022.

Classification Taxonomy

- AC/322-N(2014)0072-AS1, *Report on Cyber Defence Taxonomy and Definitions*, 30 May 2014.

ACO Documents

- ACO Directive 080-083, *Allied Command Operations (ACO) Electronic Warfare (EW) Protection of Joint Restricted Frequency List*, 01 October 2009

- ACO Directive 080-095, *Communication and Information Systems (CIS) Planning Directive*, 2 July 2014.
- *Allied Command Operations Comprehensive Operations Planning Directive* version 3.0, 15 January 2021.

ACP Documents

- AC/322-N(2015)0123-AS1, Request for Endorsement of ACP 200V1 (D), *Mobile Tactical Wide Area Networking (MTWAN) in the Maritime Environment – Operating Guidance*, 31 August 2015.
- AC/322(CP/1)D(2015)0009, Request for Review of ACP 200 V2 (D), *Maritime and Mobile Tactical Wide Area Networking (MTWAN) Technical Guidance*, March 2015.

STANAGs

- 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).

Allied Administrative and Procedural Publications

- AAP-31, *NATO Glossary of Communication and Information Systems Terms and Definitions.*
- APP-15, *NATO Information Exchange Requirement Specification Process.*

Since Allied Joint Publication-6, *Allied Joint Doctrine for Communication and Information Systems* is one of the keystone NATO doctrine publications from which level-2 and -3 doctrine is derived, only the capstone and keystone doctrine publications are listed here. References to other doctrine publications are made in the text, where appropriate.

- AJP-01, *Allied Joint Doctrine*, December 2022.
- AJP-2, *Allied Joint Doctrine for Intelligence, Counter-Intelligence and Security*, July 2020.
- AJP-3, *Allied Joint Doctrine for the Conduct of Operations*, February 2019.
- AJP-4, *Allied Joint Doctrine for Logistics*, December 2018.
- AJP-5, *Allied Joint Doctrine for the Planning of Operations*, May 2019.
- AJP-10, *Allied Joint Doctrine for Strategic Communications*, March 2023.

Contents

Intentionally blank

Preface

Context

1. Allied joint publication (AJP)-6 provides the cornerstone for communication and information systems (CIS) supporting Allied joint operations.

Scope

2. Allied Joint Publication (AJP)-6 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 provides an outline of CIS portion, describes the characteristics of CIS, the overall structure of CIS, roles and responsibilities of CIS, command and control of CIS, and CIS security.

Purpose

3. AJP-6 is prepared under the direction of the North Atlantic Treaty Organization (NATO) Standardization Office/Military Committee Joint Standardization Board and provides a joint force commander with the guidance and information necessary to establish effective, resilient, and persistent CIS in, and for, an Allied joint force. AJP-6 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 focuses on the operational level, although it also has utility at the strategic and tactical levels.

Application

4. AJP-6 is intended primarily as guidance for joint NATO commanders and staffs. However, the doctrine is instructive to, and provides a useful framework for operations conducted by a coalition of mission participants. It also provides a reference for civilian mission participants.

Linkages

5. AJP-6 is a keystone publication directly subordinated to AJP-01. AJP 6 is also related to the rest of keystone documents, e.g., AJP-2, AJP-4, AJP-5 and, especially, AJP-10 and AJP-3. Note: Military Committee Joint Standardization Board (MCJSB) tasking NSO(JOINT)0204(2022)JSB was issued to establish AJP-6.1 *Allied Joint Doctrine for Communication and Information Systems Service Management and Control*.

TAC

Chapter 1

Chapter 1 provides an overview of communication and information systems, primarily intended as guidance for NATO commanders and staff to communicate between NATO users and participants when required.

> “The secret of war lies in communications.”
>
> Napoleon Bonaparte

Chapter 1

Overview of communication and information systems

Chapter 1 provides an overview of communication and information systems (CIS) primarily intended as guidance for NATO commanders and staff to communicate between NATO users and participants when required.

Section 1 – Introduction

1.1 CIS may embrace transmission systems, switching systems, user systems, and may include storage or processing functions in support of information transfer. The evolution from joint operations to multi-domain operations and the orchestration of effects across operational domains demands increased freedom of action in and through cyberspace. In this context, the resilience of digital capabilities critical for the accomplishment of military objectives becomes increasingly important. The relevance of digital technologies, data exploitation, and information sharing for the military instrument of power is significantly growing. Military activities are increasingly relying on digital capabilities and the underlying CIS infrastructures to deliver effects across the operational domains and to deliver military deterrence and defense. Fast adoption of digital technologies and the modernization of command and control (C2) and CIS systems are critical for integrating forces and capabilities and for maintaining NATO's technological edge. The Military Committee Joint Standardization Board (MCJSB) tasking

NSO(JOINT)0204(2022)JSB was issued to establish allied joint publication (AJP)-6.1 *Allied Joint Doctrine for Communication and Information Systems Service Management and Control*.

a. CIS is made up of the aggregation of multiple systems that have different technical, procedural, or security characteristics. However, they follow agreed standards and protocols for executing the proper operation of the CIS as a whole. These systems are fundamental for commanders to operate in accordance with the accepted principles. In particular, the CIS will provide the tools to clearly, rapidly, and securely store and distribute information. In order to provide these advantages, modern CIS must be properly used and protected. Safeguarding these systems requires not only technical solutions, but also administrative solutions (i.e., standardized information labelling, acceptable data format, etc). These administrative solutions are typically identified through the use of an information planning guide which has been tailored to a specific operation.

b. CIS have an essential role in supporting C2 at the operational levels (strategic, operational, tactical) and are a critical enabler for multi-domain operations. CIS requirements stemming from multi-domain operations grow in detail as the concept matures stated in the Alliance Concept for MDO is published on 10 March 2023 (SH/PLANS/SDF/23-012578).

c. CIS operations are an integral part of cyberspace operations. Military CIS enabling C2 of operations constitutes a critical part of the physical infrastructure which makes cyberspace relevant for alliance operations and missions.

d. CIS exploits or is reliant on the electromagnetic spectrum (EMS), which can provide a medium for transmission or a threat for interception or exploitation. CIS planning must be in accordance with the NATO EMS strategy.

e. A system, in CIS terms, is an integrated set of functions to support a capability – together with their materiel elements (personnel and other resources). It is rare that a complete capability is delivered by a single system in isolation. More commonly, complete capabilities are delivered by several interdependent systems. The implementation of a system (or components thereof) is the contributory elements of a fielded capability. The relationship between CIS, service management and control, and cyberspace defense is defined by AC/322 D(2016)0017, 10 NOV 2015.

Section 2 – Communication and information systems principles

1.2 **General information.** Information is a critical enterprise asset, and supporting CIS and services are essential to the proper conduct of C2. NATO and its Allies rely on the use of CIS to share information and function effectively.

1.3 **CIS guiding precepts.** In the context of NATO consultation, command and control (C3), crisis management, and NATO-led operations, the C3 Board articulated vision is to have mission-wide, secure, resilient, interoperable, valued C2 capabilities and CIS underpinning the NATO Strategic Concept. On this basis, the following precepts should be applied when operationally feasible:[1]

a. Enable seamless flows of information between static and deployable communication and information systems (DCIS) for the conduct of operations.

(1) DCIS seamless (interoperability) flows from deployable Division/Corps Command Posts to higher command static location.

(2) DCIS seamless (interoperability) flows from deployed Division/Corps Command Posts to lower deployed Division/Brigade Command Posts.

b. Focus on the criticality of information assurance to mission assurance.

c. Support the shift of focus from delivery of information and communications technology services to C2 capability provision.

d. Apply a life-cycle approach to manage information.

e. Integrate and satisfy short-, mid-, and long-term C2 requirements for translation into information and communications technology services in a coherent way which optimize roles and responsibilities, structures, and processes.

[1] For additional information, refer to C-M(2018)0037-AS1, *Alliance Consultation, Command and Control Strategy, 24 July 2018*.

f. Emphasize the need for a dialogue between users and requirement holders at all phases of the information life-cycle, particularly during implementation.

g. Address interoperability between C2 capabilities and information and communications technology services provided by nations, and multinational or common funded programmes prior to deployment.

h. Support all information security levels and multiple communities of interest (COIs).

i. Support cyberspace activities, as well as activities using cyberspace in peacetime, crisis, and conflict by providing situational awareness on the availability of CIS in support of mission critical C2 processes. Every CIS employed in the cyberspace domain must generate standardized logs that can be monitored and aggregated to produce a sound, consistent and updated picture of the cyberspace domain.

j. Federated mission networking (FMN) is the Alliance's approach to unifying coalition networks to provide information exchange services, enable information sharing among mission partners (MP), and guide the establishment of mission network relationships between NATO, NATO nations, and MPs in which to conduct the full range of operational activities within NATO-led operations.

1.4 **CIS characteristics.** To satisfy the principles in an efficient and effective manner, CIS should comply with a number of general characteristics. CIS characteristics are significantly impacted by the level of integration of emerging and disruptive technologies (EDT) as part of CIS/C2 systems. EDTs provide technical solutions to enhance those characteristics. In general, CIS should be:

a. **Capable.** CIS should be specified, designed, implemented, and operated so that it is able to meet the commander's information exchange requirements (IER) between deployed command posts task organized formations and static higher headquarters. 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 complete IER.

b. **Interoperable.** Effective joint and multinational operations require interoperable CIS that enable the operational commander 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 improve interoperability:

(1) Developing joint and coalition force CIS concepts within a NATO-led mission at the strategic/enterprise echelons and at the tactical/operational (Corps/Division and below) deployable echelons.

(2) Harmonizing the information, semantics, and development of data management.

(3) Providing and implementing agreed operational, procedural, and technical standards within a NATO-led mission.

(4) Delivering information and services to other force elements.[2] Within mission participants, the delivery of services and information is dependent on the mission; defined relationships and the ability of participants to operate CIS, and other material and non-material capabilities within the same mission; and the specific classification and releasability levels.

(5) Establishing common training and exercises for mission participants. Training focus areas include Joint Task Force headquarters and troop contributing nation responsibilities, CIS qualification and certification standards, and CIS training resources.

c. **Agile.** The agility of C2 is dependent upon the agility of CIS enablement. 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 operations with minimum disruption or delay. For example, while changes in posture 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

[2] For additional information, refer to AC/322-D(2015)0014-REV3-AS1, *The NATO Enterprise Approach for the Delivery of C3 Capabilities and the Provision of ICT Services*, 17 December 2015.

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. Supported/supporting relationships, combined with the use of a federated approach in CIS/COI service delivery would contribute to CIS agility.

d. **Scalable.** Scalability refers to the ability of CIS to accommodate changes in required size and quality. CIS must be able to grow in line with the demand, either for a greater number of communications nodes deployed or in the bandwidth and richness of services provided. 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.

e. **Service-oriented.** The C3 Services Taxonomy[3] 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 federated mission networking.

(1) In a service-oriented architecture, functions are independent services with well-defined interfaces at the strategic/enterprise echelons and at the tactical/operational (Corps/Division and below) deployable echelons. They can be used separately or in defined sequence.

(2) Some services allow people to enter or retrieve data while others are provided by one system to another. For instance, client-server systems may be reliant on storage, processing and network transport services provided by other systems. All of this is transparent to the user who works on the client application.

f. **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. Mission command principles

[3] For additional information on the C3 Services Taxonomy, refer to AC/322-D(2021)0017, *C3 Taxonomy Baseline 5.0*, dated 30 Aug 21.

also apply to CIS, which should be provided with sufficient CIS resilience and the necessary autonomy to conduct isolated C2 during wide-area communications outages.

g. **Timely.** During operations a wide range of information types are exchanged, some more time-sensitive than others. 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 that satisfies individual timeliness requirements in a cost-effective manner.

h. **Readiness.** CIS readiness refers to the level of preparation to accommodate an immediate requirement. In general, different NATO and national headquarters (HQ), and organizations are made available at different levels of readiness, commensurate with their role. Their allocated CIS should have a similar level of readiness.

i. **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. Security principles and best practice must be applied to the whole service lifecycle, from design, through operation to disposal.

j. **Resilience.** As part of force resilience, it is imperative that information systems focus on the protection, confidentiality, integrity, interoperability and availability of our own information. Resilience also requires the ability to defend in a contested cyberspace domain, and in the electromagnetic and acoustic spectra. 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.

Swedish and Italian marines on amphibious operations training conducted prior to Exercise Nordic Response 2024

© NATO

1.5 **CIS delivery support.** CIS supports the complete C2 process in NATO and operations where NATO participates, and as such there are a number of different classification approaches for CIS. The most frequent approaches are based on provision and location. CIS modules are supported by service management and control (SMC) as required.[4]

a. **Provision** looks at the C2 entity that owns and operates the CIS. It is common to distinguish between NATO and nationally-provided CIS. In general, NATO provides full CIS support ("Through" connectivity) of strategic-level activities of the NATO Enterprise[5] at the joint force command and component command level and above, and limited CIS support (*"To" connectivity*) to multinational static or deployed force structure component-command level HQ. In operational/tactical environments, the same principle will apply between different nations or C2 entities according to the hierarchical structure. Nations provide for the national elements of the static strategic networks, the core of the multinational HQ and units CIS requirements at component

[4] The plans, procedures and activities intended to contribute to the prevention of chemical, biological, radiological and nuclear incidents, to protect forces, territories and populations against and to assist in recovering from, such incidents and their effects (NATO Agreed, 31.10.2013/TTF 2012-0289).

[5] Per MC 0593/1 Minimum Level of Command and Control Service Capabilities In Support of Combined Joint NATO Led Operations. 12 July 2017.

command and below, as well as for the national deployed components. Frameworks which utilize a FMN approach allows for flexibility and agility of CIS service provisioning in operations.

b. **Location** typically distinguishes between the static and the deployed environments. Regardless of whether the CIS is static or deployed the operational commander has the flexibility to utilize the most appropriate CIS at their disposal.

(1) **Static CIS** is usually provided by the NATO General Communications System. Those information systems cover the full spectrum of services (i.e., communications services, core services to user applications/COI services).[6]

(2) **Deployed CIS** for each operation, mission planning determines the scope, in network size and services, which in turn drives the types of CIS building blocks to be deployed.[7] Building blocks include:

- wide area network (WAN) transmission;
- core communications services modules;
- information systems modules comprising core services of COI services and user applications;[8]
- distribution networks in different security domains;
- cross domain gateways;
- interface-to-nations modules;
- end-user equipment.

[6] There are other communication and information systems (e.g., Air Command and Control System, active layered theatre missile defence, and battlefield information collection and exploitation system that have static and deployable components but do not belong to the NATO General Communications System.

[7] For additional information, refer to SH/CyOC/PLANS OPL/34/2021-TT8414, *Deployable Communications and Information Systems Concept of Operations* (DCIS CONOPS) 2021, 15 July 2021.

[8] For additional information on the C3 Services Taxonomy, refer to AC/322-D(2021)0017, *C3 Taxonomy Baseline 5.0*, dated 30 Aug 21.

1.6 **Information management.**[9] Information management (IM) should be managed by organizing and controlling information throughout its life-cycle regardless of the medium and format in which the information is held. Good IM makes other tasks less complex and aides the commander's effectiveness and the speed of C2. Data-centricity is a rapidly evolving concept which recognizes data's valuable and versatile role in the larger enterprise. The concept treats information or data as the core asset where data exists independently of applications and can empower a broad range of information stakeholders. Additionally, this approach to security emphasizes the dependability of the data itself rather than the security of networks, servers, or applications. Enhanced protection of information regardless of where data resides or who it is shared with is critical. Data-centric security management necessarily depends on organizations knowing what data they have, what its characteristics are, and what security and privacy requirements it needs to meet so the necessary protections can be achieved. A critical function of IM is ensuring that aggregated data currently held at a lower classification does not necessitate a higher classification. The key principle of CIS IM is listed below, other principles are detailed in the NATO Information Management Policy.

a. **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. 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 need to share information to the maximum extent possible, without ignoring security principles. This should be managed to facilitate access, optimize information sharing and re-use, and reduce duplication.

[9] For additional information on the information life-cycle, refer to C-M(2007)0118, *NATO Information Management Policy (NIMP)*, 28 January 2008.

Information sharing must be in accordance with security, legal, and privacy obligations.[10]

b. **Information management plan.** 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 operations, a high degree of operational information exchange is required – both vertically and horizontally – between increasing varieties of entities. In order to exercise C2 over assigned NATO forces, there must be an effective and appropriate exchange of information between cooperating forces and/or headquarters. The IM Plan is the foundation for communications and 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 services for use in systems deployment, management, and restoration.

[10] 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-REV5, *NATO Directive on the Security of NATO Classified Information*, 25 November 2020; C-M(2002)49-REV1, *Security within the North Atlantic Treaty Organization, Enclosure E – Security of Information*, 20 November 2020; 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)*, 28January 2008.

(2) **Information exchange requirements.** IERs define the need for information exchange between two or more parties that support a given process. IERs are presented in Chapter 3, Section 5, paragraph 3.5.a.(2).

1.7 **Information assurance.** Information assurance consists of five elements of security: personnel security, physical security (including chemical, biological, radiation, and nuclear hardening[11]), security of information, CIS security, and industrial security.[12] For the purposes of this publication, only CIS security is defined.

1.8 **CIS security.** Communications security measures for people, process and technology are integral elements of all military CIS operations and should be considered throughout planning and execution. 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 is determined by the needs of CIS users, and the risk represented in transmission, storage and processing of the information balanced against the intrinsic security of the hardware and software.[13]

a. **Pillars of information assurance.** The three pillars of information assurance, the so-called CIA TRIAD, are to ensure:

(1) **Confidentiality.** Information is not made available or disclosed to unauthorized individuals, entities, or processes.

(2) **Integrity.** Information (including data) has not been altered or destroyed in an unauthorized manner. Moreover, only authorized entities should be able to modify an information (including data) in specific authorized ways."

(3) **Availability.** Information is accessible and usable upon demand by an authorized individual or entity.

[11] AEP-7 (STANAG 2521) provides the guidelines to ensure that material used on the battlefield will survive CBRN hazards and can be operated by personnel in a protective posture. Furthermore, it offers information regarding the impact of decontamination on design and materials.

[12] For additional information on information assurance, refer to C-M(2002)49-REV1 20 Nov 2020 *Security within NATO, Enclosure F*, 20 November 2020.

[13] For additional information on information assurance, refer to C-M(2002)49-REV1 20 Nov 2020 *Security within NATO, Enclosure F*, 20 November 2020.

b. **Security by-products.** 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 a person or an entity.

(2) **Non-repudiation**. The measure of assurance to the recipient that shows that information was sent by a particular person or organization, and to the sender that shows that information has been received by the intended recipient(s).

c. **CIS Infrastructure operations.** CIS Infrastructure Operations are actions taken to employ, secure, operate and maintain CIS in a way that creates and preserves data availability, integrity, and confidentiality, as well as user/entity authentication and non-repudiation. CIS infrastructure operations contributes to the overall CIS security plan,[14] so NATO has adopted a comprehensive approach to CIS security, integrating incident response, countermeasures, preventive CIS security measures, and user awareness to protect NATO networks.

Risk and vulnerabilities

UK 1.1. **Risks.** There are numerous definitions of risk, with most centring on the possible future outcome of events in terms of their likelihood of occurrence and the impact they would have on individuals or an organisation. Risk cannot be eliminated from any activity; however, it must be recognised and managed. Joint Service Publication (JSP) 892, *Risk Management* defines risk as: an uncertain future event that could affect the Department's (MOD's) ability to achieve its objectives.

UK 1.2. **Vulnerabilities.** The UK National Cyber Security Centre (NCSC) describes a vulnerability as 'any weakness in a system that can be exploited by a threat actor, or can be affected by a hazard'. Vulnerabilities can occur through flaws, features or user error, which attackers will look to exploit, often in combination, to achieve their goals. Beyond the immediate technical aspects, vulnerabilities may also be induced through interaction with the operating environment, the nature of the task and human factors. Recognising and appreciating vulnerabilities is critical to the process of identifying the level of risk and implementing appropriate procedures to

[14] For additional information on information assurance, refer to C-M(2002)49-REV1 20 Nov 2020 *Security within NATO, Enclosure F*, 20 November 2020.

manage that risk effectively. This is especially crucial in areas where Defence has a degree of reliance on civilian commercial infrastructure that is not under its direct control. Mitigation can be achieved through adoption and implementation of the 'secure by design' philosophy, together with using accredited suppliers and employing appropriate encryption and agile spectrum management. To be effective, such measures must be undertaken within the context of a robust and comprehensive cybersecurity culture.

1.9 **Communication and information services.** 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 COI services. Core services provide the services common to all users. COIs 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 COI services rely on information exchange, information assurance, defensive cyberspace operations, 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.

c. **CIS security services.** These services provide 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 confidentiality, integrity, availability, authentication and non-repudiation. These measures must produce standard log files, which must be aggregated and correlated in

Security Information and Event Management systems[15], fundamental to generate and contribute to consistent cyberspace situational awareness.

d. 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 staff, via the Information Operations Coordination Board and in coordination with others, can provide inputs to aid information assurance.[16]

(3) Cryptography assures the confidentiality and integrity of communications. 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 information and information provisioning services, establishing the identity of users, and auditing operations over information and services. The coordination of all cryptographic efforts will be provided by an operational commander's senior staff.

[15] Software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.

[16] For additional information on the Information Operations staff and Information Operations Coordination Board roles and responsibilities, refer to MC 0422/6, *NATO Military Policy on Information Operations*, 21 November 2019; and AJP-10.1, *Allied Joint Doctrine for Information Operations*.

UK 1.3. Cyber mission assurance (CMA) is defined as: a process to protect or ensure the continued function of capabilities and assets that are critical to the execution of a mission.[1] CMA is an activity that aims to improve both the cyber resilience and availability of these critical capabilities and assets. Through Operation Augite permissions and authorities, Defence Digital Director Operations has standing CMA authorities over federated cyber force elements, including cyber information services operating centres (CyISOCs), delivery teams, managed service providers and parts of the supply chain. For specific operations, Chief of Joint Operations may appoint Defence Digital Director Operations as a component commander, extending their authorities to direct, coordinate and cohere defensive measures in direct or indirect support of operational capabilities.

[1] Joint Doctrine Publication (JDP) 0-01.1, *UK Terminology Supplement to NATOTerm*.

1.10 **CIS and services prioritization.** Derived from the necessary information inputs and outputs to their processes and activities, all "information consumers" and “information producers” should use information flow analysis to describe their IERs as a basis for information flow management. CIS discipline requires the identification and prioritization of information flow consistent with the projected rate of activity and scope of operations. Since available CIS and/or services may be limited and will have a finite capacity, commanders at all levels should prioritize their information requirements within the IM plan. CIS services prioritization should be linked to mission-critical processes and should provide context for CIS service restoration priorities and for C2/CIS resilience requirements. This prioritisation will also inform the planning of cyberspace operations.

Aircrew from Canada, Denmark and Italy monitor the skies over Poland in their E-3A Airborne Warning and Control System aircraft

© NATO

1.11 **Economy of CIS employment.** Economy of CIS employment is achieved by avoiding unnecessary duplication (not withstanding resilience requirements and cyber defence compliance), carefully defining and managing user requirements, and strict transmission discipline. 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 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, participants[17] 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.

Section 3 – Communication and information systems in support of operations

CIS in support of operations

1.12 **Command.** 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.

1.13 **Control.** Control is inherent in command. To control is to regulate forces and functions to execute the commander's intent. To achieve this, the operational commander 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 mission participants.

[17] 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.

1.14 **Capabilities of the available CIS.** For the commander to exercise effective command and control across their subordinates, and their staffs, they will be reliant on a range of CIS, and will depend on their own CIS staff to provide advice on the most effective C2 system. C2 systems must provide commanders with the ability to make decisions and control activities. 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 to achieve mission objectives. Furthermore, joint C2 CIS architectures must be able to adjust in support of changes to the command support structure. Review of available CIS capabilities should consider:

a. Implications of reachback

(1) Reachback is the process of obtaining products and advice from experts outside the theatre of operations. Reachback expands the capability of an operational level HQ by virtual means without expanding its footprint while reducing the footprint of the operational level HQ - without degrading efficient, effective, and timely support to operational and tactical level forces. Additionally, reachback provides operational forces with a data analysis/data science capability.

(2) The effectiveness of reachback relies upon provision of robust and resilient CIS services that adapt to mission requirements in congested, contested, degraded, or denied electromagnetic environment. The J6 staff should be aware of CIS capabilities and limitations and should adjust resource allocation to support the commander's C2 needs and escalate to the commander where CIS may place constraints on the operational plan.

b. A DCIS support group coordinates the DCIS deployment and facilitates CIS management and network control. Activities that are critical to NATO CIS should be fully coordinated with the joint operations centre.[18]

[18] For additional information on support of a deployed operational-level HQ, refer to MC 0593/1, *Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations*, 12 July 2017.

c. To meet the operational commander's C2 requirements, the J6 staff should lead the planning, coordination, and execution of CIS architectures and joint operations area CIS.

d. The cyberspace theatre component in coordination with intelligence staff and cyberspace security element, identify CIS vulnerabilities and cyberthreats. Continuous cyberspace information sharing, amongst allied forces, leads to a common understanding of threat indicators and aides in the development of codified tactics, techniques, and procedures to protect coalition CIS. Cyberspace security element develops CIS security plans and support the development of operations security plans. J6 planners in coordination with Cyberspace security element ensure the readiness of recovery and consequence management plans and procedures to be executed by service providers. Additionally, the J6 planners assesses the impact of adversary activities on coalition CIS and takes part in the production of the joint restricted frequency list, through the Theatre Spectrum Management elements inside J6, under the responsibility of the J3 (operations) staff. The J6 staff coordinates specialist support relating to protection of friendly CIS.

e. J6 planners control and coordinate use of the radio frequency EMS for a wide array of communications and electronics resources.[19] In some nations, electromagnetic warfare planning and coordination are carried out by the J6 planners.

f. The exchange of liaison officers for CIS may improve mutual understanding, unity of purpose, and action. These officers will be assigned at the discretion of the operational commander.

[19] For additional information, refer to AJP-3.6(B), *Allied Joint Doctrine for Electronic Warfare*; AJP-10.1, *Allied Joint Doctrine for Information Operations*, and ACO Directive 080-083, *Allied Command Operations (ACO) Electronic Warfare (EW) Protection of Joint Restricted Frequency List*, 01 October 2009.

Contractor support to operations

UK 1.4. Contractor support to operations covers all forms of contractor support and encompasses: contractors deployed on operations (CONDO); contractor logistic support, where in-service equipment is maintained under contract with the equipment provider; and the use of contractors through the Permanent Joint Headquarters (PJHQ) contractor logistic contract, where a range of services are provided from a long-term commercial contract. The increase of long-term partnerships with industry, through private finance initiative to deliver military CIS capability, has seen civilian staff become fully integrated into all layers of information services provision.

UK 1.5. While commercialisation and contractorisation of CIS capability may offer considerable benefits, including the potential regeneration of military capability, and a more cost-effective and capable solution, they can create additional operational risk. Commercial solutions are unlikely to be suitable in mobile, hostile or austere environments, and contractorised solutions may impose an additional force protection burden.

UK 1.6. The feasibility of a commercial or contractorised solution depends on operational circumstances and a detailed assessment of the potential risks and benefits. It is necessary to be clear in advance on the status of contractors, including their status under military law, the impact of any memoranda of understanding with a host nation (regarding their employment) and whether they are subject to a status of forces agreement. Operational circumstances may preclude the use of contractor support to operations and contractors may choose not to deploy their personnel into high threat or austere environments.

Section 4 – Overall objectives and principles of communication and information systems

1.15 **Objectives of cooperation.** The objectives of cooperation are to provide NATO-wide, cost effective, interoperable, and secure C2, supported by CIS that can ensure high-level political consultation and C2 of military forces. A federation of NATO networks, securely connected with national fixed and mobile networks, link all HQ of the NATO command structure, national capitals, and national military commands. The systems also enable secure connections between mission participants, where NATO leads such coalition operations.

a. **Federation.** FMN is the preferred way to achieve interoperability, seamless secure human-to-human information exchange, a single view of the battlespace, and timely provision of mission network services through a federated mission network. Through federation different CIS can operate with each other without requiring additional or external measures from those implemented when they were designed; these systems should be considered an 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 troop contributing nations. Federation may occur between mission participants, at a specific classification and releasability. This will still deliver the benefits of unity of effort and speed of command compared with each running isolated networks and exchanging information procedurally.

(1) In a FMN framework, a federation of different systems allows information sharing between them at a greater capacity than the sum of the individual systems acting in isolation. Every participant to the mission network manages its own portion of it. Nonetheless to adhere to the federation a set of well-defined rules (defined by the network management authority) needs to be respected.

(2) In a FMN framework at the tactical/operational levels the deployed command posts at Corps/Division and below may established a common services hub implementation where the lead nation centralizes the services for the task organized Brigades/

Divisions. This is a priority for operations in large scale combat operations.

(3) A FMN is a single governed capability, established using a flexible and tailored set of non-material (can include management, policy, processes, procedures, and standards) and material contributions (can include static and deployed networks, CIS, services, and supporting infrastructures) provided by mission participants.

(4) When employed in a FMN environment, mission network CIS should also comply with the following principles: cost effectiveness; maximum reuse; cyber defence compliance; reflect NATO network-enabled capability tenets; reflect C3 taxonomy; incremental approach; support an uncertain future; use network standards; support dynamic federations; and be information centric.

(5) Compliance with the NATO FMN framework architecture will sustain and direct the coordination and management of the federation of the national individual systems, facilitating the continuous interoperability.

b. **System characterization.** Each of the specific CIS aggregated to conform to the federated NATO CIS can be described from operational, technical or security viewpoints. 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 approaches used in other services or military functions. In this regard, NATO CIS can be classified as:

(1) NATO Static CIS.

(2) NATO Deployable CIS (DCIS).

(3) CIS provided by nations in support of NATO operations.

(4) CIS provided by partners in support of NATO-led coalition operations that involve participants.

c. **The NATO architecture framework.**[20] The NATO architecture framework (NAF) provides guidance to describe system and service architectures to aid design and interoperability between NATO and allied nations. 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 for a specific echelon. The NAF defines categories of views in terms of the functions they address (e.g., capability, operational, system, services, programme, and technical).

(1) 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 modelled. As the NATO overarching architecture, the C3 Classification Taxonomy[21] provides a tool to harmonize C2 capabilities according to the Strategic Concept[22] and Political Guidance,[23] through the NATO Defense Planning Process[24], to traditional CIS architecture and design constructs.

d. **CIS services.** In line with the Alliance C3 Strategy,[25] CIS planning, provision, and operation is articulated in terms of services. Services express the functionalities CIS offer to the user, saving them the need to manage the underpinning technical dependencies. The C3 Services taxonomy[26] captures concepts from various communities and maps them for item classification, integration, and harmonization purposes. The C3 taxonomy defines the following services categories:

[20] For additional information, refer to AC/322-D(2021)0017, *C3 Taxonomy Baseline 5.0*, dated 30 Aug 21.

[21] For additional information, refer to AC/322-D (2021)0017, *C3 Taxonomy Baseline 5.0*, dated 30 Aug 21.

[22] PO(2022)0200-REV9-AS1, *NATO Strategic Concept*, 28 Jun 22.

[23] PO(2023)0036-FINAL (INV), *Political Guidance for Defence Planning*, 15 Feb 2023.

[24] PO(2009)0042, *NATO Defence Planning Process (NDPP)*.

[25] For additional information, refer to C-M(2018)0037-AS1, *Alliance Consultation, Command and Control Strategy, 24 July 2018*.

[26] For additional information on the C3 services taxonomy, refer to AC/322-D (2021)0017, *C3 Taxonomy Baseline 5.0*, dated 30 Aug 21.

(1) **Communications services.** Communications Services interconnect systems and provide for the physical transfer of information across different media between originator and recipient.

(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) **COI services.** COI services provide functionality as required by user communities in support of NATO activities. COI services are primarily meant to directly support and enable user applications and service consumption.

(4) **User applications.** Communications, core, and COI services compose the 'technical services' layer of the C3 Taxonomy. 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.

e. **Communication and information domains.** The information processed on CIS is normally partitioned into security domains based upon the need-to-know and security clearances of the user groups. Some systems may also employ separate domains for management and monitoring traffic. It is common for all three types of domains to exist within the same operation. In NATO, domains are used for different purposes; therefore, domain taxonomy is required. The domains listed below may each support multiple network environments that operate at different security and releasability levels. In the context of NATO joint operations, the typical domains for CIS (not to be confused with the operational domains as defined in AJP-01) networks which are frequently utilized are:

(1) **NATO domain.** The security rules and implementation policies for this domain are established by NATO and apply not only to deployed forces, but also to all NATO CIS and is subject to NATO technical and management policies.

(2) **Mission domain.** The Mission domain, enabled by FMN principles and products, is the main Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) environment to be used for mission execution in NATO-led operations. Information exchange mechanisms should be established between security domain to enable seamless information exchanges in accordance with operational requirements. Persistent mission domains can be established to ensure the required level of readiness. These domains are established for a specific mission in time and scope, and incorporate CIS provided by mission participants. Mission-specific security and releasability rules and implementation policies are established by the operational commanders and agreed to by all participants. A mission domain may be established independent of strict NATO policy and to enable all partners in an operation to operate as equal peers.

(3) **National domain.** This domain contains those CIS, that follow security rules and implementation policies established by a specific nation. They are subject to national technical and management policies.

(4) **Security domains.** Security domains compartmentalize CIS attending to the sensitivity of the information that the CIS domain processes, stores, and forwards. 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 authorized 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.

(5) **NATO Secret security domain specifics.** There are three methods by which NATO Secret (NS) information may be shared with users on a NATO mission domain which does not conform to NS domain standards.

(a) NS domain terminals may access the NS WAN through end-to-end encrypted tunnels across the mission domain, enabling authorized NS users to access NS information while remote from the NS WAN itself.

(b) Establish a NATO-owned contribution to a mission domain which can connect directly with partner CIS all at the same classification.

(c) The NS WAN and a mission network may be connected through a gateway with a boundary protection device sufficient to enable information exchange at the common security classification while protecting the NS WAN.[27]

f. **Mission networks.** 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. Mission environment accreditation follows the FMN Accreditation Strategy V1.0 (or successive revisions). 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 may also be used also as a technical term for the installation.

1.16 **Overall principles and responsibilities within CIS.** The following principles apply within the context of roles, responsibilities, and relationship decisions after consultation between the MPs. Specific guidance on command relationships, (i.e., supported/supporting and degrees of authority) can be found in AJP-1 Chapter 5.

a. Higher HQs provides the required connectivity to subordinate HQ. Taking these responsibilities into consideration, the installation, operation, and maintenance of CIS are governed by the following general principles:

[27] For additional information, refer to MC 0593/1, *Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations*, 12 July 2017.

(1) NATO enables the extension of unsecure and secure CIS connectivity to the highest level of national or multinational tactical command in a theatre of operations based on eligibility.[28]

(2) 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 eligible and available.

(3) Nations provide the infrastructure for their own national rear links; however, NATO facilities may be used, if eligible and available.

b. NS is the preferred domain for C2 of NATO-led operations. When the use of NS is not operationally feasible participants must operate on a separate mission domain. This domain is established to include all coalition partners at an appropriate classification.

c. In order to enhance unity of effort all coalition members must agree to share information on the mission domain at the same classification and releasability level without impediment to distribution or access. Mission domains need not necessarily be at the secret level).

Reacher Large X-band satellite ground terminal providing communication and information systems connectivity on Exercise Flying Javelin

[28] For additional information refer to ACO Directive 080-095, *Communication and Information Systems (CIS) Planning Directive*, 2 July 2014. Additionally refer to MC 0195, MC 0593, and MC 0640.

Section 5 – Interoperability aspect of communication and information systems

1.17 **Interoperability.** Interoperability is required to enable the passage of information between different elements of a deployed joint force or, in multinational operations, with mission participants. FMN is the main NATO Interoperability Programme for establishing mission networks, however, the Multilateral Interoperability Programme still 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. CIS interoperability is the ability of different CIS to work together to improve the way the joint force commander 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. Interoperability is difficult to achieve and sustain because of design, security, or national restrictions.

Ad hoc coalitions for multinational groups

UK 1.7. Ad hoc coalitions are a feature of the modern operational landscape. They are invariably based on ad hoc command and control structures, and interoperability challenges may be exacerbated by the lack of protocols, information management or common operating procedures. A centralised coordination function is required in most ad hoc operations to enable the interconnection and interoperability of CIS.

1.18 **CIS interoperability.** Interoperable CIS enables the commander to exercise operational C2 of the whole joint force, have continuous situational awareness and permit all elements of the joint force to successfully coordinate their activities in an efficient manner to achieve the mission. Further notable aspects of interoperability are:

a. **Interoperability versus security.** The competing needs of interoperability and security must be actively managed, in compliance with respective NATO directives, particularly on multinational operations. Technical and procedural solutions based on a comprehensive risk assessment is required. Risk assessments should be detailed, prioritized, and focused on risk mitigation. These activities should focus on avoidance or mitigation of identified risks, as compromise of information will lead to breaches in operational security and damage NATO's military effectiveness and freedom of action.[29] Balance between interoperability and security can be reduced, and synergy increased, by employing mission participants materiel and non-materiel capabilities within the same classification and releasability level operating environment established for the specific mission or exercise.

b. **Joint and multinational.** The requirement for CIS to be interoperable within, and between, joint force components and supporting forces is established. However, operational trends within NATO-led coalitions, for instance 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. The technical limitations of local authorities and non-governmental organizations must be considered when information must be shared as these organizations frequently work entirely at an unclassified level on the internet.

c. **Interagency.** 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. Establishment of common standards for data exchange and security to which coalition members could choose to train and equip would set in place potential increases in CIS technical interoperability and compatibility. Implementation of CIS within a mission network environment would be further informed and shaped by guidance and direction by commanders and mutual agreements during mission planning processes.

d. **Languages.** NATO communication doctrine is based on the use of English and French as the common working language. During multinational or coalition operations, translators may be required to overcome language challenges.

[29] For additional information on risk assessment, refer to Allied Joint Doctrine; AJP-3 Allied Joint Doctrine for the Conduct of Operations; and *NATO Standardization Agreement 5524, NATO Interoperability Standards and Profiles* (NISP).

e. **Doctrine, tactics, and procedures.** Agreements and doctrine, such as NATO standardization agreements (STANAGs), memoranda of understanding, AJPs, Allied communications publications as adopted from the Combined Communications Electronics Board serves as a foundation for interoperability. These agreements and doctrine should cover principles, procedures (e.g., standard message formats), and spectrum management. These should be validated by the CIS and operational communities as an explicit aim of joint, coalition, and combined exercises.

f. **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 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, such as those found in MC 0195, MC 0593, and MC 0640 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. In some cases, established commercial off-the-shelf software also may be used to maximize interoperability.

1.19 **Interoperability requirements.** The driving factor behind the development of NATO interoperability is the need for joint force headquarters to direct its lower echelons. NATO services are those services employed in the context of NATO C2 systems and, in particular, those provided mainly by NATO-owned CIS. Interoperability requirements between NATO, allies and partners should be informed by outcomes from relevant initiatives such as FMN. Those services are provided through DCIS. The echelons and units to which the DCIS services are established by the Military Committee (MC) in the minimum military requirements. In addition to the minimum military requirements, if NATO services must be extended to other echelons or units, nations providing these forces must provide the CIS for these services to be offered. National CIS must comply with NATO standards and undergo a certification process before they can connect to NATO core services, regardless of security domain.

1.20 **Systems interoperability.** There are three aspects of interoperability:

a. **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.

b. **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.

c. **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.[30]

1.21 **Levels of interoperability.** Levels of interoperability are increased through standardization, education, training, exercises and evaluation, lessons learned, cooperative programmes, trials, and tests. Additionally, a manual gateway (e.g., diskette, memory stick, tape, and hard copy exchange) has been installed between established levels. NATO interoperability policy defines the levels of interoperability in terms of information systems as follows.[31]

a. **Level 3** – Integrated. Forces operate together effectively without technical, procedural or human barriers; it is characterized by common networks, capabilities, procedures and language.

b. **Level 2** – Compatible. Forces operate together without prohibitive technical, procedural or human barriers; it is characterized by similar or complementary processes and procedures.

[30] For additional information, refer to AAP-31, *NATO Glossary of Communication and Information Systems Terms and Definitions*.

[31] For additional information, refer to AJP-01, *Allied Joint Doctrine.*

c. **Level 1** – Deconflicted. Forces operate in the same operational area in pursuit of a common goal but with limited interaction due to prohibitive technical, procedural and human barriers.

d. Level 0 – Not interoperable. Forces have no demonstrated interoperability and must operate independently from each other.

1.22 **Achieving interoperability.** Interoperability depends on the commitment to implement and adhere to agreed upon standards. 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.**[32] 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 to make it exchangeable between different CIS or equipment.

(2) **Information Exchange Gateways.** These serve to connect different security domains to check and filter the information that can be exchanged between them.

1.23 **Interoperability.** 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

[32] For additional information on gateways, refer to MC 0593/1, *Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations*, 12 July 2017.

level 3. Finally, whenever interoperability requires manual manipulation of the information between systems (e.g., when implementing the "swivel chair" solution of MC 0640, interoperability may stay at level 0).

a. Technical interoperability to match a commander's needs requires significant time and effort. To be effective, this activity should be conducted well in advance of deployment. When such activity has not taken place, the operational commander may be faced with a combination of CIS that 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.

b. Allied joint operation interoperability, 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. These shortfalls are most frequently identified through the execution of a risk reduction event to reduce technical issues. 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. Initial phases of allied joint operations are likely to rely more heavily on human interoperability at level 0 for force elements who have no established joining, membership, and exit instructions (JMEI)s. As the operation passes through future phases the level of interoperability and the different systems involved will increase through more technical levels to allow richer more automated information exchange, as time allows testing and resolution of interoperability shortfalls. Regardless of the level or seniority of the staff, all staff elements provide operational IERs to IM staff planners. IM in conjunction with J6 planners must then specify those applications and communication services required and needed for deployment. Definition and Identification of IERs are as follows:

(1) The different C2 functions performed during an operation will define the range of information types to be exchanged between different systems. 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) Interoperability requirements express the translation of the operational information requirements as technical requirements to be fulfilled through information exchange between CIS. In this translation process, it is necessary to consider that C2 services are grouped in layers that form a structured hierarchy.

(3) A final step for defining CIS interoperability requirements is to identify the technical standards required for each service.

(4) To enable the implementation of the resulting IERs, CIS solutions and services should conform to the identified technical standards.

c. The interoperability solution must be validated by system testing. The full interoperability interface must be described in JMEIs for future reference and fault-finding. Testing and evaluation of potential solutions should be conducted as soon as feasibly possible. Waiting for testing and evaluation until deployment does not allow sufficient time for modification or correction.

1.24 **Interoperability in multi-domain communication and information systems.** CIS Interoperability is required in multi-domain operations. Joint and multinational forces will act across all domains: maritime, land, air, cyberspace and space, and CIS interoperability across all of them is essential to orchestrate operational effects. The goal of interoperability is to efficiently share tactical, operational, and selected administrative knowledge for planning and executing operations. 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.

1.25 **Interoperability in land communication and information systems.** Interoperability in the land environment is often achieved procedurally. These procedures are based on the rules stated in overall principles and responsibilities within NATO CIS.

a. 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.

b. MC 0640 NATO standardization agreement, *The Minimum Scale of Connectivity for Communication 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 that cover the technical characteristics and required interfaces for tactical area communications systems and combat net radio systems.[33]

1.26 **Interoperability of maritime communication and information systems.** The 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.

a. Naval and maritime air communications are governed by the concepts established in publications ACP-176 and ACP-176 NS 1. The main circumstance that governs naval communications is the difficulty of accessing the wide data transportation rate/capacity provided by satellite communications and the threat of these being jammed, or that the naval forces are operating under a denied, disrupted, intermittent, and limited (bandwidth) environment. Therefore, the C2 of naval forces can be exercised using the formal messaging format established in ACP-127 and STANAG 4406 Annex E which is able to effectively work with reduced bit rate. Its procedures can be automatic or manual according to the instructions established in the ACP-121, but in any case, a distributed management of normal messaging systems that allow survival in the most demanding environments is necessary.

b. 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.

[33] For additional information, refer to MC 0593/1, *Minimum Level of Command and Control (C2 Service Capabilities in Support of Combined Joint NATO Led Operations*, 12 July 2017.

c. Interoperability of maritime CIS are addressed in MC 0195 NATO Minimum Interoperability Fitting Standards for Communication and Information Systems Capabilities Onboard Maritime Platforms (or successive revisions).[34]

1.27 **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(B), *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 and special operations 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.

Royal Air Force Typhoons working with French Rafale and United States F-35 jets as part of Exercise Atlantic Trident 2023

[34] For additional guidance refer to AC/322-N(2015)0123-AS1, Request for Endorsement of *ACP 200V1 (D), Mobile Tactical Wide Area Networking (MTWAN) in the Maritime Environment- Operating Guidance, 31 August 2015*; and AC/322(CP/1)D(2015)0009, Request for Review of ACP 200 V2 (D), *Maritime and Mobile Tactical Wide Area Networking (MTWAN) Technical Guidance*, 15 July 2015.

1.28 **Interoperability of cyberspace communication and information systems.** The cyberspace component of a joint and NATO-led coalition force utilizes a standards-based cyberspace C2 system reference architecture. Interoperability of cyberspace C2 planning and execution, supporting information exchange systems, and operational processes and data is discussed in AJP-3.20, *Allied Joint Doctrine for Cyberspace Operations*, and other cyberspace C2 COI documents that frame integrated C2 processes and employment of cyberspace C2 systems.[35]

a. Cyberspace is not limited to, but at its core consists of, a computerised environment, artificially constructed and constantly under development.

b. Cyberspace infrastructure is largely globally interconnected; however, geographic boundaries do apply in the context of jurisdiction, with national responsibilities. This is why the assignment of classical operational boundaries in cyberspace is particularly difficult. Cyberspace is not only in constant flux, but even more importantly, it may be used by anyone for almost any purpose.

c. Cyberspace is also distinct in that its underlying physical elements are entirely artificial, which is different from land, air and space, and sea. Risks emerging in cyberspace may be managed through manipulation of elements in cyberspace.

[35] Additional information can be found in AJP-3.20, *Doctrine for Cyberspace Operations*.

Key points

- CIS comprises data transmission systems and associated infrastructure and includes information storage and processing functions. A CIS network may consist of multiple aggregated systems that have different technical, procedural and security characteristics but conform to agreed standards and protocols to ensure seamless and reliable operation.

- CIS may be either static or deployable. The characteristics of a CIS network include sufficient capability for the task, interoperability, agility, scalability, service orientated and resilience.

- Central to CIS planning, design and functionality is the information exchange requirements demanded of it. This gives rise to the associated information management plan.

- CIS networks may have individual characteristics but must achieve compatibility. Where several different networks are employed to meet an operational requirement, a federated approach should be adopted. A federated mission network is NATO's preferred way to achieve interoperability.

- The security and assurance of data, transmission reliability and the resilience of CIS are vital considerations.

- CIS has a strong element of mutual dependence with cyberspace and the electromagnetic spectrum.

UK Annex 1A

Information governance

UK 1A.1. This annex describes the constituent elements of information governance, particularly those within the scope of information assurance and how they relate to equipment and services so that appropriate measures may be taken before, during and after an operation. Information assurance is a contributor to operations security (OPSEC) and hence to the overall provision of security to the force.

Security considerations

UK 1A.2. **Security.** Information services are of little use to a commander if they are compromised or delayed. The threat to information services, articulated in a commander joint force CIS (JFCIS) CIS Directive, defines the appropriate security requirements.

UK 1A.3. **Aggregation of information.** Throughout an operation, there is a risk of an opponent intercepting seemingly unimportant pieces of information which, when aggregated, lead to the deduction of important intelligence about friendly operations. It is important to understand the risks of aggregation, in accordance with JSP 440, *The Defence Manual of Security*, Leaflet 4D – Information Aggregation.

UK 1A.4. **Protection.** Information services should be protected to survive physical and electromagnetic attack or system failure according to the value of the information held and its importance to users. If protection is breached, recovery measures should be available to restore capacity. Diversity and redundancy are both used to enhance network protection.

UK 1A.5. **Risk management.** The joint task force commander (JTFC), advised by commander JFCIS, balances the implications of reduced information assurance against the required operational tempo. The establishment of an information assurance officer enables commander JFCIS to provide appropriate risk management advice. Effective security risk management ensures that risk owners are aware of the level of risk they are holding and the impact should an incident occur. Development of a primary, alternate, contingency and emergency (PACE) plan will provide a commander with knowledge of reversionary CIS should primary services be unavailable.

UK 1A.6. **Vulnerability analysis.** Specialist units, with engineering, information services security and intelligence communications professionals, undertake an information security (INFOSEC) vulnerability analysis for the commander. This includes:

- defensive monitoring, which may be used to monitor unencrypted forms of communication (unencrypted radio (voice), static telephone, service mobile telephone, facsimile transmissions and email) at fixed and deployed sites;
- TEMPEST[2] inspections and assessments to help minimise compromising emanations from computer and communications systems;
- Technical security countermeasures assessment (TSCMA) to identify the presence of clandestine eavesdropping devices;
- computer security (COMPUSEC), monitoring and audit tasks to identify the vulnerabilities of networked and distributed CIS, and to recommend remedial measures; and
- social media monitoring, which will aid awareness of information flows and assist in identifying possible information security breaches.

Consideration must also be given to the physical security requirements of infrastructure housing CIS.

UK 1A.7. **Allied and coalition communications.** When UK and Allied forces operate together, secure communications are usually provided in accordance with Allied communications publications (ACPs).[3] For coalition operations, the lead nation will usually determine appropriate INFOSEC and network security joining rules. National CIS remains subject to national CIS security policy.

UK 1A.8. **Application of security policy.** Information services security policy applies to all military and civil information services used in the joint operations area. To avoid confusion with single-Service procedures, information services security policy is detailed in the CIS Directive.

[2] TEMPEST is the investigation and study of compromising emissions (AP 600).

[3] ACP-122, *Information Assurance for Allied Communications and Information Systems* outlines the NATO accreditation requirements based on national policy.

UK 1A.9. **Operations security.** OPSEC[4] is an activity that is led by the J3 staff function. By its nature, however, it has very close ties to J6.

a. **Planning.** During planning for an operation there is an increase in communications traffic between headquarters and nominated force elements. CIS used during the planning process requires appropriate protection. Subsequent force element preparation requires practise in OPSEC techniques, usually through exercises or mission rehearsals. Consideration should be given to disguising these events by deception techniques where practicable. INFOSEC is used to prevent any indication that force elements preparation is tied to a particular operation plan or geographical area.

b. **Force assembly.** Irrespective of whether the operation is mounted from the UK, or from a forward mounting base, force assembly generates significant traffic over strategic information services links. Increased communications traffic to, or from, an assembly area may focus an adversary's interest, and result in an increased hostile intercept effort. Political events may indicate UK interest, but only the interception of communications may provide information about the timing, location and scope of any future operation. Transmission security in modern systems significantly improves protection against an adversary intercepting and analysing friendly communications. INFOSEC during this phase is enhanced by using only approved information services.

c. **Deployment.** Communication increases markedly during the deployment phase, particularly on information services supporting maritime and air assets. OPSEC is critical during this period, and the imposition of radio and electronic silence should be considered to deny information to the adversary. It is vital that OPSEC is maintained during deployment and under no circumstances should insecure means be used to pass sensitive deployment information.

d. **Force entry.** Radio silence is often appropriate during force entry and compliance with the emission control (EMCON) plan is essential.

[4] Further details on OPSEC principles and measures are found in AJP-3.10.2, *Allied Joint Doctrine for Operations Security and Deception*.

Information governance

UK 1A.10. **Information security.** Within the framework of information governance and information assurance, INFOSEC describes the security measures taken to safeguard information in any form. It provides an important connection between traditional security staffs embedded within the J2/3 community and those directly charged with protecting information services and its products. The information services community has a particular INFOSEC responsibility, given its ownership of providing and maintaining CIS equipment, to ensure that the risks to information are identified and appropriately managed. The INFOSEC measures required are determined by risk analysis and implemented with the appropriate criticality level of the CIS and/or protective marking of the information being handled, stored, processed or transmitted. This process ensures that confidentiality, integrity, availability and accountability concerns are addressed.

UK 1A.11. **Computer security.** COMPUSEC covers all facets of computer security to ensure the confidentiality, integrity and availability of information technology systems, and is applied to both hardware and software. Deployed information services staffs should be aware of the significant risks that exist through a poor focus on security in some legacy, stand-alone equipment and small devices where the secure by design approach[5] has not been adopted from the outset. A first line assurance assessment review, which for legacy systems may include accreditation details, should be taken prior to deployment or after any subsequent significant system changes, including all proposed changes to connectivity. Compliance with system security policies and any additional local policies (particularly in a multinational environment) is a vital element of COMPUSEC.

UK 1A.12. **Communications security.** Communications security (COMSEC) measures are specialised protective security measures taken to ensure the confidentiality, authentication, non-repudiation and integrity of information in communications channels. On operations, COMSEC procedures are designed and issued as joint task force (JTF)-level instructions, particularly if they differ from standard operating procedures. Most COMSEC procedures are detailed in the CIS Directive, but it may be appropriate to produce a specific instruction on COMSEC depending on the scale and classification of the operation. Such an instruction covers the duties and responsibilities for COMSEC, but emphasises:

[5] See JSP 440, *The Defence Manual of Security*, Leaflet 5C – Building Cyber Secure by Design Capabilities.

- arrangements for the distribution of cryptographic material;
- transportation of cryptographic material;
- handling and storage of classified material; and
- transmission of plain language communications.

UK 1A.13. **Detection of information leakage.** Measures that indicate the levels of information leakage and that help deny an opponent the opportunity to electronically eavesdrop include the following.

a. **Defensive monitoring.** Defensive monitoring is essential to reinforce OPSEC training and to act as a deterrent against poor COMSEC, including EMCON. Defensive monitoring equipment is used to monitor all unencrypted forms of communication.

b. **Technical security countermeasures assessment.** Eavesdropping uses clandestine listening devices to overhear and transmit or record conversations. An electronically safe working area is critical in deployed environments where information is processed in unfamiliar locations. This is particularly important early in an operation or during a reconnaissance phase where untrusted facilities may have to be used. The provision of an electronically safe working area requires an inspection comprising both a physical check and a TSCMA. Specialist units and staff within deployed headquarters hold deployable TSCMA equipment.

UK 1A.14. **Communications security.** COMSEC procedures also provide protection against electromagnetic attack, including any defensive measures against search, interception and direction finding, jamming and deception. These procedures are produced as a JTF-level instruction – *Protection against Electromagnetic Attack*.

UK 1A.15. **Cryptographic security.** Specially devised methods or processes, usually called cryptosystems, are used to protect information in communications channels. Cryptosystems are used to conceal the content of communications and their effectiveness depends on the strength of the cryptologist used, the overall protection given to the cryptosystem and the correct use of operating procedures. Specific guidance on cryptographic security is published in JSP 490, *Defence Cryptosecurity Operating Instructions* and JSP 604, *Defence Manual for ICT*. UK national instructions are compatible with the corresponding NATO cryptographic security

Instructions published in Military Committee Communication and Information Systems Security and Evaluation Agency (SECAN) Doctrine and Information Publication-293/1 *Instructions for the Control and Safeguarding of NATO Cryptomaterial* and Allied instructions contained in ACP-122, *Information Assurance for Allied Communications and Information Systems*.

UK 1A.16. **Cryptographic security.** Most modern UK and NATO cryptosystems are highly resistant to cryptoanalysis, but a determined and capable adversary could obtain details of the cryptology either by theft or by suborning a UK/NATO national. Cryptographic material is safeguarded by enforcing a comprehensive security policy, articulating physical, personnel and COMSEC (including radiation security (RADSEC) and TEMPEST). Commander JFCIS directs which protective measures are applied to information exchanges and information storage, including online and offline cryptographic systems, secure speech equipment and authentication and code systems.

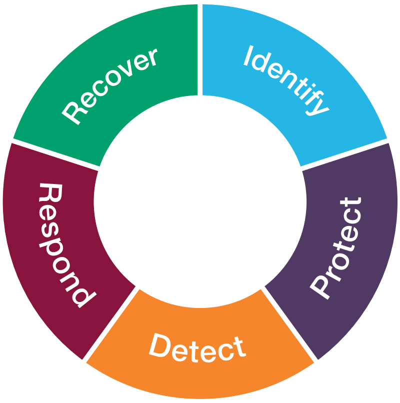
UK 1A.17. **Radiation security.** RADSEC manages the risk associated with radio signals, both intentional and unintentional. Compromising emanations, when intercepted and analysed, may disclose protectively marked information. An essential element of RADSEC is TEMPEST, the investigation and study of unintentional emanations. In addition, it is important to conceal the radio frequencies to be used by UK forces, normally conducted in conjunction with the battlespace spectrum management plan.

UK 1A.18. **Defensive cyber operations.** A defensive cyber operation is defined as: active and passive measures taken to prevent, nullify or reduce the effectiveness of adversary actions to preserve our freedom of action in or through cyberspace.[6] They may be discrete, episodic or enduring but are focused activity that is designed to secure our access to, and freedom of action in, cyberspace. They may be undertaken against a specific threat or bounded in scope, for example, when in support of a named military operation or as part of a mission assurance approach.

UK 1A.19. **The National Institute of Standards and Technology Cybersecurity Framework.** The National Institute of Standards and Technology (NIST) is a United States government organisation that has contributed significantly to international thinking on cybersecurity. Specifically, it produced an updated Framework in 2018 to aid organisations conduct cyber defence, which has been widely adopted and is colloquially known as the NIST Cybersecurity Framework. The Framework comprises five core functions

[6] JDP 0-01.1, *UK Terminology Supplement to NATOTerm*.

and is shown in UK Figure 1A.1. The Framework and the sound principles it espouses underpin much of the work of the Cyber Security Operating Capability and the NCSC, although terminology may differ.



UK Figure 1A.1 – The NIST Cybersecurity Framework

a. **Identify.** The identify function assists in developing an organisational understanding of managing cybersecurity risk to systems, people, assets, data and capabilities.

b. **Protect.** The protect function supports the ability to limit or contain the impact of potential cybersecurity events and outlines safeguards for delivery of critical services. It aims to protect an organisation's critical assets from threats by implementing security controls to protect critical services and prevent unauthorised access to sensitive information.

c. **Detect.** The detect function defines the appropriate activities to detect cybersecurity incidents as they occur. This includes implementing monitoring and detection systems that can alert the organisation to potential threats and allow a quick response.

d. **Respond.** The respond function includes appropriate activities to respond to cybersecurity incidents when they occur. This includes having a well-defined incident response and escalation plan to ensure organisations respond to and recover from an incident quickly and effectively.

e. **Recover.** The recover function identifies appropriate activities to maintain plans for resilience and to restore services impaired during cybersecurity incidents. This includes implementing measures to restore normal operations and mitigate the impact of a cybersecurity incident.

Protection against electromagnetic attack

UK 1A.20. All electromagnetic emissions are vulnerable to exploitation by an adversary conducting electromagnetic warfare. With the appropriate equipment, signals can be detected, intercepted, sourced, analysed and disrupted. The ideal result of effective electromagnetic protection is preventing an opponent from detecting friendly electromagnetic radiation. Full prevention may be unachievable, so the principal objectives of electromagnetic protection are to:

- minimise emissions and thereby reduce an opponent's intelligence collection; and

- minimise all other types of electromagnetic transmissions, such as radar and infrared lasers, which may compromise friendly operations.

UK 1.21. Effective electromagnetic protection is achieved in two ways. These are described below.

a. **Active electromagnetic protection.** This consists of detectable measures to ensure effective use of the EMS, such as changing frequencies and changing modes of operation.

b. **Passive electromagnetic protection.** This consists of undetectable measures, such as operating procedures and technical features of the equipment, to ensure the unhindered use of the EMS as well as counter electromagnetic surveillance and counter electromagnetic attack measures. While EMCON is viable, it is also complex due to the plethora of CIS involved and associated operational dependencies. The benefits of radio silence are balanced against the need for effective command and control.

Notes

QUEEN ELIZABETH
ROYAL NA
BURTON

Chapter 2

Chapter 2 outlines the communication and information systems-related roles and responsibilities of NATO organisations, nations, host nations and commands.

2

> “Quality is everyone’s responsibility.”
>
> William Edwards Deming

Chapter 2

Roles and responsibilities

This chapter outlines the communication and information systems (CIS)-related roles and responsibilities of North Atlantic Treaty Organization (NATO) organizations, nations, host nations and commands.

Section 1 – Introduction

2.1 CIS related roles and responsibilities of NATO organizations, nations, host nations and commands are generally categorized by member nation, strategic, operational, and tactical.

Section 2 – Member nation responsibilities

2.2 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 chapter 1, section 5.

Section 3 – Strategic-level roles and responsibilities

2.3 **Strategic roles and responsibilities.** The NATO command structure is composed of permanently established headquarters and supporting organizational elements at the strategic, operational and tactical levels. At the strategic level, Supreme Allied Commander Europe (SACEUR), as the commander of the Allied Command Operations (ACO), assumes the overall command of operations and is responsible for planning, preparing, conducting, executing and sustaining all NATO operations. SACEUR determines the command and control (C2) arrangements and designates those who will exercise operational and tactical authority. These arrangements are endorsed by the Military Committee (MC) and approved by the North Atlantic Council (NAC).[36]

a. **North Atlantic Council.** The NAC is the principal decision-making body within NATO and provides direction for planning and execution to ACO. It brings together high-level representatives of each NATO nation to discuss policy or operational questions requiring collective decisions.

b. **Office of the Chief Information Officer.** Mandated by the NAC. Facilitates the integration, alignment and cohesion of information and communications technology (ICT) systems across the NATO Enterprise and its civilian and military users. Additionally, this office oversees the development and operation of ICT capabilities.

c. **Consultation, command and control board.** As a subset of the MC Senior Policy Committee, the Consultation, Command, and Control (C3) Board (C3B) supports NATO C3 by providing guidance and direction, in order to enable information sharing and achieve interoperability.

d. **Allied Command Operations.** The ACO plans, prepares for, and conducts military operations to achieve Alliance political objectives. 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 headquarters (HQ). The SHAPE DCOS Cyberspace directs, monitors, and coordinates all ACO CIS and cyber defence functional area activities and staff functions. Additionally, the SHAPE DCOS Cyberspace serves as the Commander, NATO Communication and Information Systems 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 and information assurance capabilities throughout their life cycle. This

[36] For additional information review AJP-01, *Allied Joint Doctrine*, December 2022.

enables Defensive Cyberspace Operations capabilities to prevent, detect, and response to cyber incidents. Working under the direction of the SHAPE DCOS Cyberspace, the J6 planners and provides oversight of all CIS provisioning to enable C2, while the cyberspace theatre component provides cyberspace defence functional area activities on services delivered by the NATO Communications and Information Agency (NCIA) across ACO, at all levels of command, and for all ongoing operations and exercises.

e. **Allied Command Transformation.** The Allied Command Transformation (ACT) is NATO's warfare development command leading agent for change, driving, facilitating, and advocating continuous improvement of Alliance capabilities to maintain and enhance the military. ACT's strategic objectives include providing appropriate support to NATO missions and operations; leading NATO military transformation; and improving relationships, interaction, and practical cooperation with partners, nations, and international organizations. ACT is organised around four principal functions: strategic thinking; development of capabilities; education, training, and exercises; and co-operation and engagement.

f. **CIS services within multinational headquarters.** Joint force commands (JFCs) are warfighting and deterrence headquarters that plan, prepare, and conduct joint activities, missions, and operations across all operational domains. Troop Contributing Nations assign force elements of various sizes to operate under JFCs within their Regional Plans. The order of battle, and the command relationships between national contributions, must be mutually agreed, and will normally nest smaller national contributions within larger assigned formations. Where nations assign formation headquarters, which may be standing commitments or developed ad hoc, they assume responsibilities for providing communications within the formation as outlined in the principles in Chapter 1. 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.

g. **Host nation communication and information systems integration.** Host nations (HN), 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 memorandum of understanding 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 communication links via the most appropriate means.

h. **NATO communications and information organization.** The NATO Communications and Information Organization is under the authority of the NAC. It was established to meet the collective requirements of NATO nations in the fields of capability delivery and service provision related to C2, communications, information, and cyber defense functions.[37] 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) **ASB.** The ASB is responsible for the organizational governance of the NCIA. Organizational 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 Organization. It provides strategic direction and guidance to the NCIA and oversees its activities and performance.

(2) **NATO communications and information agency.** 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:

[37] For addition information, refer to C-M(2012)0049-ADD1, *Addendum to the Charter of the NATO C&I Organisation for AIRC2 and BMD Programmes*, 8 June 2015.

(a) Deliver C2 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 C2/CIS) to NATO and NATO nations, as approved by the ASB.

(3) **Pre-deployment mission preparation.** With respect to CIS support to military operations, pre-deployment mission preparation, the respective responsibilities between NCIA and NCISG are described in the C2 arrangements between SACEUR and General Manager NCIA.[38] SACEUR is responsible to the MC for the overall direction and conduct of NATO military operations to include CIS operational planning and execution. 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).

The NATO Communications and Information Agency is responsible for testing and resolving potential interoperability issues with national CIS

[38] For addition information, refer to C-M(2012)0056-AS1, *Politico-Military Advice on Command and Control Arrangements between SACEUR and the General Manager of the NATO Communications and Information Agency*, 2 July 2012; and MCM-0065-2012, *Command and Control (C2) Arrangements between SACEUR and the General Manager (GM) of the NATO Communications and Information (C&I) Agency*, 19 June 2012.

Section 4 – Operational-level roles and responsibilities

Operational level

2.4 **Operational level commands.** Operational level commands are warfighting and deterrence headquarters that plan, prepare and conduct joint activities, missions and operations across all operational domains in their assigned area of responsibility within usual peacetime activities and current operations, through crisis and up to conflict. Roles and responsibilities of the operational level commands:

- Ensure 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.

- Develop CIS plans in accordance with guidance provided in chapter 3.3 of this document.

- Publish CIS plans, annexes, and operating instructions to support the assigned mission.

- Exercise overall management of all CIS supporting the joint force.

- Review and coordinate CIS plans prepared by subordinate commands.

- Ensure CIS interoperability is achieved within the joint force.

- Establish a battlespace spectrum management plan.

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

- Incorporate J2 assessments of likely adversary actions into an operational assessment of impacts supporting CIS operational requirement definition.

- Organize the C2 of CIS support.[39]

- Assign as early as possible the following roles that require delegated authority from the higher commander and mission participants:

    - Mission Network Service Management Authority – responsible for Mission Network architecture, Mission Network service strategy, and naming, numbering, and addressing for the Mission Network.

    - Mission Network Information Management Authority – including Information Management plan development and Mission Thread analysis.

    - The Mission Network Accreditation Board to execute the responsibilities of a CIS Security Management Authority such as providing Approval to Operate to Mission Participants.

2.5 **Mission network communication and information systems operations centre.** In joint operations, successful CIS integration requires that strict technical and management standards be imposed throughout the network. Integration is the final stage of connecting the elements of coalition member mission networks such that that can all exchange information without adversely affecting each other. The purpose of joint CIS management is to provide centralized control and decentralized execution of the utilization of CIS resources consistent with the operational command's requirements and changing priorities. CIS can provide support and technical solutions to implement information management (IM) in an organization. In a joint force HQ, the J6 planner is normally responsible for joint CIS services provision – supported by NCISG during planning and by a deployable communication and information systems (DCIS) Support Group when deployed.

2.6 **Federated CIS management.** 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. In NATO-led coalition operations, successful CIS integration requires that agreed technical, management, and policy standards be imposed throughout a federation of mission networks and CIS contributed by coalition members. Integration is the final stage of connecting the elements of coalition member mission networks such that can all exchange information without adversely affecting each other.

[39] In accordance with MC 0593/1, *Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations*, 12 July 2017.

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.

2.7 **Cryptography roles and responsibilities for NATO organizations and commands.** Interoperable cryptographic solutions are critical for NATO forces to communicate. Authority to distribute cryptographic material to non-NATO entities is held above the level of operational commander. Military committee holds the governance attributions for NATO cryptography.[40]

Section 5 – Tactical-level roles and responsibilities

Tactical level of component commands

2.8 The tactical level of the component commands includes any formation subordinate to the operational commander. At the tactical level, interoperability issues are frequently encountered, particularly where a formation is composed of multi-national elements. Regardless of composition, the direction provided holds:

a. The higher level of command is responsible for providing interoperability points to its subordinated levels of command.

b. The responsibility for implementation of the applicable interoperability point falls to both interconnected parties, whether in a superior or subordinated role.

2.9 Tactical commanders should note that interoperability is considered as three elements: technical, procedural, and human. Where a technical solution is not possible, the tactical commander must implement procedural and human solutions, suitable to the environment and available resources, to enable the interoperability of forces.

[40] MC 0074/4, *Military Committee Policy for Communications Security for NATO*, 22 May 2019.

2.10 Each component commander, in consultation with their higher operational commander:

a. Develop CIS plans, annexes, and operating instructions to support the assigned mission.

b. Review and coordinate CIS plans prepared by subordinate commands.

c. Exercise management of all CIS under command.

d. Maintain an awareness of, and protection against, threat vectors in the cyberspace.

Key points

- NATO has a hierarchical command structure that supports multinational operations, and the challenges of achieving CIS interoperability amongst members at the strategic, operational and tactical levels.
- The North Atlantic Council is the principal decision-making body within NATO and provides direction for planning and execution to ACO.
- NATO Communications and Information Organization meets the collective requirements of NATO nations in the fields of capability delivery and service provision relating to command and control, communications, information and cyber defence.
- Operational level commands play a key role in CIS planning, support and management.
- Coalition operations require successful CIS integration, including agreed technical, management and policy standards imposed throughout a federation of mission networks and CIS contributed by coalition members.
- Interoperable cryptographic solutions are a critical element of CIS operations. The Military Committee holds the governance attributions for NATO cryptography.
- Interoperability can be challenging at the tactical level. The higher-level command is responsible for providing interoperability points to subordinate levels however, implementation is the responsibility of the interconnected parties themselves

Notes

EMERGENCY ESCAPE ROPE
BOSE
TIAR Portugal · NATO AWACS · Geilenkirchen

Chapter 3

Chapter 3 explores and emphasises the importance of communication and information systems planning. It is a component of the NATO planning process, at all three levels: strategic, operational and tactical.

> "In preparing for battle I have always found that plans are useless, but planning is indispensable."
>
> Dwight D. Eisenhower

Chapter 3

Communication and information systems support planning

Communication and information systems (CIS) planning is a component of the North Atlantic Treaty Organization (NATO) planning process, in all three levels; strategic, operational, and tactical.

Section 1 – Introduction

3.1 It is essential for operational commanders to focus on strategic and operational level planning as well as the nature of CIS planning and support requirements. At both levels of CIS planning, participation of committed mission participants must be considered. Annex A of this document outlines the planning and execution association between allied joint publication (AJP)-3, AJP-5, and AJP-6.

Section 2 – Strategic-level planning

3.2 At the strategic level, planning is conducted in accordance with the comprehensive crisis and operations management process, as detailed in AJP-5. Detailed descriptions for planning below the strategic level can be found in the Allied Command Operations (ACO) comprehensive operations planning directive.[41]

[41] For additional information, refer to the *Allied Command Operations Comprehensive Operations Planning Directive*, version 3.0, 15 January 2021.

a. **Strategic planning products.** Planning products at the strategic level include Supreme Allied Commander Europe's (SACEUR) Strategic Assessment, military response options, strategic operation plan (OPLAN), and strategic planning directives (which includes strategic CIS planning guidance).

b. **Strategic CIS planning products.** CIS contribute with the following supporting elements to the strategic-level plan OPLAN: strategic CIS assessment, strategic CIS estimate, strategic concept of operations (CONOPS) CIS guidance, and CIS support plan (SUPPLAN).

Section 3 – Operational-level planning

3.3 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 the Planning of Operations*. AJP-5, in turn, informs and guides the development of planning instruments, including the ACO comprehensive operations planning directive, and the underlying functional planning guides [e.g., ACO Directive 080-095, CIS Planning Directive, 2 July 2014]. As a prerequisite for operational level planning process, consideration must be given to NATO Revised High Level C3 Taxonomy of cyberspace operations where the dependencies between CIS infrastructure operations, defensive cyberspace operations, offensive cyberspace operations, and intelligence exist.

a. **Operational-level planning process steps.** The operational level planning process consists of the necessary steps to support an operational commander and staff in order to develop the operational-level OPLAN - including the conduct of the operational estimate process. J6 planners shall reference the sequence of planning activities found in AJP-5 Chapter 4. The steps outlined in this chapter serve as a guide which through experience and technical expertise the J6 planning team can leverage for CIS planning.

b. **Operational planning products.** AJP-5 describes operational planning products in generic form while the ACO comprehensive operations planning directive provides greater detail tailored to Supreme Headquarters Allied Powers Europe (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 communication and information systems planning products.** CIS focuses on the operational commander's information requirements. While the generation of information exchange requirements (IERs) is owned and driven by the operational community, the 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).

Section 4 – Nature of communication and information systems planning

3.4 CIS planning is cyclical and iterative in nature. It is conducted continually, in close synchronization with the J2 (Intelligence), J3 (Operations), and J5 (Plans), to ensure CIS plans are consistent with the overall planning effort.

3.5 **CIS planning doctrinal principles.** CIS planning should be woven into each step of the operational-level planning process, to ensure that the information needs of the operational commander are met at every stage of the operation as well as most[42] of the doctrinal principles laid-out in AJP-5.

3.6 **CIS planning factors.** The applicable list of planning factors is contingent on the nature of the operational mission and therefore there is no all-encompassing list of factors. However, when CIS planning is conducted the following common factors should be considered:[43]

a. Scale and type of operation.

b. Availability of resources.

c. CIS security.

[42] 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.

[43] For additional information, refer to ACO Directive 080-095, *Communication and Information Systems (CIS) Planning Directive*, 2 July 2014 and Annex A of this document.

d. Capability limitations.

e. Interoperability.

f. Time.

g. Budget.

h. Deployable communication and information systems (DCIS) impact on on-going missions and tasks.

i. DCIS real-life support and force protection.

j. Threat capabilities in cyberspace and the electromagnetic.

k. environment.

3.7 **Additional planning factors.** CIS planning also considers the following additional planning factors that are used to guide the estimates for CIS:

a. The time available for planning, pre-deployment, deployment, redeployment, and reaction to contingency plans.

b. Established service and information sharing and security agreements among assigned mission participants.

c. An understanding of the IERs and information systems and facilities.

d. External / commercial service provided solutions may be available for employment at the discretion of the operational commander. Special consideration must be given when implementing these solutions dependent on the phase of the operation. A commander must consider the availability of non-commercial CIS especially during the deployment and drawdown phases.

e. The availability of in-service CIS or, if required, commercial CIS, and the ability to respond to urgent operational requirements.

f. Data transportation rate/capacity and channel availability, particularly on strategic satellite communications bearers and within national communications networks.

g. Data storage according to the provided services.

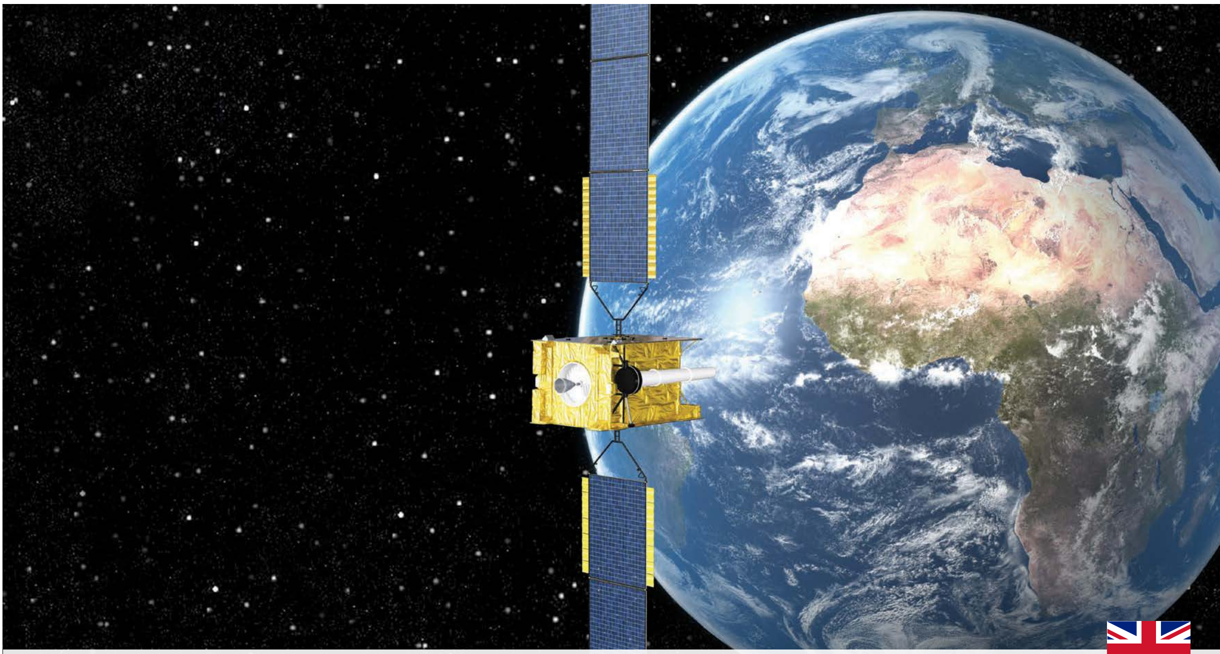
h. The availability of, and ability to control and manage, the radio frequency electromagnetic spectrum (EMS).

i. The readiness and availability of those required to deploy, operate, and maintain CIS, particularly that which is newly procured.

j. The availability of, and adherence to, international standardization of technical protocols.

k. Architecture of systems to be used (e.g., centralized vs. distributed; local vs. remote; and static vs. mobile).

3.8 **Outcome of CIS planning process.** 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.



The Skynet 5b communications satellite will provide a significant boost to operational capability for our forces, both on land and sea

Spectrum management

UK 3.1. Reliance on access to the EMS leads to resource contention across the EMS frequency bands. EMS management is a function that understands, plans, coordinates and deconflicts spectrum allocation to enable Defence activities; it includes Defence spectrum management and battlespace spectrum management (BSM). Spectrum management and protection are underpinned by the Defence Electromagnetic Authority (DEMA). The DEMA enables the use of spectrum-dependent systems for Defence through: planning and assessment during the acquisition phase; issuing authority to radiate to Defence EMS users operating in the UK (including planned jamming activity); and securing assured access to EMS frequency bands overseas. Where necessary, the DEMA also conduct incident management and assures that electromagnetic capabilities are protected, secure and resilient to interference and attack by preventing mutual interference, overexposure to radiation and illegal eavesdropping. These functions allow the management and protection of spectrum-dependent systems delivered through the enable and inform roles.

a. **Defence spectrum management.** Defence spectrum management is concerned with spectrum policy, release and sharing activities, along with consideration of wider civil regulation. Its objective is to enable spectrum-dependent systems to perform their functions without causing or suffering unacceptable interference. Defence spectrum management involves gaining an understanding of electromagnetic operations to enable the planning, coordination and management of the EMS through operational, engineering and administrative procedures.

b. **Battlespace spectrum management.** BSM deconflicts frequency use in the electromagnetic environment, preventing friendly forces from jamming their own communications and defensive aids. The joint restricted frequency list is a time and geographically oriented listing that is used to minimise undesired effects of friendly force electromagnetic countermeasure activity.

Section 5 – Communication and information systems support planning activities

3.9 CIS planning supports and informs the overall planning process. The CIS planning process and the activities associated to each organizational function must be available in a strategic and operational CIS task matrix.[44] This matrix can be tailored by the commander to suit the needs and complexity of the mission. The subsections below outline products and activities associated with CIS planning, Annex A of this document aligns these activities to their respective phases when compared to AJP-3, AJP-5, and AJP-6.

Communication and information systems assessment

3.10 **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 joint operations area (JOA). The CIS estimate of capabilities is designed for strategic level planning; however, the principles can be applied at all levels of planning as required. 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, facilitation of IERs provided by the JFC J6, evaluation of factors, potential solutions, and selected service delivery solutions. The development of this assessment should consider scoping the demand signal to troop contributing nations, assigning force elements to JFCs, and planning distribution of formation. The CIS assessment is formulated, in close coordination with NATO Communication and Information Services Group (NCISG) and NATO Communications and Information Agency (NCIA), during drafting of the strategic CIS architecture.

3.11 **Information exchange requirements.** Information exchange requirements (IER) are pivotal inputs to the CIS planning process. They ensure that all relevant command and control (C2) services required in support of the mission are identified, and adequate planning and provision of C2 services can be achieved. IERs in the form of orders, reports etc. also reflect the exchange of information products in support of the chain of command. Sample IER development templates are outlined in MC 0195, MC 0593, and MC 0640. To ensure effective C2, a high degree of operational information

[44] For an example of a CIS task matrix, refer to ACO Directive 080-095, *Communication and Information Systems (CIS) Planning Directive*, 2 July 2014.

exchange is required both vertically and horizontally. 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 headquarters (HQ). Regardless of the level or seniority of the staff, all staff elements provide operational IERs to information knowledge manager staff planners to specify those applications and communication services required and needed for deployment. It is a responsibility of all staff elements, per the information management (IM) plan, to provide theirs specific IERs regarding data format, content, and context relating to the IER, 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 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 will then allow the CIS solution, incorporating services, systems and bearers, to be developed.

3.12 **Information providing systems and facilities.** The cyberspace theatre component staff analyses information-providing systems and facilities (e.g., sensors, command posts, and weapon systems) to define information that might be of interest to an operational commander within a community of interest (COI). The information provided by cyberspace theatre component demonstrates to an operational commander the resources available to them and allows the commander to tailor their CIS to accommodate their level of risk acceptance and mission requirements. This information is published and accessible for the relevant COIs.

3.13 **Evaluation of factors.** Subject to NATO provisioning rules, CIS resource status information is included in CIS operational staff work. The J6 staff should be informing the CIS assets required to enable the J5 plan. If NATO resources are not sufficient to fill J6 identified requirements the 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 internal service providers, 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 participants cannot meet CIS SOR capabilities, they should seek commercial options.

Strategic CIS architecture

3.14 The draft strategic CIS architecture is based upon the OPLAN which is supported by the CONOPS and JFC J6 staff input. To overcome strategic CIS architecture shortfalls, contracted, commercial CIS may provide an effective solution.

Mission analysis

3.15 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. The products provided from this analysis will be utilized to inform and guide the planning of subordinate J6 elements through a collaborative process. Since each participating nation brings 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, at a minimum:

- Situation overview and higher commander's intent.
- Review of limitations.
- Review of assumptions.
- Review of Mission Essential Functions and critical capabilities, identifying and capturing their dependencies to CIS.
- Recommend the commander's initial CIS priorities.
- Identify the main effort and desired end state among the SHAPE J6 planning staff and establish an agreed-upon solution for providing CIS.
- Establish all specified and implied priorities for providing CIS, as a result of the previous steps and current objectives.
- Conduct CIS risk assessment, to include a review of CIS vulnerabilities, identified threats and potential impact.

Orientation

3.16 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.

Commander's planning guidance and initial intent

3.17 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. J6 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:

- Identify the basic strategic, operational, and tactical facts.

- Establish the commander's CIS priorities based on an analysis of the CONOPS.

- Identify the main effort and end state.

- Establish agreed conclusions for providing CIS among the J6 planning staff.

- Establish the agreed CIS guidelines among the participating nations.

- Establish all specified and implied requirements for providing CIS.

- Establish the specified and implied time factors for providing CIS. This should include the timeliness of warning orders.

Concept development

3.18 Courses of Action (COA) and Selected COA.

a. COAs developed should adequately account for potential and likely adversary courses of action, including adversary activities in cyberspace which may affect the friendly COA or require additional CIS capabilities to counter. The J6 planner must work to incorporate J2 assessments of likely adversary action into COA development.

b. 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 several potential J6 planner's tasks. Prior to more detailed planning, it is advantageous to develop a broad CIS CONOPS for each potential COA.

c. 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. The CONOPS shall also capture critical CIS dependencies and enabling services for the given COA in order to enable cyberspace operations to defend identified key terrains. The CONOPS describes how the CIS picture is built and shared. For J6 planners, this includes how the capabilities of the available CIS resources are synchronized to meet the IERs of the chosen COA.

3.19 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 narrow and the level of detail at this stage becomes progressively more important.

3.20 In the event of a crisis activation NATO is likely to draw upon standing high readiness response forces provided by nations, which will have organic CIS. For a deliberate activation strategic J6 planners will develop a SOR for submission to the mission participants 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. It should be emphasized that the CIS focus may change throughout the phases of an operation. While the CIS assessment may also differ between the strategic and the operational or tactical level, much of the information required may also be the same or similar.

Review of limitations

3.21 Constraints and restraints on providing CIS may be at the strategic, operational, or tactical level. They may be affected by legal, or military effects. Analysis of the constraints and restraints expressed in operational staff work should be an essential early consideration in J6 staff planning.

3.22 CIS resource status information should be reflected in CIS operational staff work. This may be expressed in the form of a task organization. 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 mission participants should be considered.

(3) International CIS contributions from non-governmental organizations 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 may be sought through the emergency procurement 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 and in accordance with the logistics procurement procedures outlined in AJP-5 to ensure support is adequately covered and procurement lead times are considered.

c. Personnel:

(1) J6 planners should determine the availability of workforce required to deploy, install, maintain, and operate CIS equipment. They should also ensure that the J6 planners are correctly staffed since the deployment of civilians to a JOA may be constrained. Any identified workforce deficiencies should be referred to J1 (Personnel and Administration) staffs.

(2) Operational requirements might dictate personnel level changes to ease transitioning to the operating environment, or for parallel operations.

Plan development

3.23 During plan development, the OPLAN is developed. It is normally the final outcome of planning and is produced in sufficient detail for mission execution. Missions and tasks are assigned to subordinate HQs and forces within the plan, which will enable them to initiate their own estimate activities. Other operational-level plans are approved by the author's next higher superior authority.

3.24 The OPLAN is comprised of a main body and supporting annexes. J6 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. This applies to both inter- and intra-theatre communications. OPLAN inputs from the J6 could consists of the following:

- Communications architecture (Level 0-3)
- Maritime communications
- Land communications
- Air communications
- Video teleconference
- Formal message traffic
- Information assurance
- Spectrum management

Each participant in a NATO-led coalition mission will have different CIS capabilities and CIS levels of expertise

Plan review

3.25 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 subordinate HQ supporting plans.

3.26 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, J6 planners should analyse the scope and scale of any change and identify corresponding CIS changes.

Section 6 – Other considerations

Other considerations

3.27 **Mission participants.** Each participant brings 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, mission participants may or may not require communication between the JFC and the higher political and military organizations. Participants will bring and contribute their own capabilities, to include CIS, to the extent that their leadership directs. Existing materiel and non-materiel interoperability between mission participants will differ according to the extent and currency of interactions with participants. Each participant 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, participants may request bi-lateral CIS and services support from NATO, a NATO LN, or another mission partner to assist with their mission support objectives.

3.28 Lead nation. If the staff of a NATO HQ designated to lead a coalition mission is unable to meet coalition mission CIS coordination requirements a NATO LN is expected to assist CIS management structures for that mission. All Alliance and coalition partners should engage continuously during the mission 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 participating entities, requires a robust liaison and collaboration structure at the JFC level to facilitate coordination of collective CIS operations.

3.29 Mission network relationships. The option of allowing participant personnel access to NS or NATO Unclassified mission domains does not exist within NATO security policy. As a result, the inclusion of mission participants 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, polices, and best practices to present and future mission network contributors. When considering future mission network design planners must consider rapidly evolving concepts and technology such as data centricity and zero trust framework, a security approach which requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated. The pace at which these technologies change requires planners to conduct a thorough mission analysis for each mission network being developed. Regular and frequent practice in establishing a federation of mission networks during exercises should improve the ability to establish and operate using capabilities in a federated mission network at non-NS security classification. 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 theatre of operations.

3.30 **Special operations forces CIS.** Special operations forces (SOF) CIS must be integrated into planning, with specific regard to access control to SOF information on mission networks. This includes IT services from traditional forces.

Key points

- Strategic-level planning is conducted as detailed in AJP-5. Inclusion of CIS within the strategic-level OPLAN is vital.

- The operational-level planning process consists of the necessary steps to support an operational commander and staff to develop the operational-level OPLAN. CIS should be woven into each stage of the operational-level planning process.

- CIS planning is comprehensive, cyclical and iterative in nature. It is conducted in close synchronisation with J2, J3 and J5 to ensure consistency with the overall planning effect.

- The main outcome of the CIS planning process is the CIS SUPPLAN.

- The CIS estimate provides an assessment of the CIS capabilities required to support an operation against the CIS assets likely to be available.

- Information exchange requirements are pivotal inputs to the CIS planning process. They ensure that all relevant command and control services required in support of the mission are identified, and that adequate planning and provision of command and control services can be achieved.

- Factors such as spectrum management, vulnerabilities and risk must be factored into the planning process and considered appropriately.

UK Annex 3A

Operational level J6/communication and information systems planning

Operational planning overview

UK 3A.1. Military operations are initiated by political direction through the Defence Crisis Management Process, managed by Security Policy and Operations (SPO), in response to changes in the physical or virtual environment, which could be anything from natural disaster to threatened or actual armed conflict. Military operations form part of the wider pan-government diplomatic, information, military and economic (DIME) response. Political direction may come from the cabinet, the National Security Council or direct from ministers and will result in military-strategic direction issued by the Chief of the Defence Staff (CDS), the Chief of Staff Committee or the Strategy Delivery Group (SDG) or, when time is scarce, direct from Director Operations. Through the Deputy Chief of the Defence Staff (Military Strategic Operations) and the relevant international policy and strategy teams, a CDS planning directive, with planning guidance, is issued to the joint commander, normally Chief of Joint Operations (CJO) and the Permanent Joint Headquarters (PJHQ).

UK 3A.2. The planning directive and guidance shape the operational estimate led by PJHQ J5 or J3, depending on whether the operation is contingency, crisis or conflict. This estimate is conducted by a cross-branch J1–J9 operational planning team (OPT) and results in CJO's operational plan and a statement of requirement.[7] The former is submitted to CDS and then ministers for approval and the latter is staffed back in to SPO for the force sensing and force generation process, where the resources required to deliver the plan are identified in the front line commands (FLCs). The approved operational plan is developed either into a joint contingency plan or an operation order (OPORD)

[7] A combined joint statement of requirement of force elements in a draft order of battle and a theatre capability statement of requirement describing enabling and support requirements.

for immediate use. Following the force generation process SPO, as the Defence Single Tasking Authority (DSTA), will draft an activation order, which places the necessary force elements under command of CJO.

UK 3A.3. This overview describes in a linear manner a process which is far more iterative at every level: CDS is consulted during the drafting of the political direction; CJO informs CDS's directive and guidance; FLCs are engaged to provide environmental and operational domain advice in the SDG and throughout the operational estimate. This ensures the operational plan is realistic and enables concurrent preparation. The finalised OPORD, together with its CIS annex, are issued to the joint task force commander (JTFC), their subordinate component commanders and the other Defence organisations who are supporting the operation.

Command, control, communication, computers, cyber and information in operational planning

UK 3A.4. At the joint level the CIS estimate is not conducted as a stand-alone activity in response to the joint commander's estimate, but through the OPT and integrated at every stage of the operations planning process described in AJP-5. In stages one and two the J6 staff is likely to work with J2 in understanding the information environment. During stages three to six, command, control, communication, computers, cyber and information (C5i)[8] as a limited resource, is likely to place restraints on the different COAs, relating to distance, bandwidth and concurrency or phasing which must be fed into the OPT and may influence the scoring of COAs. In stage seven a large amount of technical detail must be marshalled to write the C5i annex.

UK 3A.5. During the estimate process the J3/J5 focus will be on identifying the fighting power required to achieve the decisive conditions defined in the operational design. The enabling staff, J6 alongside J1/J4, must identify whether the force elements will deploy with organic CIS capability and even if they do, what additional CIS and cyber capability is required to enable operational or wide area command and control, which must be included in the statement of requirement raised to the DSTA. While a complete information flow analysis is unlikely to be possible for each of the COAs in detail during the estimate process, PJHQ J6 must engage with the FLC 6-branches to understand the key joint and component-level flows to identify the services required at each security classification across the whole force. UK Table 3A.1

[8] Defence Digital interpret C5i as standing for (defensive) cyber, command, control, communications, computers and information.

(split in to parts a–d) contains a non-exhaustive outline of the J6 factors to be considered at each stage, broken down by their relevance to the operational plan, the C5i plan and the C5i annex.

Level of planning	Step 1 – initiation
Factors for the operational estimate	• Where in the world is the JOA? o What is the cyber force protection guidance there? o What is the Global System for Mobile Communication (GSM)/4G coverage there? o What is the satellite communications (SATCOM) coverage there (military satellite and commercial satellite)? • What are the likely cyber and electromagnetic activities threats? o Cyberspace (within the JOA and beyond)? o Electromagnetic warfare – direction finding, intercept and jamming? o Electromagnetic countermeasures (force protection) requirements? o Cyber force protection – country portable electronic device colour? • Who is the information asset owner for this operation, and are they qualified to fulfil the role? • What are the likely cross-border protectively marked material movement implications? o Is the country a Vienna Conventions signatory? o Is there a history of protectively marked material holdups or disputes at border (King's Messenger Service or Defence Courier Service)? • Is there an existing joint contingency plan for this theatre? o How current is it? • What recent recce reports are available, is an operational liaison and reconnaissance team deployed that can conduct recce? o Develop requests for information. • What is the data/information management hierarchy for the operation?

Level of planning	Step 1 – initiation
Factors for the communications plan	• What is the size of the JOA? o What distances are communications required, intra- and inter-theatre (including lines of communication, ports of debarkation, forward mounting bases)? o Likely number of points of presence? • What is the terrain for the operation? o How will this affect terrestrial communications (microwave line of sight, Combat Net Radio (CNR) ground plane)? o How will this affect SATCOM azimuth and elevation? • What are the seasonal and weather effects? o Hot and cold effects on equipment? o Wind on masts and dishes? o Foliage affecting line of sight? o Moisture affecting CNR ground plane? o Climatic high frequency/ultra high frequency propagation effects? • Is the JOA covered by Defence High Frequency Communications Service (DHFCS) services? o Are there any memorandum of understanding that need activating to create service effect in the region?
Factors for the communications annex	N/A

UK Table 3A.1a – Step 1: initiation

Level of planning	Step 2 – mission analysis
Factors for the operational estimate	• What is the likely size of the force? • Is the likely force a formed formation or unit with organic communications? o If not, what additional C5i force generation is required? • For each force element required, has the operations information, knowledge management generated the likely information flow analysis? o To/from the joint commander or higher formation? o Between components? o Within components? • What are the critical information flows for success? • With J2/Geographic, identify any J6 named areas of interest/target areas of interest (broadcast facilities, communications hubs, likely locations for headquarters (green field, airport of debarkation, commercial)) across the JOA. • What is the cyber risk to critical infrastructure required to support the operation (for example, airfields, power, ports, rail and road)?

Level of planning	Step 2 – mission analysis
Factors for the communications plan	• What are the likely security considerations for the operation (sovereign – red/black: multinational – blue, and OFFICIAL, OFFICIAL-SENSITIVE, SECRET, TOP SECRET)? o What is the coalition architecture (sovereign, lead nation provides, or mission partner environment)? o What existing coalition networks are relevant (NATO SECRET/ NATO MISSION SECRET)? o What existing fixed gateways are relevant? o What coalition networks can be established over what time frames (joining, membership and exit instructions (JMEIs)/Code of Connection)? o What tactical-level interoperability can be achieved? o What is the plan for coalition key material (keymat)? • What external agencies are there, and how will we communicate with them? o Host nation, non-governmental? o Protective marking of interactions? o Communications provision to detached liaison officers? • For enduring campaigns, can commercial services relieve expeditionary systems for deployment elsewhere, and when should this be done (then plan backwards)? • What critical assets (both CIS and critical infrastructure) need cyber defence?
Factors for the communications annex	N/A

UK Table 3A.1b – Step 2: mission analysis

Level of planning	Steps 3, 4, 5 and 6 – course of action development, analysis, validation and decision
Factors for the operational estimate	• Is the proposed COA going to be constrained by available J6 assets through each phase? • Where is the commander, and are their information requirements met through each phase? • What is the cyber risk against each phase of each COA? • For each force element deployed, how will the CIS information exchange requirements available meet the information flow analysis? • What CIS reserve is required and where (operational CIS and tactical CIS)? • Is re-tasking going to have an impact? Does any preparatory work need to occur to support re-tasking? • At the decision points in the J3 plan, will the decision-makers be able to access the right information (validation of information flow analysis)?
Factors for the communications plan	• Primary, alternative, contingency and emergency (PACE) policy? (Set the J6 commander's appetite for resilience/risk) • Command and control of CIS: is a joint force CIS (JFCIS) required at the outset? Is a JFCIS required if the operation becomes enduring? o What are the command relationships? o Where are the delegations? • What is the impact on J6 of sequencing? • How will cyber force protection measures affect the different COAs? • Are additional defensive cyber operations force elements required to defend CIS and critical infrastructure? • What are the residual J6 risk, and how can they be mitigated? • What emission control measures need to be imposed for each phase? • If electromagnetic countermeasures (force protection) is being used, what are the implications for other emitters? • Have C5i assets been correctly prioritised in the desired order of arrival staff table?
Factors for the communications annex	n/a

UK Table 3A.1c – Steps 3, 4, 5 and 6: course of action development, analysis, validation and decision

Level of planning	Step 7 – plan development
Factors for the operational estimate	• What is the urgent capability requirement/accelerated operational support process for unfulfilled requirements? • If the operation is likely to endure, start to consider commercialisation options.
Factors for the communications plan	• What are the frequency requirements, and through whom are they bid (Defence Electromagnetic Authority, host nation, coalition BSM cell)? o Establish the joint restricted frequency list. • What enhanced support requests need to be raised for Defence Digital-delivered systems? • What enhanced cybersecurity monitoring requests need to be raised for Defence Digital-delivered systems? • Are cyber force protection measure complete and appropriate? o What portable electronic devices permissible? o Cyber mission assurance usage and instructions? • What is the common operating picture (COP) application (at operational and tactical levels)? o Is the COP complete (all necessary feeds)? o Is the COP accessible to the right headquarters? o Is the COP timely? o What is the database and hosting architecture? o Is there a requirement for any specialist equipment, such as specialist audio-visual equipment? • What are the tactical data link requirements? o Key sensors? o Key recipients? o Protocols, modernisation? • What are the information management plans for: o SharePoint structure and management? o Email naming conventions, distribution? o Dialling directories? o Hosting and server locations? • How are the record retention/operational record keeping policies going to be delivered (electronic archiving or hard disk drive date cuts)? • How will crypto be distributed (electronic, data crypto system, casual courier)? o Is a theatre distribution agency required? • How will welfare communications be delivered, in line with cyber force protection?

Level of planning	Step 7 – plan development
Factors for the communications annex	• Can all crypto and keymat be distributed across the force in a timely manner? o How much keymat needs to be held at each point of presence? • Are all force elements included in the communications electronic instruction? o Bowman plan o Tactical satellite channels o Owner o Attachments and Detachments • Develop operation-specific J6/defensive cyber operations input to pre-deployment training, Joint Air Movement Centre briefs, reception, staging, onward movement and integration. • Sustainment of CIS in all points of presence. o Fuel and batteries. o Second line support affiliations. o Spares packs and where they should be located. • What are the crypto compromise procedures, and are they understood by everyone? • What are the crypto emergency destruction procedures, and are they understood by everyone?

UK Table 3A.1d – Step 7: plan development

UK 3A.6. The delivery and management of joint CIS across the JOA is a complex task, usually requiring a commander joint force CIS (JFCIS). For this, the joint commander issues a CIS annex to their own directive, written by PJHQ J6, detailing commander JFCIS' responsibilities to direct the CIS in the JOA and to provide operational CIS advice to the JTFC and staff. The CIS annex also specifies the operational-level freedoms and constraints for commander JFCIS. Commander JFCIS is delegated operational control (OPCON) of all CIS resources in the JOA (apart from special forces) and draws core staff from the lead deploying headquarters. It may also be augmented by other J6 staff from PJHQ, FLCs, Defence Digital and other organisations, to match the scale and nature of the operation. Commander JFCIS' responsibilities are outlined in the generic terms of reference at UK Annex 3B. When CDS' Directive does not stipulate the need for a dedicated commander JFCIS, on a small-scale operation for example, then a post should be nominated within the joint task force headquarters or the J6 division at PJHQ to fulfil the role. In the case of concurrent operations, when more than one commander JFCIS is required, they may be force generated as ad hoc organisations or the task may be directed to an FLC.

UK 3A.7. **Joint force communications and information services functions.** Operational experience has identified nine broad functions delivered by a JFCIS. The size and complexity of the operation will determine how each of them is met: this may be entirely through a deployed JFCIS or some may be delivered remotely by external organisations operating from base locations.

a. **Understand.** Underpinning all other functions is the need to comprehensively understand the intent, priorities, concerns and requirements of the various operational headquarters and supported commanders by engaging with them and their C5i enablers frequently. It also encompasses understanding emerging requirements, the capabilities currently deployed and the threat environment, which may be external or from poor cybersecurity practice from users within the force.

b. **Plan.** The need to plan is most likely to be driven by changes in the operational situation, whether in disposition or scope. By planning sufficiently far in advance, the need for additional assets can be raised early to enable force sensing and force generation.

c. **Deliver.** This function encompasses development and delivery of changes, improvements and new capabilities. Delivery encompasses both where it can be delivered using in-theatre resources and where additional resources, infrastructure, expertise or finance are required. A Defence Digital liaison officer embedded in JFCIS is pivotal.

d. **Operate.** There is a requirement for sensors and tools to be able to monitor and interrogate networks and information systems. The operation function is focused on ensuring optimal performance of systems and services. Where an event or incident is beyond the capability of the information and communication services detachment to resolve, additional capacity, skills, analysis and resources may be required. These capabilities are delivered through service management and are essential to enable the mission through information and communication services. This is provided through a combination of military personnel and contractor support. This function is likely to be delivered, on behalf of the JFCIS, by the cyber security operations capability (CSOC) described below.

e. **Defend.** There is a requirement for sensors, tools and a comprehensive recognised cyberspace picture[9] to enable us to identify, protect, detect, respond and recover systems and services. There is also a need to inculcate a culture that prioritises information security to project a suitable defensive cyber posture across the force. This should be supplemented by deliberate defensive cyber operations to target offensive activity and preserve our freedom of manoeuvre within cyberspace. Responsibility for this is likely to be split, with the CSOC delivering the technical monitoring elements and the deployed JFCIS providing direction and guidance to deployed force elements.

f. **Support.** Support can be provided through a combination of military CIS detachments and contractor support. First line support for many systems is provided via the Single Point of Contact (SPOC), with shadow support provided by CIS detachments to mitigate contractual limitations and the lack of operational context. The CIS detachments themselves rely on the JFCIS for logistic and cryptographic replenishment.

g. **Exploit.** Decision-makers and the broader user base must be supported to exploit all available technology and information best practice. This involves assisting in better organising of data and information, use of relevant and timely information displays, and development of low-code applications, which would ensure optimal situational awareness and improved decision-making.

h. **Assure.** Linked to defence, support and exploit, there is a requirement to assure these functions across the JFCIS JOA. As well as mandated cryptographic and security checks, assurance is ensuring compliance with correct procedures by users and reporting of security incidents. This should include level 1 (C5i detachment self-assessment) and level 2 (JFCIS) assurance, with primary focus on advice, guidance and the capture and dissemination of best practice.

[9] See AJP-3.20, *Allied Joint Doctrine for Cyberspace Operations* for more detail.

i. **Develop.** Finally, there is a requirement for continuous improvement in terms of organisation and structure, functions delivered, the tools used, the quality of services delivered, efficiencies that can be realised and communication to improve the perception of our supported commands. This may be through the force generation of additional resources through PJHQ to the DSTA or through urgent capability requirements.

UK 3A.8. **Joint force communications and information services structure.** The core structure of JFCIS includes the following branches.

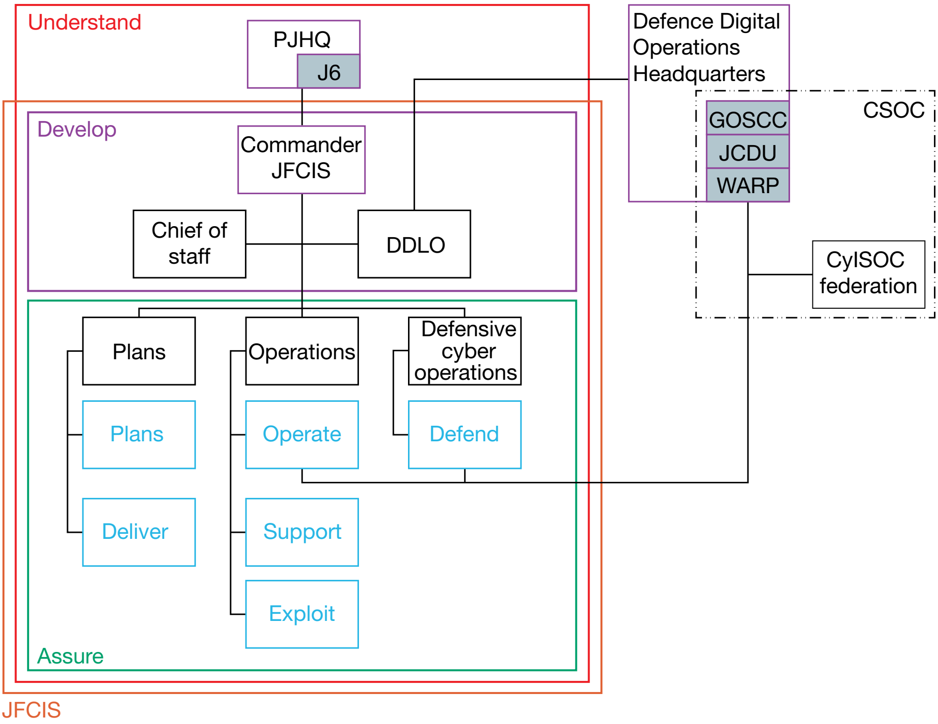
a. **Operations.** This involves current tasking and engineering support of CIS assets supporting manoeuvre operations.

b. **Plans.** This covers planning future manoeuvre operations and delivering against new requirements and major technical changes.

c. **Defensive cyber operations.** This covers managing information assurance policy and risk.

d. **Information management.** This covers administering permissions and information structures, and supporting information management best practice.

An outline of how these branches deliver the functions is shown in UK Figure 3A.1.



CSOC	cyber security operations capability
CyISOC	cyber and information services operations centre
DDLO	Defence Digital liaison officer
GOSCC	Global Operations and Security Control Centre
JCDU	Joint Defensive Cyber Unit
JFCIS	joint force communication and information systems
PJHQ	Permanent Joint Headquarters
WARP	warning advice and reporting point

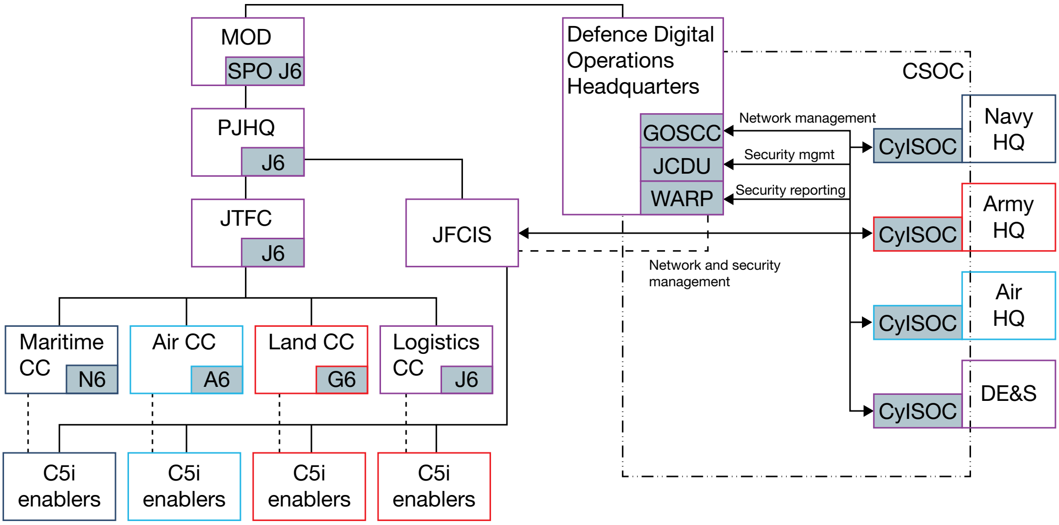
UK Figure 3A.1 – Joint force communications and information systems functions and basic structure

UK 3A.9. **Multinational operations.** The CIS requirements of a UK force in multinational operations, whether NATO or within ad hoc coalitions, are influenced by the UK's role and status within the operation.

Command, control, communication, computers, cyber and information organisations

UK 3A.10. Several key organisations contribute to C5i.[10] The relationship between them is shown in UK Figure 3A.2.

[10] All of the organisations shown, from the strategic to the tactical level, either liaise or work directly with civilian partner companies to deliver operational CIS capability.



C5i	command, control, communication, computers, cyber and information
CC	component command
CSOC	cyber security operations capability
CyISOC	cyber and information services operations centre
DE&S	Defence Equipment and Support
GOSCC	Global Operations and Security Control Centre
HQ	headquarters
JFCIS	joint force communication and information systems
JTFC	joint task force commander
JCDU	Joint Defensive Cyber Unit
MOD	Ministry of Defence
PJHQ	Permanent Joint Headquarters
WARP	warning advice and reporting point

←→	liaison
- - - - -	tactical command
———	operational command/control

UK Figure 3A.2 – C5i organisations

Defence Digital

UK 3A.11. Defence Digital provides CIS to meet Defence needs and a single point of contact for strategic planning. The Operations Directorate provides direct support through:

- conducting network and security operations, and defensive cyber operations to provide C5i mission assurance for the totality of Defence;

- leading digital federation activity in support of military operations, and providing spectrum management, configuration management and complex change projects; and

- providing service integration and management, and the underpinning tooling the information technology operations processes.

UK 3A.12. Defence Digital advises PJHQ J6 during the operational estimate. Defence Digital Operations Headquarters achieves this by coordinating the efforts of its delivery teams and Defence CIS service delivery partners, and by working with PJHQ, commander JFCIS and FLCs to design the optimum CIS solution. The resultant 'network of networks' is managed through Defence Digital's Global Operations and Security Control Centre (GOSCC) and the federated CSOC. As the primary Defence CIS service provider, Defence Digital is the design authority for the core-funded operational CIS solutions.

Cyber security operations capability

UK 3A.13. Each of the single-Service commands and Defence Equipment and Support, has its own cyber and information services operations centre (CyISOC). These organisations, which deliver both network operations and security operations centre functions, are responsible for managing an assigned portion of the Defence Digital enterprise, as well as those platform-focused systems with large C5i components unique to its role. They are responsible to their single-Service commands (or other) chains of command but are entities within the CSOC federation.

UK Annex 3B

Generic terms of reference for commander joint force communication and information systems

UK 3B.1. Commander JFCIS is an officer experienced in joint CIS matters, normally from the permanent CIS staff of the FLCs, PJHQ or joint force headquarters. They are delegated OPCON of all CIS capabilities in the JOA (apart from special forces) and directs all CIS on behalf of the JTFC.

UK 3B.2. Commander JFCIS is appointed by the joint commander, as detailed in the CIS annex of the joint commander's directive to the JTFC. The rank of the commander JFCIS is determined by the scale of the operation, the quantity and complexity of the CIS support required, and by any representational considerations arising in multinational operations. Commander JFCIS is responsible for:

- providing CIS advice to the JTFC;

- exercising OPCON of all JTFC-assigned CIS capability within the JOA (apart from special forces) commensurate with the JTFC's scheme of manoeuvre;

- in conjunction with J3 staffs, developing, ratifying and maintaining the joint information flow analysis and information exchange requirement of the operation;

- CIS input to the joint estimate process;

- leading the CIS capability audit for the operation, facilitating the agreed design of the CIS solution and staffing urgent statements of user requirement to PJHQ so that existing capability can be generated or accelerated operational support or urgent capability requirements can be staffed;

- overseeing and updating the cyber mission assurance plan, incorporating the cyber prioritised defended asset list for CIS deployed in the JOA;

- informing PJHQ J6 of all CIS and cybersecurity issues and risks that may have impact at the operational level, including the alerting, warning and reporting of incidents, as the sub-warning and reporting point;

- liaison with host nation, multinational, other government department, non-governmental organisation and international organisation representatives for JOA CIS requirements;

- implementing local network changes and system updates as directed by Defence Digital Operations Directorate. Work with the GOSCC and relevant CyISOCs for systems deployed in the JOA to ensure continuity and security of CIS delivery; and

- ensuring the effective integration of any civilian service providers to achieve the required level of operational CIS capability.

Notes

Chapter 4

Chapter 4 briefly outlines the relevance of communication and information systems to the command and control environment and provides a short overview of command facilities. Consideration factors for exercises, and for the pre-deployment, deployment and drawdown phase of operations, are also explored.

> Science is organised knowledge.
> Wisdom is organised life.
>
> Immanuel Kant

Chapter 4

Employment of communication and information systems

Command and control (C2) services support information collection, situation assessment, decision making, collaboration, C2, and mission planning and execution. Coordinated and coherent C2 within a North Atlantic Treaty Organization (NATO)-led mission is enabled by NATO communication and information systems (CIS)[45] employed at the strategic and operational levels of command.

Section 1 – Introduction to the command and control environment

4.1 NATO doctrine recognizes two valid planning processes, strategic and operational. The second planning process is utilized in below strategic planning efforts and is outlined in AJP-5. 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 0593/1, *Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations*.

[45] Per Military Committee Joint Standardization Board (MCJSB) tasking NSO(JOINT)0204(2022)JSB, AJP 6.1 *Allied Joint Doctrine for Communications and Information Systems Service Management & Control*, is in development.

Section 2 – Command facilities

4.2 A requisite headquarters (HQ) command facility can be static or deployable and may consist of HQ joint operations centre (JOC) 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 and security and real-life support to the staff. HQ CIS facilities should have well-trained personnel and formal procedures in place to be able to constantly monitor and assess CIS status and restore or repair CIS services, when required. Service management and control (SMC) is the single governed capability which covers all layers from communication and information systems, management processes and procedures created for the purpose of an operation, exercise, training event and /or interoperability verification activity, using a flexible and tailored set of non-materiel (policy, processes, procedures and standards) and materiel (static and deployed networks, services, supporting infrastructures) contributions provided by all participants. Non-material contributions can include policy, processes, procedures, and standards. Material contributions can include static and deployed networks, services and supporting infrastructures. SMC requirements and processes for federated CIS should be thoroughly implemented. There are four tiers of communications. Tier 1 is strategic communications, tier 2 is theatre communications, tier 3 is force level communications, and tier 4 is communications within mobile units.

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.

c. **Mobile command nodes.** These nodes may be embedded on tactical command post (CP) platforms, in order to ensure minimal C2 capabilities. Mobile command nodes could be deployed to low tactical levels (up to tier 4, by exception tier 3) or on-board specific air or maritime platforms.

Section 3 – Exercises

4.3 NATO education and training is governed by MC 0458, *NATO Education, Training, Exercise and Evaluation (ETEE) Policy*, 3 January 2023. 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. Additionally multinational CIS exercises are essential in proving and developing interoperability profiles for different services, such that standing multinational formation can have JMEIs available for crisis response.

Section 4 – Pre-deployment, deployment considerations

4.4 Each stage of operations[46] has unique activities in communications planning.

Pre-deployment activities (associated with force generation stage and build up of enabling capabilities in AJP-3)

4.5 During this time, the operational commander is designated and forces are assigned. The North Atlantic Council initiating directive provides the operational commander with guidance to initiate planning. The joint force commander (JFC) issues a mission statement and commander's intent. Subsequent to the mission statement and commander's intent, the concept of operations (CONOPS) is developed.

[46] Additional information regarding planning and execution can be found in AJP-3 and AJP-5.

4.6 The objective of pre-deployment 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 operation plan (OPLAN). This OPLAN may have to consider en-route communications to support initial tactical entry.

4.7 To begin mission analysis and initial planning, the Supreme Headquarters Allied Powers Europe (SHAPE) and JFC J2, J3, J5, and J6 staffs should clearly understand the command relationships of the joint force.

4.8 This phase of the operation normally relies exclusively on the existing commercial, strategic, and tactical communications infrastructure.

4.9 The operational commander must assign a spectrum manager to coordinate national spectrum management requirements of all mission participants. Establish a theatre spectrum management cell to support sending nations during deployment with spectrum coordination activities, and to ensure sufficient spectrum resources are available in the joint operations area (JOA) in support of mission activities. Battlespace spectrum management is the practical coordination, consolidation, deconfliction, and allocation of all radio frequency electromagnetic spectrum (EMS) usage, as well as the identification and resolution of electromagnetic interference within the operating environment. It is an integral part of supporting the theatre commander in managing the overall operating environment. The theatre spectrum management cell works with the host nation (HN) or the organization that assumes responsibility for the EMS.

4.10 Reachback capabilities need to be considered in pre-deployment activities. These considerations should include types of data required for analysis, means of data transport, and procedural requirements for the request of information.

Deployment activities (associated with deploying to the area of responsibility in AJP-3)

4.11 As the OPLAN is completed and published, CIS are expanded to provide improved information flow between the joint force commander 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.

4.12 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.

4.13 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.

Execution activities (associated with execute operations and assess and review in AJP-3)

4.14 On commencement of the execution stage, CIS plans are to be reviewed for detailed transition planning. Strong coordination is required between internal service providers and J6 staffs of all participants to minimise service disruption during plan execution. These reviews and plan adjustments are an iterative process which will occur throughout mission execution.

Drawdown activities (associated with redeploy force in AJP-3)

4.15 The end of an operation requires a force downsizing phase. Therefore, the J6 planners should develop a CIS plan to reduce CIS services and resources accordingly. Where the JOA has been commercialized during the campaign, it may be necessary to re-insert expeditionary systems in order to allow forces to draw-down gracefully. Throughout the drawdown, information services should continue to meet the operation's information exchange requirements (IER)s for the remaining force elements until final departure.

4.16 Critical redeployment considerations are split between incoming replacement forces and HN coordination.

4.17 The theatre spectrum management cell should ensure sufficient spectrum resources are retained in order to support redeployment operations. The theatre spectrum management cell works with the HN or the organization that assumes responsibility for the radio frequency EMS.

Key points

- A headquarters command facility provides the working environment and CIS support for the functional staff areas and security and real-life support to the staff. Headquarters CIS facilities should have formal procedures in place to consistently monitor and assess CIS status and restore or repair CIS services when required.

- Pre-deployment considerations include producing a CIS plan to support the commander's intent, CONOPS to support the initial and follow on CIS deployment package, spectrum management and reachback considerations. This phase may rely heavily on existing commercial, strategic and tactical CIS infrastructure.

- During the deployment phase, CIS are expanded to provide improved information flows. CIS support should factor in resilience to ensure maintenance of support.

- Coordination, constant review and plan adjustments as required are a key feature of the execution phase.

- A comprehensive drawdown plan should be prepared in advance. During this phase, information services should continue to meet the commander's IERs for remaining force elements until final departure.

Annex A

AJP-3, AJP-5, AJP-6 alignment points

AJP-3, AJP-5, AJP-6 alignment points

	AJP-5 **Planning Phases**	**AJP-6** **Chapter 3/4 Sections**	**AJP-3** **Operations Stages**
		CIS Readiness	
See tables 1 and 2 of this Annex for a list of products and potential planning factors.	1 Initiation	Operations Planning	Analysis (framing the problem and environment);
	2 Mission analysis		
	3,4,5 & 6 COA Dev, Analysis, Validation, Decision		Developing an OPLAN
	7 Plan Development		
		Pre-Deployment	Force generation and preparation, including build-up, assembly, and pre-mission training
			Build-up of enabling capabilities like logistic and medical support
		Deployment	Deploying to the area where operations are to be conducted or to reinforce in-place forces
		Execution, including operational planning is a cyclical process which utilizes the AJP-5 planning phases, nested at all levels of operation.	Execute operations
See tables 1 and 2 of this Annex for a list of products and potential planning factors.	1 Initiation		Assess and review
	2 Mission analysis		Adjust the conduct of operations as required
	3,4,5 & 6 COA Dev, Analysis, Validation, Decision		
	7 Plan Development		
		Draw Down	Operations (mission) termination and transition
			Re-deploy forces
			Identity lessons

Figure 1 – AJP alignment points

Sample Products			
1 Initiation	2 Mission analysis	3, 4, 5 & 6 COA Dev, Analysis, Validation, Decision	7 Plan Development
(I) Strategic Planning Directives or Strategic CIS Planning Guidance		O) Operational CONOPS (incl. CIS Annex with IERs)	
(I) Strategic CIS Assessment	(O) Operational CIS Assessment		(O) Operational OPLAN (incl. CIS Annex with CIS Service Matrix)
(I) Strategic CIS Estimate	(O) Operational CIS Estimate		(O) CIS Support Plan (SUPPLAN)
(I) Strategic OPLAN (incl. CIS Annex)			((O) Draft CJSOR (CIS requirements)
(I) Operational Commanders Information Requirements			(O) Draft TCSOR (CIS Requirements)

Table 1 – Sample Products

Sample Products			
1 Initiation	2 Mission analysis	3, 4, 5 & 6 COA Dev, Analysis, Validation, Decision	7 Plan Development
Mission Type	Size of joint force and likely number of points of presence in-theatre	CIS availability / constraints in a proposed COA	Capability delivery processes for unfulfilled requirements
JOA Location and Size, climate conditions	Type of the force (degree of jointness and multi-nationality requirement to deploy air and maritime operation centres forward, incorporation of non-military agencies)	Joint Force Commander's information requirements through each phase	Record retention policies and method of delivery

Sample Products			
1 Initiation	2 Mission analysis	3, 4, 5 & 6 COA Dev, Analysis, Validation, Decision	7 Plan Development
Cyber Electromagnetic Activity Threats	Depth of multi-nationality (down to which level of command - battalion, brigade, division, corps or component command	CIS reserve requirements (OpCIS and TacCIS)	frequency requirements and controlling authority (host nation, coalition battle space management (BSM) cell)
Applicable Security Policy(s) for the operation	Known IERs between C2 nodes and external agencies	ToA/Tasking limitations CIS units and assets	Status of CIS force protection measures
Terrain characteristics (what kind of bearer systems can be used)	Likely security domain(s) for the operation	Known interoperability shortfalls of potential participants	Status of IERs
SATCOM coverage (MILSAT and COMSAT)	Critical CIS Terrain (broadcast facilities, high points etc.)	Sustainment of CIS capabilities	IM Authority appointment and availability of an initial IM Plan
Existing communications infrastructure (e.g., mobile and static phone networks)	Coalition architecture (types and sizes of C2 nodes that need to be supported)	Impact of Cyber Force Protection requirements	Service Management Authority appointment and availability of an initial SM Plan
Protectively Marked Material (e.g., Crypto) movement restrictions	For enduring campaigns, can commercial services relieve expeditionary systems	Maturity of Service Management capabilities of CIS units	Crypto management and distribution system requirements
Electromagnetic Spectrum availability	Lines of Communications	Redundancy and resiliency requirements	CIS logistics requirements and integration into the Logistics and Deployment Plans
		Electronic countermeasures requirements	
		Tactical Data Link requirements	

Table 2 – Potential planning factors

Intentionally blank

Lexicon

Part 1 – Acronyms and abbreviations

ACO	Allied Command Operations
ACP	Allied communications publication
ACT	Allied Command Transformation
AJP	Allied joint publication
ASB	Agency Supervisory Board
BSM	battlespace spectrum management
C2	command and control
C3	consultation, command and control
C5i	command, control, communications, computers, cyber and information
CDS	Chief of the Defence Staff
CIS	communication and information systems
CJO	Chief of Joint Operations
CMA	cyber mission assurance
CNR	Combat Net Radio
COA	course of action
COI	community of interest
COMPUSEC	computer security
COMSEC	communications security
CONDO	contractors deployed on operations
CONOPS	concept of operations
COP	common operating picture
CP	command post
CSOC	cyber security operations centre
CyISOC	cyber information services operating centre
DCIS	deployable communication and information systems
DCOS	Deputy Chief of Staff
DEMA	Defence Electromagnetic Agency
DHFCS	Defence High Frequency Communications Service
DIME	diplomatic, information, military and economic
DSTA	Defence Single Tasking Authority

EDT	emerging and disruptive technologies
EMCON	emission control
EMS	electromagnetic spectrum
FLC	front line command
FMN	federated mission networking
GOSCC	Global Operations and Security Control Centre
GSM	Global System for Mobile Communication
HN	host nation
HQ	headquarters
ICT	information and communications technology
IER	information exchange requirement
IM	information management
INFOSEC	information security
JDP	joint doctrine publication
JFC	joint force commander
JFCIS	joint force communication and information systems
JMEI	joining, membership, and exit instructions
JOA	joint operations area
JOC	joint operations centre
JSP	joint Service publication
JTF	joint task force
JTFC	joint task force commander
LN	lead nation
MC	Military Committee
MOD	Ministry of Defence
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 Group
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NS	NATO secret

OPCON	operational control
OPLAN	operation plan
OPORD	operation order
OPSEC	operations security
OPT	operational planning team
PACE	primary, alternative, contingency and emergency
PJHQ	Permanent Joint Headquarters
RADSEC	radiation security
SACEUR	Supreme Allied Commander Europe
SDG	Strategy Delivery Group
SECAN	Military Committee Communication and Information Systems Security and Evaluation Agency
SHAPE	Supreme Headquarters Allied Powers Europe
SMC	service management and control
SOF	special operation forces
SOR	statement of requirements
SPO	Security Policy and Operations
SPOC	Single Point of Contact
STANAG	NATO standardization agreement
SUPPLAN	support plan
TSCMA	technical security countermeasures assessment
WAN	wide area network

Part 2 – Term and definitions

architecture

The fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution Architecture is a consistent whole of principles, methods and models that are used in the design and realisation of organizational structure, business processes, information systems, and infrastructure.

(Not NATO Agreed)

communication and information system security

The application of security measures for the protection of communication, information and other electronic systems, as well as the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

(NATO Agreed)

commonality

The state achieved when the same doctrine, procedures or equipment are used.

(NATO Agreed)

communication

The imparting or exchanging of information by speaking, writing, or using some other medium.

(Concise Oxford English Dictionary).

communication and information systems

CIS

Collective term for communication systems and information systems.

(NATO Agreed)

communication system

An assembly of equipment, methods and procedures and, if necessary, personnel, organized to accomplish information transfer functions.

Notes:

1. A communication system provides communication between its users and may embrace transmission systems, switching systems and user systems.
2. A communication system may also include storage or processing functions in support of information transfer.

(NATO Agreed)

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

concept of operations
CONOPS
A clear and concise statement of the line of action chosen by a commander in order to accomplish his given mission.
(NATO Agreed)

control
The authority exercised by a commander over part of the activities of subordinate organizations, or other organizations not normally under their command, encompassing the responsibility for implementing orders or directives.
(NATO Agreed)

coordinating authority
The authority granted to a commander, or other individual with assigned responsibility, to coordinate specific functions or activities involving two or more forces, commands, services or organizations.
Note: The commander or individual has the authority to require consultation between the organizations involved or their representatives, but does not have the authority to compel agreement.
(NATO Agreed)

cyber mission assurance
A process to protect or ensure the continued function of capabilities and assets that are critical to the execution of a mission.
(JDP 0-01.1)

cyberspace
The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.
(NATO Agreed)

cyber defence
The means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed, or transmitted in these systems.
(NATO Agreed)

data centric security
DCS
A security model that relies on self-describing and self-protecting data and information, and is implemented through a comprehensive set of policies, metadata, and other means to protect, control, and share data and information independent of the business context and across all lifecycle stages.
(This term is a new term and definition and has been processed for NATO Agreed status via terminology tracking file 2022-0177)

defensive cyber operation
Active and passive measures taken to prevent, nullify or reduce the effectiveness of adversary actions to preserve our freedom of action in or through cyberspace.
(JDP 0-01.1)

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. (NATO Agreed)

enterprise architecture
The formal description of a capability, or its detailed plan, at the level required to guide its implementation, including a description of the capability components, their relationships, and the principles and guidelines governing design and evolution over time.
(This term is a new term and definition and has been processed for NATO Agreed status via terminology tracking file 2022-0175)

federated
(Of a country or organization) set up as a single centralized unit within which each state or division keeps some internal autonomy.
(Concise Oxford English Dictionary)

federation
A named set of interacting federates, a common federation object model and supporting runtime infrastructure that are used as a whole to achieve some specific objective.
Note: A federation thus offers a synthetic environment within which humans may interact through simulation at multiple sites networked using compliant architecture, modelling, protocols, standards, and data.
(NATO Agreed)

host nation
A country that, by agreement:
a. receives forces and materiel of NATO member states or other countries operating on/from or transiting through its territory;
b. allows materiel and/or NATO and other organizations to be located on its territory; and/or
c. provides support for these purposes.
(NATO Agreed)

information
The knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning.
(NATO Adopted)

information management
IM
In an information processing system, the functions of controlling the acquisition, analysis, retention, retrieval, and distribution of information.
(NATO Agreed)

information system
An assembly of equipment, methods and procedures and, if necessary, personnel, organized to accomplish information processing functions.
(NATO Agreed)

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

interchangeability
The ability of one product, process or service to be used in place of another to fulfil the same requirements.
(NATO Agreed)

interoperability
The ability to act together coherently, effectively and efficiently to achieve Allied tactical, operational and strategic objectives.
(NATO Agreed)

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

mission assurance
A process to protect or ensure the continued function and resilience of capabilities and assets, critical to the execution of mission-essential functions in any operating environment or condition.
(NATO Agreed)

operation
A sequence of coordinated actions with a defined purpose.
(NATO Agreed)

operations security
All measures taken to give a military operation or exercise appropriate security, using passive or active means, to deny an adversary knowledge of the essential elements of friendly information or indicators thereof.
(NATO Agreed)

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

risk
An uncertain future event that could affect the Department's (MOD's) ability to achieve its objectives.
(JSP 892)

tactical command
The authority delegated to a commander to assign tasks to forces under their command for the accomplishment of the mission assigned by higher authority, and to retain or delegate tactical control of units.
(NATO Agreed)

Corporate member of
Plain English Campaign
Committed to clearer
communication
235

Designed by the Development, Concepts and Doctrine Centre

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