ATP 6-02.61

Expeditionary Mission Partner Network Operations

DECEMBER 2023

HEADQUARTERS, DEPARTMENT OF THE ARMY

Army Techniques Publication
No. 6-02.61

Headquarters
Department of the Army
Washington, D.C., 06 December 2023

Expeditionary Mission Partner Network Operations

Contents

Figures

Tables

This page intentionally left blank.

Preface

ATP 6-02.61 provides guidance for the Army to conduct operations with mission partners; federal departments and agencies; state, local, and tribal governments and agencies; nongovernment organizations; private sector organizations; allies; coalition members; host nations; and other nations and multinational treaty organizations. Working on a common network, these entities exchange information to facilitate command and control. These entities use a digital common operational picture and collaborate among commanders and staffs to facilitate real-time coordination and the exchange of staff products, reports, and returns.

The principal audience for ATP 6-02.61 is Army professionals who plan, install, operate, maintain, and secure tactical networks as a United States lead corps or division multinational force headquarters with staff sections lead by U.S. officers. Commanders and staffs of Army headquarters serving as a joint task force or multinational headquarters also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Trainers and educators throughout the Army also use this publication.

Commanders, staffs, and subordinates ensure decisions and actions comply with applicable United States, international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure that their Soldiers operate in accordance with the law of armed conflict and the rules of engagement. Refer to FM 6-27 for more information on the law of armed conflict.

ATP 6-02.61 implements American, British, Canadian, Australian, and New Zealand (ABCANZ) Standard 2100 Edition 4 by integrating it into Army doctrine.

ATP 6-02.61 uses joint terms where applicable. Selected joint and Army terms and their definitions appear in both the glossary and the text. For definitions shown in the text, the term is italicized and the proponent publication follows the definition.

Providing information on the product ITIL® does not constitute the Army's endorsement of the product.

ATP 6-02.61 applies to the Active Army, Army National Guard/Army National Guard of the United States and United States Army Reserve unless otherwise stated.

The proponent of ATP 6-02.61 is the United States Army Combined Arms Center. The preparing agency is the Combined Arms Doctrine Directorate, United States Army Combined Arms Center. Send comments and recommendations on DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, United States Army Combined Arms Center and Fort Leavenworth, ATZL-MCD (ATP 6-02.61), 300 McPherson Avenue, Fort Leavenworth, KS 66027-2337; by email to usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@army.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Introduction

The future of Army warfare will consist of unified action partner operations with multiple mission partners from all levels of government and participating allies. Requirements for combined multinational formations have intensified since America's entry into the First World War. Coupled with shrinking defense budgets and growing or competing requirements, requirements have resulted in multiple levels of strategic goals, operational needs, and doctrinal shifts that drive permissive information sharing.

Past operations display a trend of stovepiping information that hinders permissive sharing of operational information with multinational mission partners. Throughout the Army, interoperability is viewed by institutional force and operating forces as a purely technical problem. The level or degree of interoperability to succeed at the tactical edge requires equal emphases on the human and procedural aspects of interoperability. This publication provides technical, human, and procedural integrational planning for corps and below multinational force command post Department of Defense information network operations.

ATP 6-02.61 outlines doctrinal techniques for planning and executing Department of Defense information network operations on an expeditionary mission partner network as part of a United States lead multinational force headquarters at the corps and division levels with staff sections led by United States officers. It provides operational framework to support multinational interoperability planning efforts to increase overall command and control information exchange interoperability. There is information to assist the signal planners in multinational planning—to include an operation order and the signals annex development—and network, automated system, and application information exchange execution. This information helps when developing Department of Defense information network operations on a mission partner network in multinational program of instruction products and unit multinational interoperability standard operating procedures.

To apply the techniques contained in this publication, readers should be familiar with ADP 1, ADP 3-0, FM 3-0, and FM 3-16 to understand how Army forces conduct operations as part of a multinational force. Commanders and network planners should also be familiar with FM 6-02, ATP 6-02.12, ATP 6-02.60, and ATP 6-02.62 to understand the role of signal formations and staffs in support of Army and multinational force operations.

This publication contains six chapters and five appendices. The following paragraphs provide a brief introduction by chapter and appendix.

Chapter 1 introduces the mission partner network. It provides an overview of the general operational requirements and discusses the specific requirements by area.

Chapter 2 discusses conducting Department of Defense information network operations in a multinational force. Section I provides an overview of Department of Defense information network operations. Section II describes a coalition network operations and security center at the multinational force headquarters and a network operations center at the subordinate units. Section III discusses the components of Department of Defense information network operations in a multinational force.

Chapter 3 discusses network management on the mission partner network.

Chapter 4 discusses information dissemination management and content staging on the mission partner network.

Chapter 5 discusses cybersecurity on the mission partner network.

Chapter 6 discusses integrating the multinational force common operational picture.

Appendix A is an excerpt from the American, British, Canadian, Australian, and New Zealand Coalition Handbook. It has a collection of planning questions for staffs to answer to mitigate interoperability gaps.

Appendix B is a list of high priority command and control information exchange products, reports, and returns that may be exchanged among the multinational force and subordinate headquarters.

Appendix C discusses change management on the mission partner network. It outlines the requirement for and function of a multinational force change advisory board and articulates its role in the change management process.

Appendix D discusses service desk operations within a coalition network operations and security center and network operations center to support multinational operations.

Appendix E discusses the common operational picture coordination cell. Section I provides an overview of the common operational picture coordination cell. Section II provides an example standard operating procedure for the common operational picture coordination cell.

Chapter 1
The Expeditionary Mission Partner Network

This chapter introduces the mission partner network (MPN). Section I gives an overview of the expeditionary MPN. Section II gives an overview of the general operational capabilities for the MPN. Section III provides specific capabilities by area.

SECTION I – OVERVIEW OF THE EXPEDITIONARY MISSION PARTNER NETWORK

1-1. In current dynamic operational environments, the U.S. Army has a short timeline (hours to days) to integrate with mission partners in key functions and capabilities. The current Army's smaller size, combined with the nature of today's multidomain operations (air, land, maritime, space, and cyberspace), requires the Army to train and be prepared to fight with coalition and mission partner forces. The Army component of a multinational force must be able to leverage all the capabilities in ways that facilitate accomplishing both U.S. and multinational objectives. Within a multinational force, various levels of interoperability exist among mission partners. Commanders, planners, and operators make every effort to maximize interoperability understanding that some partners may not be able to achieve full integration.

1-2. Mission partner is the Department of Defense term that includes other Federal departments and agencies; state, local, and tribal governments and agencies; nongovernment organizations; private sector organizations; and allies, coalition members, host nations, and other nations. Refer to DODI 8110.01 for more information on mission partners.

1-3. To integrate and share information with mission partners, the Army uses a shared network and services, allowing the mutual use of information services and communications capabilities at all echelons. Shared networks enable collaboration, rapid dissemination of information and intelligence products, and the ability to project decisions based on common situational understanding. In multinational operations, signal elements provide shared networking capabilities by implementing a mission partner environment (MPE). Refer to FM 6-02 for more information on shared networking.

1-4. An MPE is an operating framework enabling command and control and information sharing for planning and execution across the range of military operations at a single security level with a common language. An MPE enables a multinational force to exchange information with all participants in a specific partnership or coalition. An effective MPE includes technical, human, and procedural dimensions of interoperability to enable timely, complete, and accurate information sharing, process execution, and unity of effort among mission partners. Refer to DODI 8110.01 for more information on MPE.

1-5. An MPN is a network portion of a MPE and is a specific partnership or coalition-wide area network, planned and implemented using standards and protocols agreed to by participants. The MPN is tasked with the operational requirements to enable a robust network transmission capability and execution of tactical Department of Defense information network (DODIN) operations. It enables the display and sharing of relevant, collaborative information among mission partners. The MPN provides the backbone or end-to-end capabilities used for acquiring, processing, storing, transporting, controlling, and presenting information on demand to multinational forces. Mission partner staffs manage the MPN using relevant processes and qualified personnel. The MPN is a closed network facilitating information exchange using common protocols and standards. This publication focuses on the expeditionary MPN that enables an expeditionary MPE and provides the capabilities to support deployed forces in the conduct of regionally focused missions.

SECTION II – GENERAL OPERATIONAL CAPABILITIES

1-6. A MPN has general operational capabilities to enable success in a multinational operation. Paragraphs 1-7 through 1-10 discuss these capabilities.

ROBUST NETWORK TRANSMISSION

1-7. A MPN has a robust network transmission capability. It consists of a converged secure voice, data, and video transmission layer comprised of reliable, protected, layered, and secure line of sight and beyond line of sight means in cyberspace and electromagnetic warfare environments.

TACTICAL DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS EXECUTION

1-8. A MPN allows for effective tactical DODIN operations executed by the coalition network operations and security center (CNOSC) and the subordinate network operations and security center (NOSC). It includes the efficient and dynamic allocation of network resources to maximize information exchange.

DISPLAYED AND SHARED RELEVANT INFORMATION

1-9. A MPN enables the receipt and dissemination of essential information to a command post platform for display on the common operational picture (COP). This includes a common geospatial foundation (map set), symbology, graphic control measures, threat information derived from intelligence, operational information, civil considerations, and information on an operational environment.

ENABLED COLLABORATION

1-10. A MPN provides common services that enable multi-forum and real-time collaboration in tactical and operational areas. Multi-forum and real-time collaboration is the ability to exchange operational products, reports, and returns per standard battle rhythm as defined in information management and knowledge management plans. Such collaboration includes the sharing of ideas and situational understanding among commanders and staffs in the form of videos, messages, and shared applications throughout the planning and execution processes.

OPERATIONAL CAPABILITIES FOR MULTINATIONAL INFORMATION EXCHANGE

1-11. A MPN has general operational capabilities for multinational information exchange. Paragraphs 1-12 through 1-15 discuss these capabilities. Appendix B has more on information exchange documentation.

COLLABORATION

1-12. A MPN provides capabilities to support a collaborative information environment with user-to-user, user-to-machine, user-to-virtual, and machine-to-machine interaction in synchronous, asynchronous, concurrent, and emergent mission environments. It also provides the capabilities to assist the supported and supporting staffs in transient and distributed groups with the collaborative management and sharing of information throughout the enterprise.

VISUALIZATION

1-13. A MPN enables all participants to visualize and display data and information that is accurate, timely, and relevant, and to visualize and display data and information that provides situational awareness to support effective decision making.

COMMUNICATIONS

1-14. MPN provides the supporting capabilities to communicate by secure text, speech, voice, and imagery (still and motion) with all MPN partners, superiors, peers, and subordinates. The channels used for these communications capabilities require a combination of synchronous or asynchronous and secure or nonsecure methods that use emergent technology-mediated communications means. For example, these means can include speech recognition and audio-to-text conversions, telephone, radio, television, web and email, text, chat, and video teleconference (VTC).

SYNCHRONIZATION

1-15. Another capability provided by a MPN is a structured, orchestrated joint planning and execution environment. This environment has capabilities to interact, interpret, and smartly adapt the display and information flow of decision-making content (data and information) from all participants with decision support tools.

SECTION III – SPECIFIC CAPABILITIES

1-16. Paragraphs 1-17 through 1-20 provide specific capabilities for a MPN divided into MPN capabilities, cybersecurity capabilities, and information management capabilities.

MISSION PARTNER NETWORK SPECIFIC CAPABILITIES

1-17. Multinational force commanders, subordinate force commanders, and other joint or mission partners require the exchange of information to plan, train, and execute a mission in a collaborative, single security MPN domain.

1-18. A MPN provides the following capabilities:

- An information-sharing environment with appropriate security components to protect mission partners' information.
- Common services to support military operations.
- Classified and unclassified information sharing and data exchange with joint and mission partners via email, web services, file sharing, chat, voice telephony, VTC, and access to a situational awareness visualization capability that is accurate in time and space to include air, ground, and maritime tracks.
- Tested and validated joining, membership, and exiting instructions (JMEI) to participate in the MPN.
- Standardized classification tools for marking email with the appropriate security caveats in accordance with defined mission information sharing agreements.
- Processes or measures for classified releasability defined in the information management and knowledge management plans for information sharing.
- Standardized air, ground, and maritime tracks from national secret networks to the MPN. Sharing track information across networks requires nations to agree to share their information with other nations in accordance with the information management and knowledge management plans and the specifications required.
- An open standards and hardware-independent means to connect to the MPN.
- Access to the mission network transport communications infrastructure to host multiple virtual enclaves simultaneously with ensured control.
- Approved cross-domain solutions to maintain separation between domains of different classifications and to move information across classification boundaries.
- Information management and knowledge management plans with policy and action to move information from one environment to another.

CYBERSECURITY SPECIFIC CAPABILITIES

1-19. A MPN provides cybersecurity capabilities to—

- Protect information, detect and react to intrusions, and restore access to information to include shared data sources.
- Provide role-based access based on a user's task, skills, and other attribute-based control parameters.
- Restore information by incorporating detection and reaction capabilities.
- Securely exchange mission-essential data with mission partners using appropriate security components to protect their national data and resources.
- Deny access to unauthorized persons and nonperson entities by employing approved access control capabilities.
- Access information on the MPN based on the user's identity, clearance, role, and need to share.
- Ensure high availability and disaster recovery within each nation's hosting location.
- Conduct real-time network monitoring, threat identification, access control, event logging, and reporting across the environment.
- Perform data analysis of event logs to correlate any anomalous activity that exceeds network and services' baseline behaviors.

INFORMATION MANAGEMENT SPECIFIC CAPABILITIES

1-20. A MPN provides information management capabilities to—

- Collaboratively manage, assess, monitor, execute, and adjust plans and operational outcomes in an interdependent enterprise services network comprised of joint and mission partner data and information components to achieve integrated mission operations.
- Support commanders' and their staffs' information exchange requirements (IERs) when disconnected from, intermittently connected to, or connected with limited bandwidth to enterprise networks.
- Process, maintain, and deliver real-time data in a tailorable format to provide relevant critical information to support key decision points.
- Work in an environment that accommodates mission partners for a single mission.
- Facilitate multinational information sharing.
- Upload, delete, and archive files in shareable locations.
- Work and collaborate in an environment as defined by information management and knowledge management plans in which data exchange processes are clearly articulated in compliance with the multinational force headquarters cybersecurity governance.
- Access service desk support.
- Establish means and processes for validation and maintenance to ensure standardization of content management for MPN common services and applications information exchange.

Chapter 2

Department of Defense Information Network Operations on the Mission Partner Network

This chapter provides guidance on conducting DODIN operations in a multinational force on the MPN. Section I provides an overview of DODIN operations. Section II describes the CNOSC and subordinate NOSCs. Section III describes the components of DODIN operations in a multinational force on the MPN.

SECTION I – OVERVIEW

2-1. *Department of Defense information network operations* are operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense information network (JP 3-12). DODIN operations are conducted on all Army operated networks to include MPNs supporting expeditionary multinational forces. DODIN operations allow commanders to effectively communicate, collaborate, share, manage, and disseminate information using automated information systems and provide system and network availability, information delivery, and information protection through defensive tools and procedures. DODIN operations allow effective and efficient execution of all warfighting functions, facilitate information superiority, and are required to ensure successful exchanges of information across the MPN. Effective DODIN operations ensure service to the multinational force and facilitate network-enabled information exchange. Corps and division signal officers (G-6) or brigade and battalion signal officers (S-6) and staffs establish, manage, and defend the MPN in support of the operational planning process.

Note. Only U.S. officers have the authority and ability to ensure compliance with DODIN policies and supporting directives within a multinational force connecting to the DODIN.

ORGANIZATION OF DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS ON A MISSION PARTNER NETWORK

2-2. Paragraphs 2-3 through 2-13 discuss the organization and hierarchy of all elements involved in conducting DODIN operations on the MPN. Figure 2-1 on page 2-2 provides a hierarchal view of the DODIN operations organization.

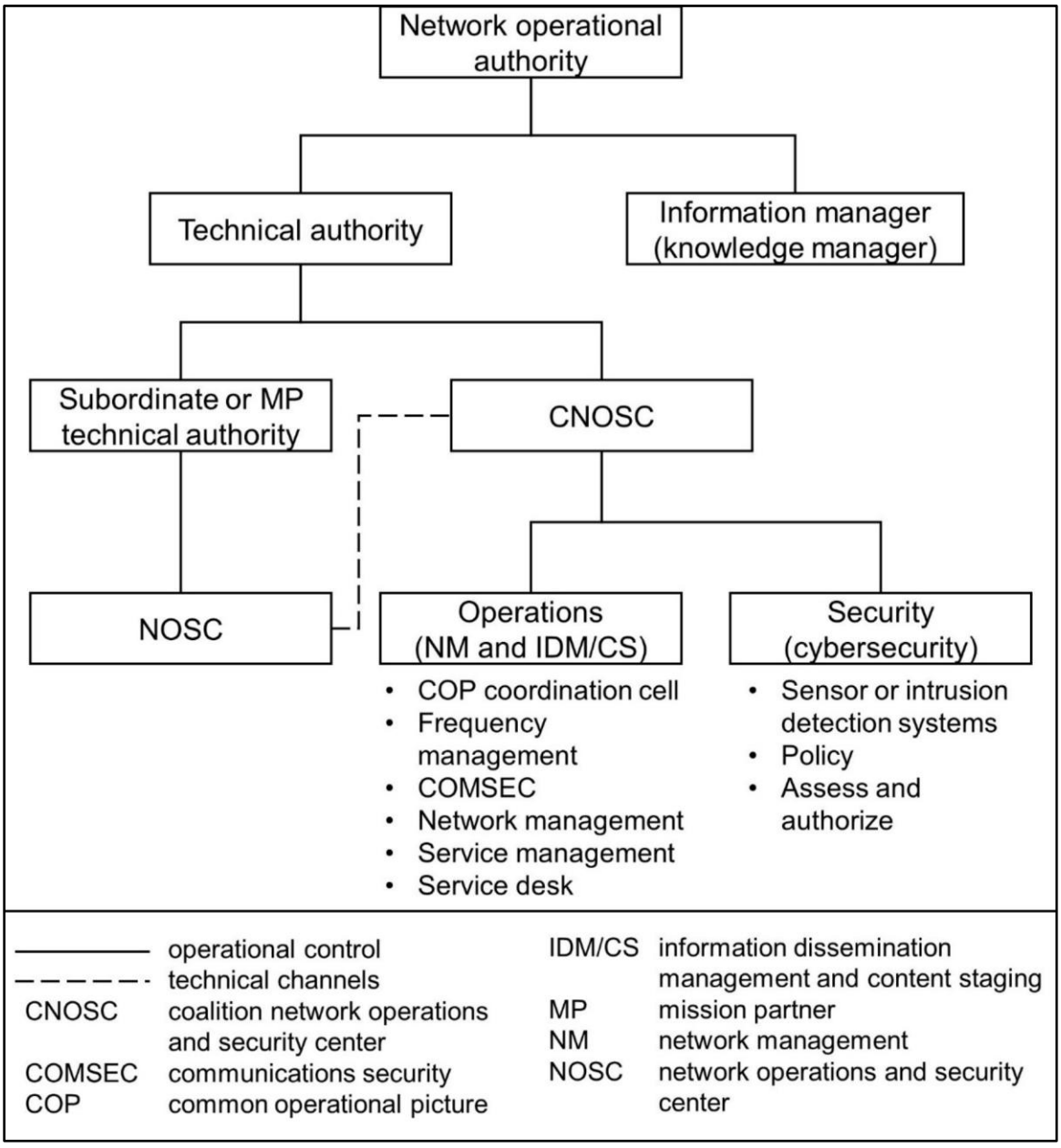

Figure 2-1. Network operations roles

MULTINATIONAL FORCE HEADQUARTERS

2-3. With the United States as lead, a multinational force headquarters with staff sections led by U.S. officers provides the leadership and standards to manage DODIN operations by establishing a CNOSC. The CNOSC is the lead for DODIN operations. It provides standards and policies for operating on the MPN using contributions from units and mission partners. The multinational force commander integrates the multinational force's capabilities in accordance with standards, procedures, and gaps identified by the CNOSC. Connection or integration of subordinate units and other mission partner systems to the MPN is achieved individually against core security policies.

SUBORDINATE UNITS AND OTHER MISSION PARTNERS

2-4. Subordinate units are mission partners, joint units, or Army units task-organized to the corps or division providing the core of the multinational force headquarters. Other participants are the federal, state, and local departments and agencies; tribal governments and agencies; and other organizations that support—but are not directly subordinate to—the corps or division.

2-5. Subordinate units and other mission partners report to the multinational force headquarters for command and control information system planning and integration. After they ensure their network operations capability aligns with the standards and procedures of the CNOSC, these units and mission partners establish their subordinate NOSCs. The subordinate NOSC directly reports to the CNOSC to coordinate network operations. All mission partners have direct responsible for their own network operations equipment and software.

2-6. Mission partners are directly responsible for their national network extensions. A national network extension is the part of the network that an individual nation provides, manages, maintains, and secures within the context of the governing policy and network operations procedures defined by the multinational force.

2-7. The United States and its allies may allow different equipment and software on their networks (for example, the United States bans some manufactures and country-of-origin equipment that other allies permit). In such situations, staffs maintain close coordination to ensure interoperability while minimizing vulnerabilities and protecting the networks.

NETWORK OPERATIONAL AUTHORITY

2-8. The network operational authority is based on the command authority of the responsible commander and is the operational owner of the MPN and its DODIN operations functions. The multinational force commander has overall responsibility for the MPN, but typically the authority is delegated to the multinational force chief of staff to provide oversight for the commander. The network operational authority must be a U.S. officer in a multinational force connected to the DODIN to ensure compliance with DODIN policies and supporting directives.

2-9. The Department of Defense assigns the authorization decision authority to the authorizing official. The Army chief information officer appoints Army authorizing officials. The Network Enterprise Technology Command commanding general is the approval authority for the authority to connect. The authority to connect is granted to mission partner forces wanting to connect to the DODIN-Army, the Army's portion of the DODIN. The U.S. commander of a multinational force coordinates with joint force commanders who support Cyber Command for authority to connect and authority to operate an expeditionary MPN established on portions of the DODIN other than the DODIN-Army.

TECHNICAL AUTHORITY

2-10. The technical authority is vested in the multinational force G-6 by the network operational authority for operating and managing the MPN and its inherent DODIN operations functions. The technical authority is responsible for technical advice, setting specifications and standards, managing configurations, and ensuring compliance with published standards. The technical authority must be a U.S. officer in a multinational force connected to the DODIN to ensure compliance with DODIN policies and supporting directives.

PROGRAM INFORMATION SYSTEMS SECURITY MANAGER

2-11. The program information systems security manager (P-ISSM) supports the technical authority. The P-ISSM establishes the security authorization board and manages the policies, procedures, and processes that govern and monitor the MPN regulatory, legal, environmental, and operational cybersecurity risks. The P-ISSM typically is located at the CNOSC and is responsible for cybersecurity, identifying vulnerabilities, providing advice and standards on the security aspects of a system, and monitoring compliance to those standards.

INFORMATION MANAGEMENT AND KNOWLEDGE MANAGEMENT OFFICER

2-12. The information management officer and knowledge management officer work for the multinational force chief of staff. Multinational information and knowledge management planning is conducted during multinational operations planning as a key enabler to a multinational force commander's situational understanding. Refer to JP 3-33 for more on information management and knowledge management officers.

COALITION NETWORK OPERATIONS AND SECURITY CENTER

2-13. The composition of the CNOSC is determined by the multinational force commander. Its manning and equipping varies and is influenced by operational environments, doctrine, and manning constraints inherent in all operations. It is essential that the CNOSC has sufficient manning to fulfill the roles and responsibilities outlined. Subordinates may provide embedded officers and Soldiers in the CNOSC to help with coordination to subordinate NOSCs.

ROLES AND RESPONSIBILITIES OF DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS ON A MISSION PARTNER NETWORK

2-14. Paragraphs 2-15 through 2-17 identify the organization and agencies with DODIN operations roles and responsibilities that ensure connectivity of network and information system users throughout the MPN. The DODIN operations roles discussed in this chapter are the multinational force commander, the G-6 or S-6, and subordinate unit and mission partner signal officers. Figure 2-2 illustrates the organizational technical channel relationships.

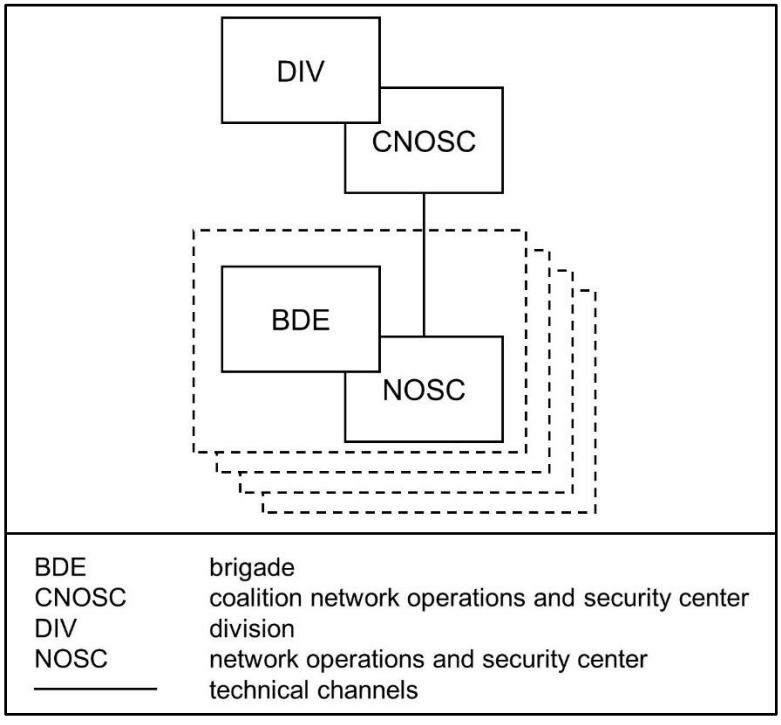

Figure 2-2. Mission partner network relationships

COMMANDER, MULTINATIONAL FORCE

2-15. The multinational force commander is the network operational authority. This officer is responsible for the network. The multinational force commander—

- Ensures compliance with related DODIN operations policies and supporting directives.
- Assesses the effectiveness and efficiency of managing information throughout its lifecycle and continuously works to improve the organization's DODIN operations capabilities.
- Implements organizational, governance, and accountability structures, and ensures the implementation of DODIN operations.
- Allocates appropriate resources in the organization to support implementing DODIN operations.
- Appoints a technical authority who reports directly to the network operational authority and is responsible for ensuring the implementation of all matters concerning DODIN operations.
- Provides IER guidance and direction for developing information management and knowledge management plans used to initiate DODIN operations planning.

MULTINATIONAL FORCE ASSISTANT CHIEF OF STAFF, SIGNAL

2-16. The multinational force G-6 is the technical authority for both the multinational force and subordinates. This signal officer is responsible for matters related to DODIN operations. The multinational force G-6—

- Advises the commander on network operational authority responsibilities and executes the network operational authority activities.
- Establishes the technical control chain.
- Executes DODIN operations by integrating network management, cybersecurity and information dissemination management, and content staging into a core MPN operational capability.
- Establishes DODIN operations through the CNOSC.
- Establishes and chairs the network change advisory board.
- Establishes network ownership boundaries and responsibilities.
- Ensures compliance with related DODIN operations policies and supporting directives.
- Operates and defends the MPN.
- Advises the network operational authority on all network matters.
- Applies allocated resources to meet the commander's requirements.
- Develops and manages the DODIN operations plan.
- Develops and manages the JMEI.
- Establishes spectrum management operations (SMO) procedures.
- Manages communications security (COMSEC) materials.
- Provides G-6 input to operational planning.
- Coordinates subordinate contributions to the MPN.
- Issues instructions.
- Coordinates for the multinational force headquarters, subordinate units, and other joint and mission partners "authority to operate" to authorize the MPN.
- Appoints a P-ISSM.
- Establish satellite communications (SATCOM) operations and planning procedures.

SUBORDINATE UNITS AND OTHER MISSION PARTNER ASSISTANT CHIEF OF STAFF, SIGNAL AND SIGNAL OFFICER

2-17. Subordinate unit G-6s and S-6s are the technical authority for network extensions and integrating into the MPN. Subordinate unit G-6s and S-6s—

- Execute network operations by integrating network management operations, cybersecurity, and information dissemination management and content staging into a core MPN operational capability.
- Comply with the CNOSC DODIN operations standards and policies.
- Establish individual unit NOSCs.
- Participate in the network change advisory board.
- Comply with network ownership boundaries and responsibilities.

- Operate and defend the MPN.
- Advise the multinational force technical authority on all network matters.
- Comply with the DODIN operations plan.
- Manage common COMSEC materials.
- Provide input to operational planning.
- Implement CNOSC instructions.
- Maintain the national network extension.
- Conduct SMO.
- Conduct SATCOM management.

SECTION II – COALITION NETWORK OPERATIONS AND SECURITY CENTER AND SUBORDINATE NETWORK OPERATIONS AND SECURITY CENTERS

2-18. Paragraphs 2-19 through 2-23 discuss the organization, roles, and responsibilities for a CNOSC and subordinate NOSCs. See Appendix A for more information on communications in coalition operations.

COALITION NETWORK OPERATIONS AND SECURITY CENTER

2-19. The CNOSC is the central DODIN operations authority for the MPN. The CNOSC provides network management, information dissemination management and content staging, and cybersecurity for the MPN, as well as ensuring quality of service. It may have the same responsibilities for the corps or division headquarters network extension. Figure 2-3 provides a CNOSC capability example. Figure 2-4 on page 2-8 provides a CNOSC organization and manning example.

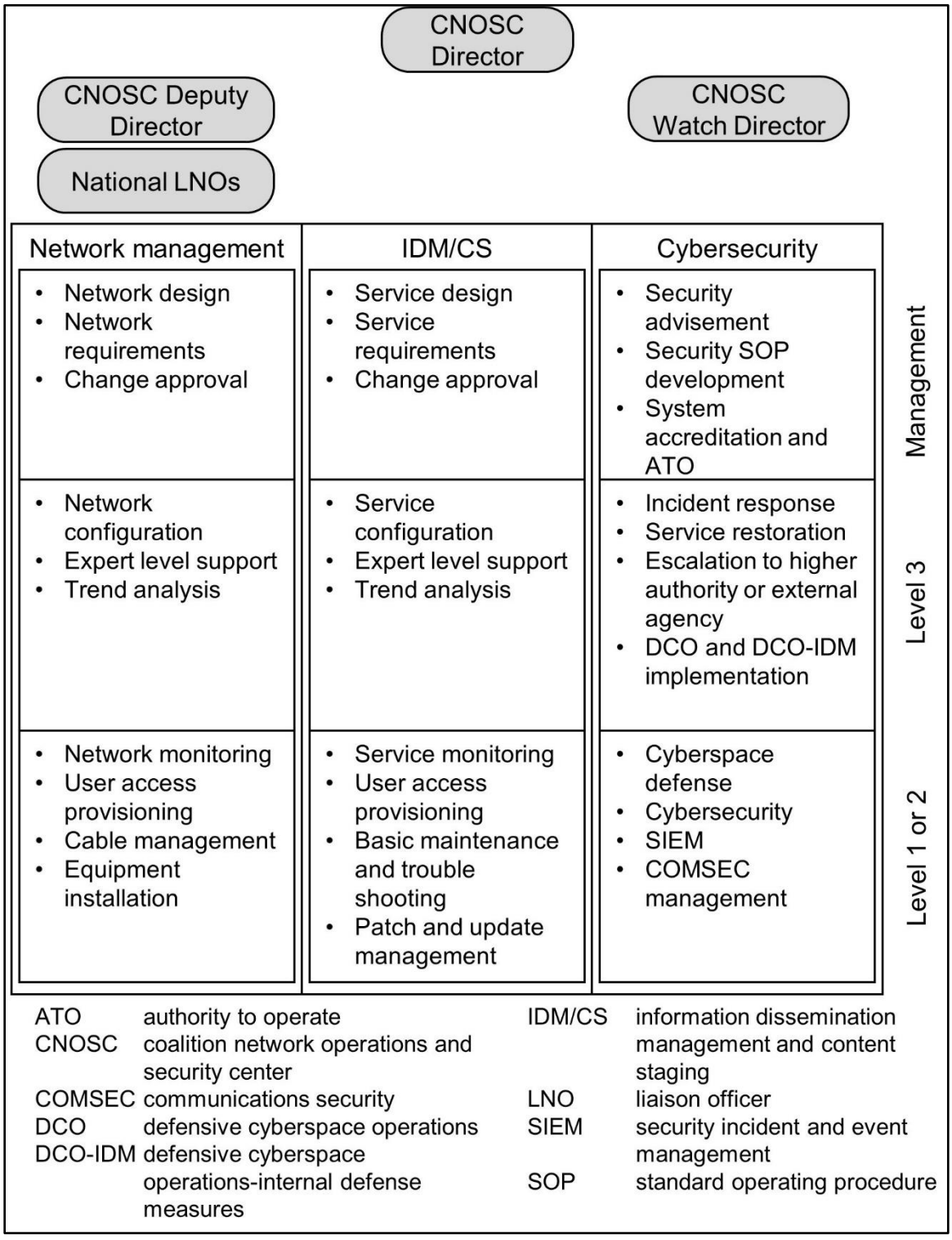

Figure 2-3. Coalition network operations and security center capability example

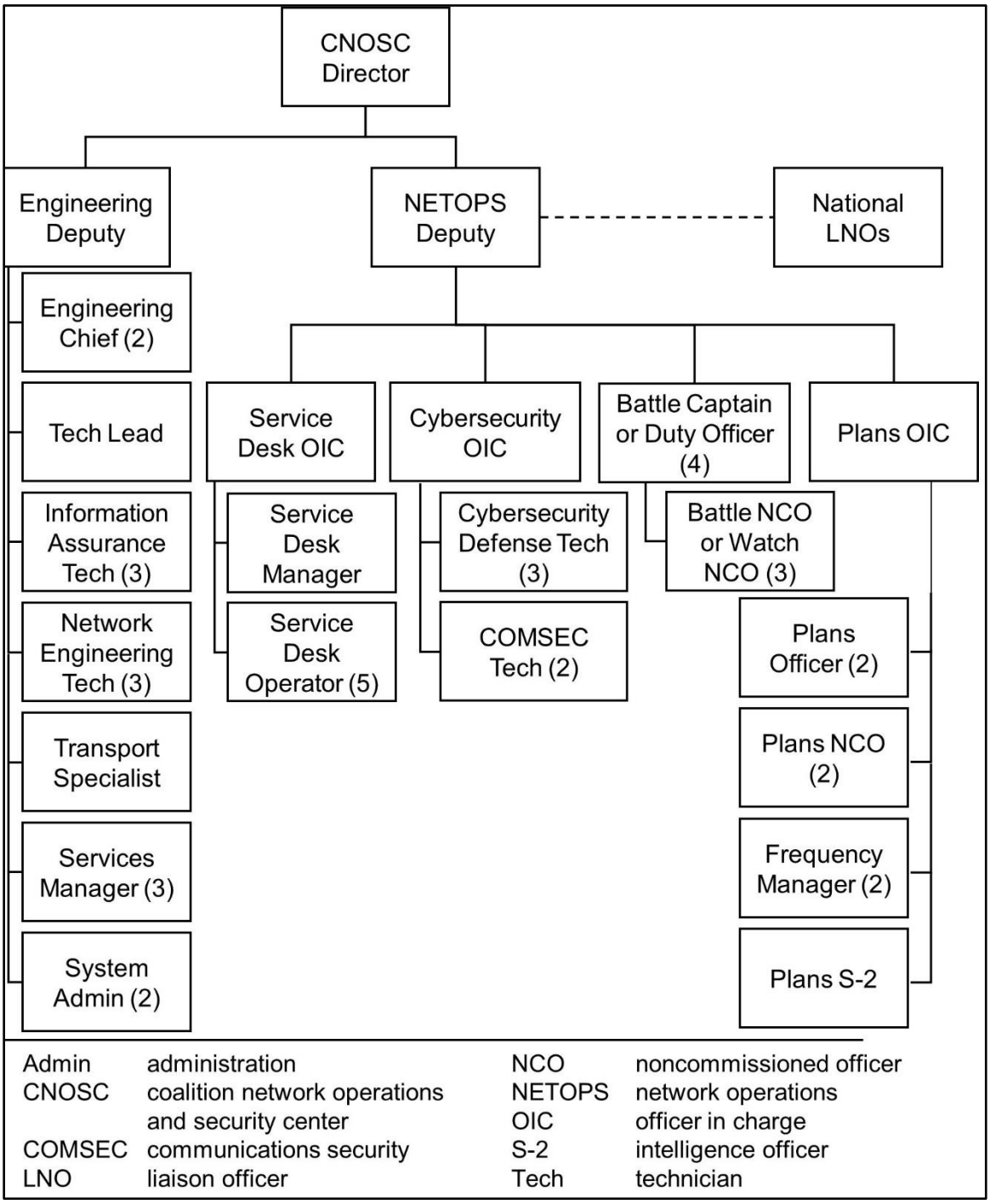

Figure 2-4. Coalition network operations and security center organization and manning example

2-20. The multinational force commander, usually either at corps or division, provides a CNOSC with staff contributions from subordinate units and other mission partners as part of the technical control hierarchy. The CNOSC is functionally located at the multinational force headquarters, is responsible for the day-to-day operation and management of the network on behalf of the multinational force G-6, and provides direct support to the multinational force headquarters. Each subordinate unit and other mission partners provide a

NOSC for management of their portion of the network. Each mission partner NOSC also manages its national extensions. The responsibilities of the CNOSC include the following:

- Conduct initial configuration of the network.
- Develop and maintain a network situational awareness view.
- Manage the network and common services.
- Operate a multinational force headquarters service desk.
- Establish a trouble-ticketing system, manage incidents, conduct first-line systems administration, and conduct user help and troubleshooting to manage escalated network issues from subordinate unit network operations centers.
- Lead the change advisory board and implement changes in accordance with change advisory board outcomes.
- Report and escalate network outages to the appropriate agency while maintaining ownership of the incident until full resolution.
- Monitor overall network performance.
- Apply information systems security standards for network information, access, transmission, storage, and processing.
- Implement network priorities as determined by the network operational authority and technical authority.
- Establish and monitor security by applying standards in accordance with applicable regulations.
- Implement recovery and restoration plans.
- Establish COMSEC management procedures.
- Conduct electromagnetic SMO.
- Stipulate roles required for subordinate unit embeds and augmenters.
- Integrate service providers, embeds, and liaison officers as required.
- Develop incident response policies and procedures.
- Develop and execute the MPN activities for the continuity of the operation plan.
- Coordinate planned MPN outages with subordinate NOSC.
- Establish a security authorization board.
- Establish certificate management authority.
- Establish defensive cyberspace operations.
- Manage SATCOM networks for the multinational force headquarters and subordinate units.

2-21. Subordinate units and other mission partners provide liaison officers (LNOs) to help coordinate, synchronize, and plan DODIN operations on the MPN. LNOs require the experience and skills to speak on behalf of their parent commander or director and represent multinational force headquarters actions to their parent NOSC to ensure clarity and understanding. LNOs may require a foreign language capability when working with mission partners.

SUBORDINATE UNIT NETWORK OPERATIONS AND SECURITY CENTER

2-22. Subordinate units are responsible for establishing a NOSC and for implementing connectivity to the MPN in accordance with configurations directed by the CNOSC. The subordinate unit may provide a liaison to the CNOSC for initial coordination as required.

2-23. Subordinate NOSCs are responsible for day-to-day operations, managing their portion of the MPN, and providing direct support to its subordinate entities. Mission partners are responsible for their national network extension. The roles and responsibilities for subordinate NOSC include the following:

- Report network status to the CNOSC.
- Maintain a network situational awareness view.
- Manage the network and services that host the voice, data, and video networks.

- Operate a service desk for the subordinate entities to include managing escalated network issues by managing incidents, conducting first-line systems administration, and conducting user help and troubleshooting.
- Participate in the change advisory board and implement changes in accordance with change advisory board outcomes.
- Manage and maintain the approved configuration of the network.
- Report and escalate network and circuit outages to the appropriate service provider based on the G-6 critical information requirements.
- Monitor overall network performance.
- Apply information systems security standards for network information, access, transmission, storage, and processing.
- Implement network priorities.
- Record and process information gathered from DODIN operations systems that monitor the operation and security of the network, and collect and report DODIN operations statistics, such as bandwidth usage, error rates, and equipment failure rates for trend analysis and higher echelons.
- Establish and monitor security by applying security standards in accordance with applicable regulations and standards.
- Implement recovery and restoration plans.
- Establish patch management procedures.
- Establish COMSEC management procedures.
- Conduct electromagnetic SMO.
- Integrate embeds and augmentation staff service providers and LNOs.
- Conduct SATCOM management.

SECTION III – DEPARTMENT OF DEFENSE INFORMATION NETWORK OPERATIONS ON A MISSION PARTNER NETWORK

2-24. DODIN operations are the critical fusion point in a multinational force command post, combining infrastructure and services which provide processing, storing, and transporting information across the network. The functional areas that comprise this infrastructure and services consist of the wide area network (WAN) and local area network management, command and control information systems, cybersecurity, COMSEC, and SMO. All these areas are interrelated. They cannot be viewed and operated as a single national planning factor but are required to be viewed from a multinational force approach. Forces conduct these operations at all levels, and commanders must synchronize them both horizontally and vertically between echelons.

2-25. DODIN operations are an integrated construct of three critical components: network management, information dissemination management and content staging, and cybersecurity. DODIN operations guide the installation, management, and protection of communications networks and information services necessary to support operations. Figure 2-5 shows the construct of DODIN operations for the MPN.

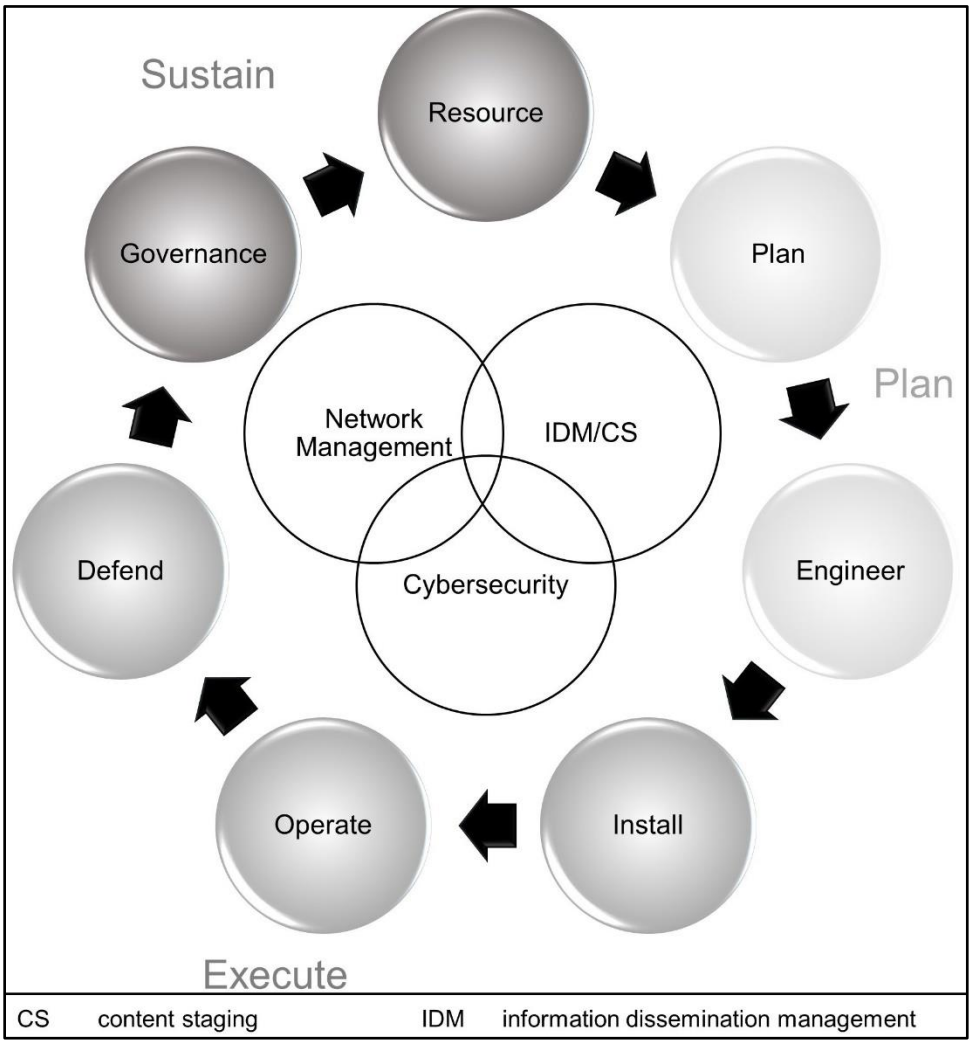

Figure 2-5. Department of Defense information network operations components on a mission partner network.

2-26. DODIN operations provide the means to operate and defend MPN services and applications to allow the effective and efficient execution of all warfighting functions and facilitate information superiority. This allows for better user and system support by—

- Having a detailed understanding of the user's IERs provided by the information and knowledge management staff.
- Identifying the communications network and information service resources.
- Coordinating hardware and software interoperability planning using JMEI to fulfill user and system information exchanges.
- Protecting the confidentiality, integrity, and availability of information and information systems.
- Designing, establishing, and operating the network to support and enable the information management and knowledge management plans to flow and process so the right information is disseminated to the right place, at the right time, and in the right format.
- Ensuring the efficient use of resources.

2-27. The CNOSC and subordinate NOSCs maintain technical control and operational management of DODIN operations. Figure 2-6 details the tier management and reporting functions of DODIN operations

associated with network management, information dissemination management and content staging, and cybersecurity. Reporting is conducted per corps or division standard operating procedures (SOPs).

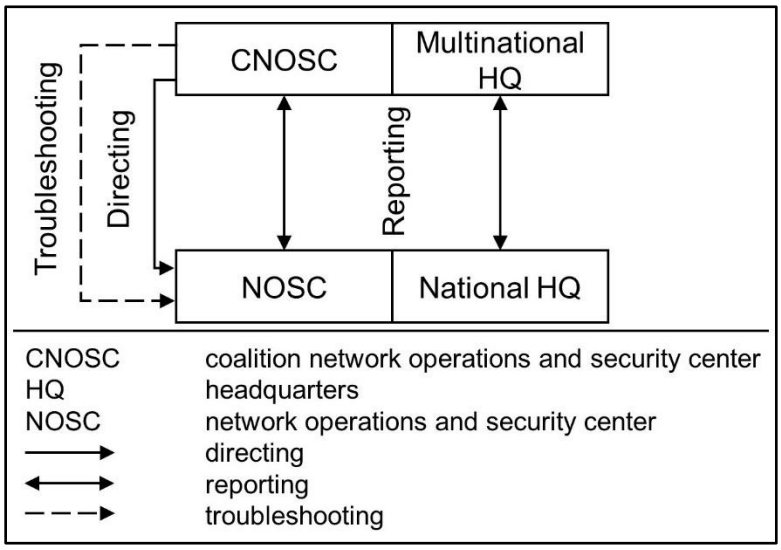

Figure 2-6. Department of Defense information network operations management and reporting on a mission partner network

2-28. DODIN operations components have the following characteristics:

- Core functions drive the delivery of internal capabilities to accomplish the DODIN operations components.
- Critical capabilities are the management tasks applied to each of the core functions.
- Enabled effects are the outcomes of applying the critical capabilities to achieve DODIN operations.

NETWORK MANAGEMENT COMPONENT

2-29. The network management component consists of the technologies, processes, and policies necessary to plan, execute, and sustain communications networks effectively and efficiently. This component uses four core functions, integrates three critical capabilities, and creates staging effects.

CORE FUNCTIONS

2-30. NOSC employs four major functions within network management that foster the planning, engineering, installation, operation, and management of communications networks and information services. More information for each of these core functions is given in paragraphs 2-31 through 2-34.

Common Services Management

2-31. Common services management focuses on the accessibility, availability, performance, and responsiveness of common services capabilities of systems applications for end users.

Systems Management

2-32. Systems management provides day-to-day management of information systems and services to include software applications, operating systems, databases, and host-end users. It comprises all the measures necessary to ensure effective and efficient operations of systems and services.

Network Management

2-33. Network management ensures the functionality and performance of the network infrastructure with the desired level of services.

Spectrum Management Operations

2-34. *Spectrum management operations* are the interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations (FM 6-02). Refer to FM 6-02 for more information on SMO.

CRITICAL CAPABILITIES

2-35. Network management involves several DODIN operations critical capabilities associated with information technology services. Signal staffs achieve the critical capabilities for network management (fault management, configuration management, and performance management) at the strategic, operational, and tactical levels across all warfighting functions. More information for each of these critical capabilities is given in paragraphs 2-36 through 2-38.

Fault Management

2-36. Fault management includes incident management and problem management and is associated with failure of the network or information systems, which impact connectivity and functionality. Fault management involves a five-step process of detecting faults, locating faults, restoring services, identifying the root cause of the fault, and establishing solutions so that similar faults do not occur in the future.

Configuration Management

2-37. Configuration management is used to discover specific network and information system architecture requirements and then develop configuration parameters. The parameters guide the provision, deployment, and management of hardware and software resources.

Performance Management

2-38. Performance management is the monitoring and management of parameters related to networks and information systems. It involves data monitoring, problem isolation, performance tuning, and analysis of statistical data for recognizing trends, resource planning, and proactive management of network performance.

STAGING EFFECTS

2-39. Network management enables network and information system availability and information delivery. These staging effects are achieved by—

- Maintaining robust network capabilities in the face of component or system failure or adversary attack.
- Configuring and allocating network and information system resources.
- Rapidly and flexibly deploying network resources.
- Ensuring effective, efficient, and prompt processing.
- Ensuring connectivity, routing, and information flow.
- Planning for increased network use.

INFORMATION DISSEMINATION MANAGEMENT AND CONTENT STAGING COMPONENT

2-40. Information dissemination management and content staging consists of managing access to, and delivery of, relevant, accurate information to the appropriate users promptly, efficiently, and in the proper format. This component allows the CNOSC to optimize the flow and location of information over the MPN

by positioning and repositioning data and services to optimum locations on the MPN relative to the information producers, consumers, and mission requirements.

CORE FUNCTIONS

2-41. The core functions of information dissemination management and content staging are employed at the strategic, operational, and tactical levels. The information dissemination management and content staging core functions are—

- Messaging. Enables networked information exchange among users and systems.
- Discovery. Helps users discover content or services by exploiting unique descriptions stored in directories, registries, and catalogs.
- Mediation. Enables system interoperability by processing data to translate, combine, fuse, or integrate it with other data.
- Collaboration. Allows users to work together in collaborative portals and chat rooms.
- Storage. Provides physical and virtual data hosting with varying degrees of persistence.
- User assistance. Provides centralized service desk assistance and automated access to lessons and best practices, which may improve processes or reduce the effort required to perform tasks.

CRITICAL CAPABILITIES

2-42. The critical capabilities for information dissemination management and content staging must be achieved at the strategic, operational, and tactical levels across all warfighting functions. These capabilities are—

- Collection of information. Acquiring data based on information requirements.
- Processing of information. Translating data from one form to another.
- Storage of information. Recording information to any storage medium on the network.
- Transmission of information. Conveying information from one place to another based on prescribed information flow.
- Display of information. Visually presenting collected information, data, or knowledge.
- Dissemination of information. Using automation to ensure timely collection, processing, and transmission of information to the right user.

STAGING EFFECTS

2-43. Information dissemination management and content staging enables effects by—

- Retrieving critical information that directly contributes to situational understanding, collaboration, and decision making from systems in the MPN.
- Compiling retrieved information for processing and storage until needed.
- Caching compiled information in secure systems according to applicable regulations and policies.
- Cataloging cached information to facilitate future search and discovery.
- Distributing critical information to develop situational understanding, collaborate, or execute decisions.

CYBERSECURITY COMPONENT

2-44. The cybersecurity role in DODIN operations provides end-to-end, defense-in-depth protection of the network that ensures data confidentiality, integrity, availability, and impact. DODIN operations cybersecurity incorporates those actions taken to protect the network and prevent, identify, recover, and respond to unauthorized activity. These actions include proactive cyberspace security actions which address vulnerabilities of the MPN. With respect to cyberspace operations, DODIN operations are network focused and threat agnostic; the workforce undertaking this mission endeavors to prevent all threats from negatively impacting the network or system they are assigned to protect.

2-45. Cybersecurity considers both technical and nontechnical measures. Cybersecurity staff is responsible for developing policies and procedures for incidents that occur through malicious and accidental activity by enemy or friendly entities.

2-46. Cybersecurity is enabled by—

- Evaluating subordinate units' security readiness and vulnerability for compliance with communications instructions and reporting compliance to higher echelons.
- Ensuring network management and defense training, awareness, and certification program compliance according to established policies and directives.
- Developing and deconflicting local contingency plans to defend against malicious activity and providing copies to higher level commands.
- Conducting network risk assessments.
- Incorporating intelligence to identify risks and vulnerabilities aligned with an adversary's offensive cyberspace capabilities.
- Sharing cybersecurity according to formal agreements and national disclosure policies.
- Reconstituting capabilities from reserve or reallocated assets when original capabilities are destroyed.

2-47. Cybersecurity enables information protection and network and system availability by—

- Instituting agile capabilities to resist adversary attacks by recognizing such attacks as they begin or progress.
- Detecting and analyzing anomalies or intrusions and reporting incidents to the CNOSC and subordinate NOSCs.
- Implementing efficient, effective responses to reduce the effects of an attack and to recover from attacks safely and securely.
- Informing others across the MPN of local actions to counter intrusions or correct other incidents.
- Certifying, accrediting, and reporting on all networks, peripherals, and edge devices in their portion of the network, and enforcing cybersecurity controls.
- Submitting reports.
- Coordinating among user elements to distinguish between hostile cybersecurity incidents and other system outages or degradations.

This page intentionally left blank.

Chapter 3
Network Management

This chapter provides guidance on executing network management activities, functions, and tasks on the MPN.

NETWORK PURPOSE

3-1. Network management provides control for the operation of the MPN. The multinational force headquarters, subordinate units, and other joint and mission partners' network managers perform network management within the multinational force task organization, with the multinational force headquarters directing the allocation of responsibilities among organizations. Specific functions and tasks may vary depending on the mission and capabilities of the organization. Network managers perform a common set of activities for effective and efficient network management: planning, engineering, and service management.

NETWORK PLANNING

3-2. Planners must read and understand doctrine on MPN. This doctrine includes this publication and its partner publication, ATP 6-02.62, *Expeditionary Mission Partner Network Techniques for Joining, Membership and Exiting Instructions*. ATP 6-02.62 establishes the processes for the multinational force's headquarters, subordinate units, and other mission partners to conduct network management on the MPN in support of multinational force interoperability planning and execution. Conducting network management includes the joining, membership, and exiting instruction processes and configuration required of units and mission partners when connecting to the MPN at a single security classification level.

3-3. Normal network planning for a single deploying force into an operational environment is challenging enough. Continuous technical upgrades, demanding user requirements, technological limits, resource caps, hostile threats, and austere environments impose ever-present constraints on planners. Multinational force planners have an added set of facts to address when considering how communications affect units and mission partners such as technological disparity, technical interoperability, procedural dissimilarities, language differences, security concerns, resourcing limitations, and command and control issues.

3-4. As the core of the multinational force headquarters, the corps or division provides its own national force and rear-link communications. The MPN provides the core network through which the corps or division and its mission partners connect to share information. Multinational operations planning for the MPN includes planning the multinational force headquarters down to the brigade to battalions.

3-5. The signal sections use the network planning activity to assess information management plans, knowledge management plans, and user requirements to develop the schedule and resources to meet these requirements. The goal of network planning is to ensure the network meets the commander's requirements. Network planning activities involve—

- Capacity planning.
- Identifying network capabilities available.
- Architecture development, system planning, interoperability planning, and security planning.
- Boundary planning.
- Spectrum planning.
- Contingency and restoration planning.
- SATCOM management.
- The development and publication of JMEI and supporting plans.
- Test and validation, communication exercises, and rehearsals as time permits.

See Appendix A for additional network planning considerations.

3-6. The basis of multinational operations is the exchange of information in the form of products, reports, and returns. Appendix B provides the high priority IERs expected between command posts to develop the architecture database.

NETWORK ENGINEERING

3-7. The multinational force G-6 plans the network, and the CNOSC executes network engineering. The network engineering activity tailors network and information system resources to meet requirements. Network engineering is required from the highest headquarters down to the user. Network engineering activities involve—

- Technical documentation.
- Building the MPN.
- Testing the MPN.
- Authorizing the MPN by integrating subordinate units and other joint and mission partners' authorizations.
- Deploying, sustaining, and recovering the MPN.

3-8. Network engineering starts prior to deployment through a persistent test environment and by using a standardized test plan. The test plan development and execution are a function of the CNOSC.

SERVICE MANAGEMENT

3-9. Information technology service management refers to the end-to-end delivery of information technology services to information technology system users. Information technology service management identifies the processes and activities required to design, build, deliver, and support information technology systems. ITIL®, one accepted approach in the Army, is considered an information technology service management best practice, and is used by many mission partners. Implementing ITIL® in the CNOSC and subordinate NOSCs work well to manage information technology service management.

Note. Providing information on ITIL® does not constitute the Army's endorsement of the product.

SERVICE OPERATION

3-10. Service operation seeks to meet the user's needs through a prioritized and coordinated approach to managing requests, incidents, and problems. Service operation consists of the following processes: event management, incident management, request fulfillment, access management, problem management, and information technology operations management. Service operation also has the functions of service desk, application management, and technical management.

3-11. The CNOSC and subordinate NOSCs are responsible for the performance of service operation processes and functions at their respective headquarters. Hardware and software tools required to undertake the service operation processes and functions are the responsibility of the unit providing the respective CNOSC or subordinate NOSC. Appendix D provides additional information on how the service desk function applies specifically to the MPN, CNOSC, and subordinate NOSCs.

SERVICE DESIGN

3-12. Service design understands the interactions among people, processes, products, and partners necessary to design changes to the system and prepare these changes for introduction into an operational environment. Given an operational environment of the MPN, service design practitioners always remain cognizant of the operational imperative behind proposed changes. Service design includes the following processes: service catalog management, service-level management, availability management, capacity management, service continuity management, information technology security management, and supplier management.

SERVICE TRANSITION

3-13. Service transition describes the processes required to build, deploy, and continually implement improvements in a coordinated way. Service transition includes the following processes: change management, change evaluation, transition planning and support, release and deployment management, service validation and testing, service assessment, configuration management, and knowledge management. Appendix C provides additional information on how the change management process applies specifically to the MPN and CNOSC.

SERVICE STRATEGY

3-14. Service strategy determines which services will be available to which units and staff sections. The principles of service strategy address the issues pertaining to corporate governance and compliance, business processes, policies, decision making, corporate culture, and service improvement. Service strategy consists of the following processes: service portfolio management, demand management, financial management, and strategy operations.

CONTINUOUS IMPROVEMENT

3-15. Continuous improvement employs a quality management approach, so commanders learn from past successes or failures. Continuous improvement seeks to improve the effectiveness and efficiency of information technology processes and services. Continuous improvement is a single process consisting of multiple steps.

QUALITY OF SERVICE

3-16. The MPN consists of various network portions and systems with variable bandwidths and application demands. The network topology, link capacity, packet loss rate, and end-to-end latency varies dramatically as link conditions change due to node movement, environmental conditions, and jamming. In addition, the demand placed on the network also varies significantly and unpredictably during operations. These conditions create the significant need to prioritize and ensure delivery of essential traffic across the entire MPN.

3-17. Quality of service deals with these conditions by enabling the effective use of constrained bandwidth to accomplish the most important and valuable missions at the expense of less critical objectives or information flows. This includes adopting quality of service policies that adjust for mission priorities.

3-18. Accomplishing quality of service objectives of an overall mission require involvement from all layers of the system—from domain application services to resource managers who control and schedule access to physical resources.

3-19. The MPN quality of service framework and mechanisms have the following characteristics:

- Integrated into the architecture, not an add-on.
- Optimized to achieve the most mission value.
- Flexible, adaptive, mission needs-based rules for categorizing priorities and allocating resources.
- Resource management based on mission value and deadlines, not best effort.
- Proactive, not reactive, congestion avoidance, control, and management.
- Consistent and configurable quality of service policy and implementation across the MPN.

3-20. Quality of service policies and mechanisms are part of the underlying software, clients, and network devices to support all MPN participants. The quality of service capabilities—

- Support differential service code point mapping to prioritize types of traffic.
- Include consistent forwarding behavior of quality of service traffic across the MPN to include the radios and waveforms.
- Enforce rate limiting based upon mission needs and congestion status.

3-21. Each MPN participant engineers and aligns its network architecture according to the quality of service requirements directed in the Annex H (Signal) and Annex Q (Knowledge Management) to the operation order to achieve interoperability across the MPN. Figure 3-1 illustrates a network quality of service system.

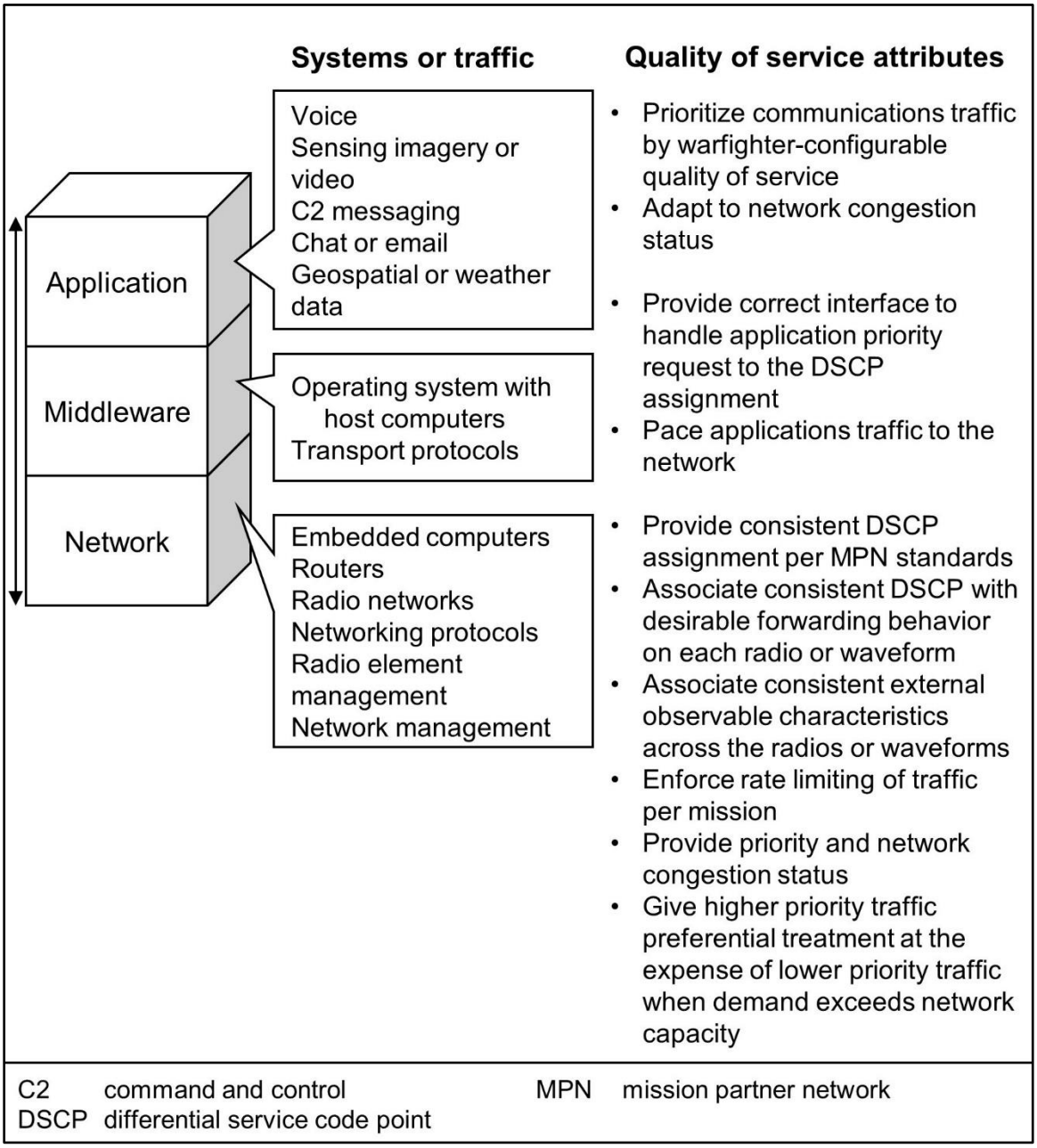

Figure 3-1. Network quality of service

Chapter 4

Information Dissemination Management and Content Staging

This chapter provides guidance on executing information dissemination management and content staging activities, functions, and tasks on the MPN.

INTRODUCTION TO INFORMATION DISSEMINATION MANAGEMENT AND CONTENT STAGING

4-1. Managing and protecting the MPN for users does not ensure the multinational force receives relevant information. Information dissemination management and content staging is the DODIN operations component that manages access to, and delivery of, relevant, accurate information to the appropriate users promptly, efficiently, and in the proper format. DODIN operations support information management and knowledge management functions.

4-2. Information dissemination management allows the CNOSC and subordinate NOSCs to optimize the flow and location of information over the MPN. Dissemination management does this by positioning and repositioning data and services to optimum locations on the MPN relative to the information producers, consumers, and mission requirements. Placing the content on servers closer to the end users reduces demands on limited network transport bandwidth. Information dissemination management and content staging objectives include the following:

- Enabling the multinational force commander to adjust information delivery methods and priorities for enhanced situational understanding.
- Enabling information producers to advertise, publish, and distribute information.
- Allowing users to define and set information needs to facilitate prompt, efficient information delivery.
- Allowing users to search information databases to retrieve desired products as needed.
- Improving bandwidth utilization.
- Enhancing network transport capabilities by storing data as close as possible to the point of use to reduce bandwidth requirements per plans for multinational force information management and knowledge management.

4-3. Information dissemination management and content staging seeks to get the right information to the right place at the right time in a usable format. It uses specific processes, services, and applications to deliver this information. It provides awareness of the following:

- Relevant, accurate information.
- Automated access to new or recurring information.
- Prompt, efficient information delivery based on the commander’s priorities.

4-4. Information dissemination management and content staging delivers video, voice, and data products to the multinational force efficiently and ensures the multinational force knows these products are available. It uses a distribution system to integrate delivery and user notification. Information dissemination management and content staging allows users to—

- Define the types of data, information, and information products they need and have them delivered as requested.
- Access data from various information systems.

- Retrieve relevant, accurate data and information to develop and maintain situational understanding.

4-5. Information dissemination management and content staging provides services used across the MPN to ensure information is available to all authorized users. Information dissemination management and content staging provides three core services. These services are—

- Content discovery that provides the ability to quickly search for information throughout the MPN.
- Content delivery that allows users to replicate files and directories as well as publish and subscribe to information based on their roles and responsibilities. It provides timely, ensured information transport.
- Content storage that provides physical and virtual data storage locations on the network with varying degrees of persistence.

INFORMATION DISSEMINATION MANAGEMENT AND CONTENT STAGING ACTIVITIES

4-6. To improve understanding, information dissemination management and content staging delivers relevant data and information by any means from one person or place to another in a usable form. Information dissemination management and content staging activities use a judicious combination of dissemination methods as directed in the information management and knowledge management plans and by the staff needs of the headquarters.

4-7. CNOSC personnel ensure the software-based information dissemination management and content staging capability directs a producer-to-user information flow throughout the MPN and across all echelons. These personnel also ensure the basic functions of information dissemination management and content staging are instituted. CNOSC planners ensure services—

- Enable users to electronically see and find available information throughout the network and identify what previously acquired information has changed.
- Require producers to publish or register with the network descriptions of their information products and any access restrictions they apply.
- Enable users to access information they need automatically without having to know its location.
- Optimize the network’s transport capabilities by managing information transmission by established priority.
- Provide information on an automatic basis under a user-profile management scheme and on a request basis under an individual query scheme.

Chapter 5
Cybersecurity

This chapter provides guidance on executing cybersecurity activities, functions, and tasks on the MPN.

INTRODUCTION TO CYBERSECURITY

5-1. As a multinational force headquarters, the corps or division relies on DODIN operations, defensive cyberspace operations, cybersecurity, and, at times, offensive cyberspace operations for freedom of maneuver to employ a network capability. Cybersecurity and defensive cyberspace operations protect and defend the MPN, thereby maintaining communications and command and control. Current intrusion information may lead to future defensive cyberspace operations response action or offensive cyberspace operations missions. Defensive cyberspace operations and offensive cyberspace operations depend on the MPN for planning, synchronizing, and integrating missions. Figure 5-1 on page 5-2 illustrates the core activities of cyberspace operations in the MPN.

MISSION PARTNER NETWORK CYBERSPACE ACTIONS AND MISSIONS

5-2. The multinational force uses a defense-in-depth concept incorporating a layered approach to defend the network. It incorporates both cyberspace actions and cyberspace missions to defend the network. Cyberspace operations external to the MPN are outside the scope of this publication.

CYBERSPACE ACTIONS

5-3. Cyberspace actions conducted internal to the MPN are cyberspace defense and cybersecurity. Cyberspace offense operations are under the authority of the President of the United States and are beyond the scope of MPN operations and this publication.

Cyberspace Defense Actions

5-4. Cyberspace defense actions are normally taken within the multinational force cyberspace for securing, operating, and defending the MPN against specific threats. The purpose of cyberspace defense includes identification of, protection from, detection of, response to, and recovery from cyber threats and attacks. Defensive actions of each subordinate network are the responsibility of the respective subordinate NOSC and may be integrated into the CNOSC.

Cybersecurity Actions

5-5. Cybersecurity actions are those taken within the MPN to prevent unauthorized access to, and exploitation of, or damage to computers, electromagnetic communications systems, and other information technology. These actions aim to ensure the MPN's confidentiality, integrity, and availability. It is not specific to an enemy, threat, or adversary.

5-6. Cybersecurity actions protect the networks and systems through all phases of network planning, implementation, and operation. This includes vulnerability assessment and analysis, vulnerability management, incident handling, patch management, configuration management, continuous monitoring, and detection and restoration capabilities to shield and preserve information and information systems.

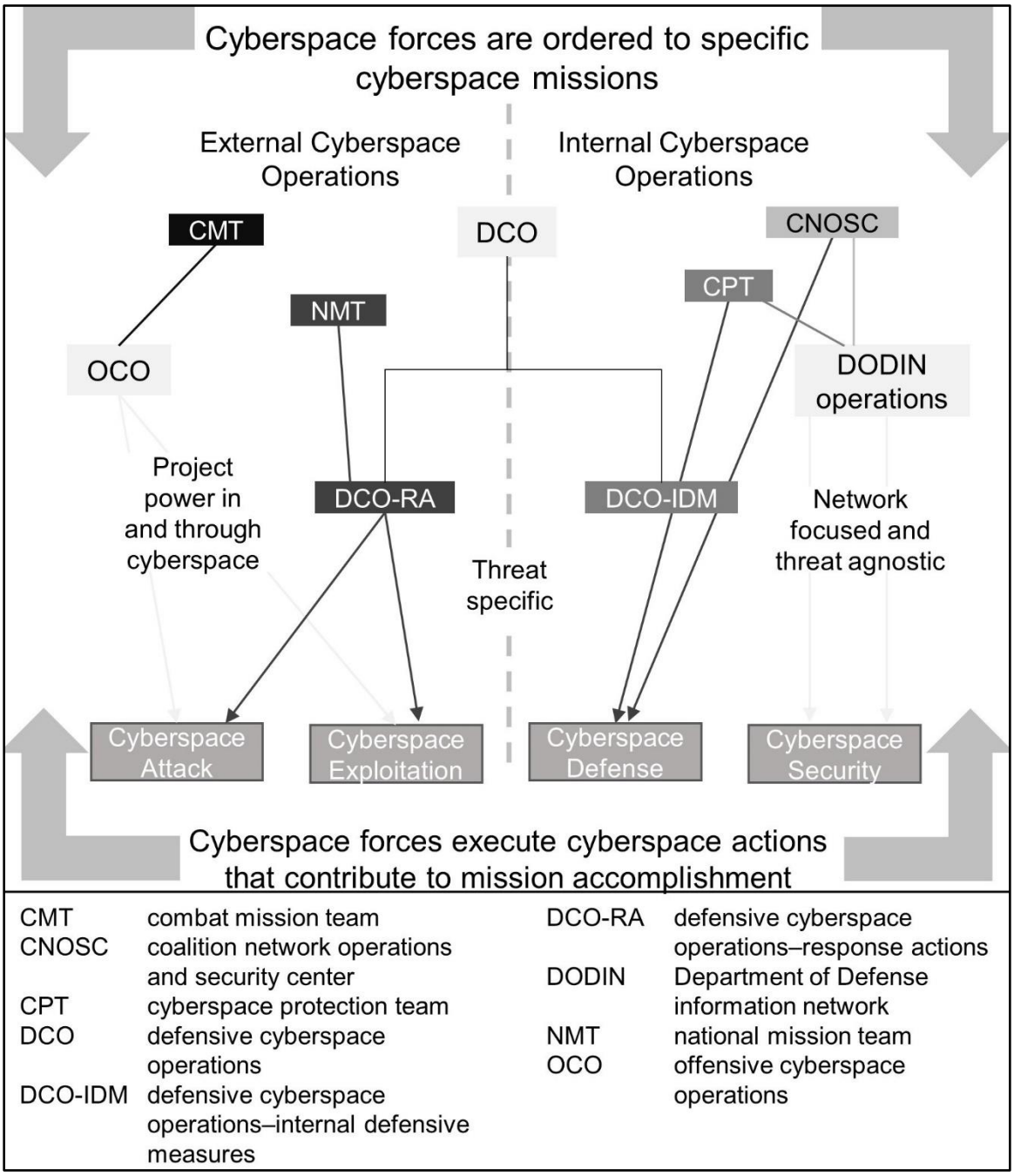

Figure 5-1. Cyberspace operations core activities

CYBERSPACE MISSIONS

5-7. Cyberspace missions conducted internal to the MPN are DODIN operations and defensive cyberspace operations–internal defensive measures.

Network Operations

5-8. With respect to cyberspace operations, DODIN operations are threat agnostic. These network operations provide users and systems at all levels with end-to-end network and information system availability, information protection, and prompt information delivery.

Defensive Cyberspace Operations–Internal Defensive Measures

5-9. Defensive cyberspace operations–internal defensive measures are threat specific and mission prioritized to retain the ability to use the MPN. These measures may involve reconnaissance measures in the MPN to locate internal threats and may respond to unauthorized activity, alerts, and threat information. Internal threat cueing may come from cybersecurity tools employed on the network. Defensive cyberspace operations–internal defensive measures focus on dynamically reestablishing, re-securing, rerouting, or isolating degraded or compromised local networks to ensure sufficient cyberspace access for multinational forces.

MISSION PARTNER NETWORK CYBERSECURITY OPERATIONS

5-10. MPN cybersecurity operations are aligned with the National Institute of Standards and Technology (NIST) *Cybersecurity Framework*. The framework relies on a variety of existing standards, guidelines, and practices that enable the multinational forces to achieve resilience across the MPN. The tools and methods available to achieve the framework outcomes range across mission partners and evolve with technological advances and operational requirements. The use of existing and emerging standards enables economies of scale and drives the development of effective products, services, and practices that meet identified operational needs.

5-11. MPN cybersecurity operations use the NIST *Cybersecurity Framework* core to define the set of cybersecurity activities, desired outcomes, and applicable references that are required across the MPN. Using the NIST *Cybersecurity Framework* core also allows for communication of cybersecurity activities and successful outcomes across the MPN from the command level to the implementation level.

MISSION PARTNER NETWORK CYBERSECURITY FUNCTIONS

5-12. The MPN cybersecurity operations consist of the NIST's *Cybersecurity Framework* five concurrent and continuous functions. Table 5-1 lists these functions and what is included in each.

Table 5-1. Cybersecurity framework functions

Identify	*Protect*	*Detect*	*Respond*	*Recover*
• Asset management • Operational environment • Governance • Risk assessment • Risk management strategy • Supply chain risk management	• Access control • Awareness and training • Data security • Standard operating procedures • Maintenance • Protective technology	• Anomalies and events • Security continuous monitoring • Detection processes	• Response planning • Communi-cations • Analysis • Mitigation • Improvements	• Recovery planning • Improvements • Communi-cations

MISSION PARTNER NETWORK SECURITY PLAN AND STANDARD OPERATING PROCEDURES

5-13. Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets. The CNOSC is responsible for incorporation of mitigation strategies into the MPN security plan and SOPs as required. This plan proposes countermeasures that involve mitigating, eliminating, accepting, or transferring the risks and considers prevention, detection, and response to threats. Countermeasures include technical tools such as firewall and antivirus software, policies, and procedures requiring such controls as regular backups and configuration hardening, training in security awareness, and establishing defensive cyberspace operations teams and capabilities.

5-14. The NIST *Cybersecurity Framework* specifies several plans that should be developed. Generally, planners write and develop these plans in the CNOSC SOPs.

Chapter 6
Integration of the Digital Common Operational Picture

This chapter provides guidance on integrating the multinational force's digital COP.

COMMON OPERATIONAL PICTURE OVERVIEW

6-1. A multinational force COP is more difficult to create and maintain than an Army unit COP. A *common operational picture* is a display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command (ADP 6-0). The Army unit COP is created from command and control information systems designed to operate together. However, a multinational force COP must be just as timely, accurate, complete, relevant, and shared with confirmed data integrity and secure network connectivity from command and control information systems developed by different nations. Creating and maintaining a multinational force COP requires more planning and integration than an Army COP.

6-2. To enable situational awareness in multinational operations, the COP—

- Provides a digital exchange between the multinational force headquarters' and subordinate units' command and control systems graphically using digital maps and overlays depicting operational graphics, unit locations, enemy positions, and control measures.
- Displays the friendly and enemy locations, significant activities, and operational graphics for staff sections to maintain area of operations situational awareness.
- Is continuously monitored ensure consistency with subordinate units' operational pictures.

COMMON OPERATIONAL PICTURE PLANNING

6-3. Upon receipt of an operation plan, warning order, operation order, or fragmentary order from the higher headquarters, and upon commencement of command and control activities, the commander issues guidance on displaying a COP. The multinational force headquarters then establishes communications with subordinate units, other mission partners, adjacent units, and higher headquarters to establish the COP requirements. Staffs then take the following steps:

- The planners conduct a multinational force COP tabletop discussion to identify and prioritize the multinational force COP display priorities. Examples are number and type of graphic objects exchanged and timing of updates.
- The information management officer and knowledge management officer develop the COP information exchange plan.
- The G-6 and assistant chief of staff, operations (G-3) network, and command and control systems planners identify the digital COP capabilities that subordinate units can implement and develop a COP technical architecture. Once a COP technical architecture is developed, risk reduction events are scheduled to validate the COP capability to develop a COP primary, alternate, contingency, and emergency (known as PACE) plan.
- The G-6 and G-3 plan for the COP coordination cell to overcome difficulties in creating and maintaining a digital multinational COP. See Appendix E for more on the COP coordination cell.

6-4. The multinational force headquarters is responsible for providing a digital liaison detachment team, sourced either internally or externally, to any mission partner that does not have a digital COP capability.

COMMON OPERATIONAL PICTURE NETWORK OPERATIONS PLANNING

6-5. Network managers consider the following COP areas that the network and command and control systems use to exchange the digital COP:

- Current friendly locations down to platform level.
- Enemy situation.
- Enemy size-activity-location-uniform-time-equipment reports.
- Significant activities.
- Operational graphics.
- Obstacles.

6-6. The network and command and control systems should support essential information interoperability requirements. These requirements produce the COPs defined in Table 6-1.

Table 6-1. Common operational picture essential information interoperability requirements

Operational Information Group	***Requirement***	***Description***	***Related Information Product Examples***
Friendly and neutral organization	Force tracking	Current positions and associated movement data – Friendly (two levels down)	Position location indicator Situation report (SITREP)
	Entity tracking		
Friendly and neutral nonorganization	Control measures	Boundaries and routes (Higher and two levels down)	Main supply route Alternate supply route Area of operations Area of interest
Friendly and neutral nonorganization	Coordination measures	Specific areas of interest required for coordinating operations	No-fly zone Protected area Fire support coordination measure Phase lines Air space control Mission synchronization matrix
Friendly and neutral nonorganization	Environmental data	Environmental (natural or man-made) obstacles and installations that impact at a global level	Obstacles plan Obstacles report Key terrain Protected areas
Enemy uncorrelated	Force reporting	Internal collection of enemy activity reporting prior to conduct of intelligence assessment	Significant activity Contact report Battle damage assessment Intelligence reports
Enemy correlated	Enemy assessment	Intelligence picture of assessed and confirmed enemy activity and intentions	Intelligence summary Emitter emission map
Globally significant	Significant activity	Reporting of significant activities or events, warning, and alerts	Significant activity SITREP Intelligence report
Battlefield management system feed	Fires, intelligence, sustainment, and air support	Metadata attributes and descriptors	Imagery status

COMMON OPERATIONAL PICTURE TECHNICAL STANDARD

6-7. A multinational force COP follows standards for a multinational force COP exchange. This type of exchange adheres to guidance from a multilateral interoperability programme (known as MIP). Refer to American, British, Canadian, Australian, and New Zealand (ABCANZ) Standard 2100 for information on a multinational force COP exchange.

This page intentionally left blank.

Appendix A

Coalition Operations Handbook Communications and Information Systems

The information in this appendix is drawn from the communications and information systems chapter in ABCANZ Publication 332 concerning coalition operations.

COALITION COMMUNICATIONS OVERVIEW

A-1. For communications and information systems, effective planners understand the factors that affect coalitions. Multinational operational planners must provide the framework of the mission intent, objective, the mission partners, and the expected operational phases of the mission. The ABCANZ *Coalition Operations Handbook* (also called ABCANZ Publication 332) provides coalition planning questions that a coalition task force needs to answer to mitigate interoperability gaps. This handbook aids all coalition functional area planners in developing an integrated coalition operation order. Specifically, the communications and information systems planning aid is in chapter 10 of the handbook. Effective communications among members of the coalition and coalition headquarters is critical to mission accomplishment. Detailed analysis of the IERs for the coalition communications planning is fundamental to successfully supporting the commander's ability to exercise command and control. The primary staff officer responsible for communications and information systems is the G-6.

A-2. Normally, the coalition headquarters determines the appropriate communications procedures for working closely with other national contingents. The coalition headquarters and national contingent headquarters follow these procedures. National contingents normally provide a mission network extension to the coalition WAN in a MPE. Internal to national contingents, individual national procedures are used. If national contingents cannot provide a network extension to the mission network, then the coalition headquarters, where feasible, provides unique communications and information systems equipment, software, and operators to national component headquarters of the other nations to facilitate communications. See appendix B for high-priority IERs.

COALITION COMMUNICATIONS PLANNING

A-3. Communications planning for deploying a single, national force into an operational environment is challenging enough. Continuous technical upgrades, demanding user requirements, technological limits, resource caps, hostile threats, and austere environments impose ever-present constraints on national planners. Coalition planners have an added set of factors to address when considering how communications impact coalition partners. These planners consider technological disparity, technical interoperability, procedural dissimilarities, language differences, security concerns, resourcing limitations, and command and control issues.

A-4. Communications and information systems planning assumes the lead nation will deploy a headquarters to form the coalition headquarters and will provide its own national force and rear-link communications. The MPN provides a core network through the framework nation and supporting nations are connected to share information. Coalition operations planning for the MPN should go from division headquarters down to brigade to battalion. This appendix discusses adjustments and added considerations required to provide communications for the larger coalitions. It focuses on the coalition planning factors.

A-5. Planners consider past efforts among mission partners while commanders consider what partners can currently do. In the past, coalition forces achieved communications using limited simple voice and data links. Some partners made efforts to become interoperable at an integrated level with communications and information systems' technological and procedural standards. The commander must take steps and make

decisions to mitigate risks of including partners who are not interoperable—including through equipment loans and liaison teams—with the lead nation. Such connections will continue to occur for the immediate future. Still, user demands, sophisticated applications, and the goal of network-enabled operations push communications planners to integrate coalition partners into a richly connected information-sharing environment. Any hope to achieve this vision requires communications planners to liaise with their coalition counterparts as early as possible in the planning phase of the operation. Early liaison helps planners identify and solve interoperability and security problems.

Note: If the United States is the lead nation, planners confirm the authorities, responsibilities, and processes to loan U.S. information technology to mission partners who are not interoperable.

JOINING, MEMBERSHIP, AND EXITING INSTRUCTIONS

A-6. The coalition headquarters determines the appropriate communications procedures for working closely with the other national contingents. The headquarters uses the JMEI which provide a framework for planning and executing the expeditionary MPN to enable operations. The expeditionary MPN enables commanders to implement a standardized approach to DODIN operations, assign clear responsibilities, and allocate resources. The JMEI support network management and are consistent with the North Atlantic Treaty Organization Federated Mission Networking (known as FMN) construct. The JMEI will also assist coalition partners in achieving authority to operate and authority to connect to the mission network. These instructions also spell out the internet protocol ranges for participating nations and provide each nation a place to list all core and command and control services required to accomplish each mission. The JMEI provide the method to enter, operate on, and exit the mission network. Coalition forces use the network to share information from the higher headquarters to participating national forces and organizations, supporting division headquarters, and subordinates as required. This network enables trusted, secure, and ensured information sharing without impediment among all participants. The key to a successful operation is the focus on connecting common services for exchanging and sharing information. Some common services include—

- Voice over internet protocol.
- VTC.
- Email.
- Chat.
- Global address list synchronization.
- Network time protocol.
- Web or portal collaboration (for example, SharePoint).

A-7. There are also provisions for bilateral agreements between mission participants to provide services to one another.

COALITION WIDE AREA NETWORK CONSIDERATIONS

A-8. Coalition planners account for and consider certain details when planning a coalition WAN.

NETWORK PLANNING

A-9. The following are considerations for network planning:

- How will the coalition's mission, commander's vision, coalition make-up, and command and control relationships impact implementing the coalition communications and information systems?
- Who is the designated lead nation for communications and information systems?
- How will the size, terrain, and climate of the coalition's area of operations impact coalition communications and information systems?
- What changes will impact the headquarters staff and liaison arrangements on requirements and configuration of coalition communications and information systems?

- In addition to the coalition, what indigenous government, civilian agency, and higher-level theater elements need to be connected through coalition communications and information systems?
- What is the implementation schedule and priority for communications and information systems in the coalition?
- How and to whom will orders, directives, instructions, and procedures relating to the coalition communications and information systems be disseminated?
- Have the planners coordinated the coalition's communications and information systems power requirements with the coalition's overall power requirements?
- Does a coalition electromagnetic warfare plan exist that includes the threat from hostile electromagnetic warfare?
- To what extent will the coalition use tactical radio (number, type, and priority of networks)? Will rebroadcast be required (consider location and security)? Based on the permissiveness of the electromagnetic environment, what transmission security safeguards will be implemented and do all participating nations have equipment compatible with these measures? What is the plan to mitigate if participating nations do not (equipment loan, use of liaison teams)?
- What is the plan for handling continuity of operations, disaster recovery, and performance degradation of the communications and information systems within the coalition?
- What options exist to provide connectivity in a degraded, contested, or denied electromagnetic environment?
- Are there any changes to the network from the planning to the preparation environment (such as working in an intermediate staging base versus home station)?

INFORMATION MANAGEMENT

A-10. IERs are described as the lead nation products, reports, and returns expected from the higher to lower and lower to higher headquarters. This should include higher to lower, left to right, and interagency and intergovernmental. The brigade or battalion operations staff officer (known as S-3), G-3, and operations directorate of a joint staff (known as J-3) confirm IERs within the coalition as well as the battle rhythm of reporting the IERs. The following are considerations for information management:

- What messaging services will be used by the coalition?
- What are the policies for authorization, authentication, nonrepudiation, and archiving with respect to coalition messaging?
- What is the quality of service policy to support the information management plan?
- How will flash traffic or other high-priority traffic be disseminated, and which system will be used for early warning?
- What services or formats will be used for status reporting within the coalition?
- What collaboration services and tools will be used?
- Will the coalition use VTC? If so, do troop contributing nations have the appropriate terminal equipment? Does the information system have the requisite capacity to support VTC?
- What is the COP distribution requirement?
- Are coalition and troop contributing nations communications and information systems interoperable?
- Can the command and control information systems achieve interoperability through a gateway?
- Will coalition compatible communications and information systems terminals need to be loaned to troop contributing nations?
- What plan exists for archiving coalition information, both for official record and for disaster recovery?
- What is the fall back for the loss of automated capability?
- How will LNOs interface with communications and information systems at various headquarters?
- What is the coalition service management policy?

NETWORK ARCHITECTURE

A-11. The following are considerations for network architecture:

- What is the mission network's (coalition WAN transport and command and control information systems architecture) concept of employment?
- Will the principle of providing communications and information systems connectivity within the coalition be higher-to-lower, left-to-right, and supporting-to-supported; or will an alternative methodology or exceptions be followed?
- What is the primary, alternate, contingency, and emergency plan?
- Has the command and control information systems architecture been coordinated with the coalition WAN transport system architecture?

Note. Planners consider bandwidth requirements in the network architecture.

NETWORK MANAGEMENT

A-12. The following are considerations for network management (refer to ABCANZ Standard 2100):

- What are the CNOSC responsibilities?
- What is the makeup of the CNOSC (by role and by nation)?
- To what extent can coalition communications and information systems resources be reallocated or reconfigured? Where is each nation's boundary for CNOSC control?
- Do personnel within the CNOSC have appropriate permissions to work on the network?
- Do all member of the coalition have appropriate access and permissions to systems and networks required to execute operations?
- Are there any technical interoperability challenges that were not discovered in planning that will negatively impact operations?
- What is the coalition plan to interconnect the coalition WAN to the national WANs?
- How will coalition partners initiate, authorize, coordinate, and review technical maintenance in the coalition?
- What is the internet protocol address and routing plan?
- What is the time synchronization plan (for example, network time protocol)?
- What is the quality of service policy?

Note. In addition to appropriate access and permissions, planners also consider if mission partners have appropriate training and clearance.

SPECTRUM MANAGEMENT OPERATIONS

A-13. The following are considerations for SMO:

- Has the lead nation created the coalition frequency spectrum management plan in coordination with the partner nations?
- What are the priorities for emergency frequencies?
- What extant agreements exist for coalition use of the frequency spectrum?
- What are the coalition policies for emission control?

Note. Refer to ATP 6-02.70 for information on Army SMO.

COALITION WIDE AREA NETWORK TRANSPORT SYSTEM

A-14. The following are considerations for the coalition WAN transport system:

- Has the lead nation established the common services hub (CSHub) and its connections from the higher headquarters to the division headquarters on the IERs of the higher headquarters? Have connections from the division headquarters to subordinate formations been established?
- What method of black or colorless WAN transport will each partner nation use to connect to the CSHub?
- Have the partner nations established redundant black or colorless WAN transport connections (such as SATCOMs, tropospheric scatter, high-capacity line of sight, combat net radio, and cable)?
- What is the plan to integrate the CSHub into a Federated Mission Networking compliant solution?
- Are all deployed force elements in the division, brigade, and battalion headquarters or command post construct equipped with coalition WAN transport systems, providing connectivity to enable information exchange in support of the commander and staff and the exercising of command and control of the deployed force elements?

COMMUNICATIONS SECURITY AND TRANSMISSION SECURITY

A-15. The following are considerations concerning COMSEC and transmission security:

- What cryptographic capabilities will forces use in the coalition? Identify the devices that coalition partners will use. Are the devices interoperable and to what level? Will coalition partners need to deploy with or borrow cryptographic equipment and capabilities (for example, operators and technicians)?
- What is the key management plan? What is the sharing plan and permissions required to share keys? Have forces negotiated sharing responsibilities and processes?
- What is the public key infrastructure management plan (if used)?
- How will encryption keys or X.509 certificates be disseminated throughout the coalition?
- Is there a requirement for overlay virtual private networks or communities of interest?
- What transmission security key is the lead nation going to specify for each nation to use?

Note. The sharing of COMSEC with mission partners is governed by bilateral and multilateral agreements. If the sharing of COMSEC is required, planners confirm the required authorities, responsibilities, and processes to share the COMSEC with each mission partner needing it.

INFORMATION TECHNOLOGY SECURITY

A-16. The following are considerations for information technology security:

- Has a security risk management plan been conducted for the MPE?
- Will the coalition operate in one security domain, or will it be compartmentalized into separate security domains for coalition and national information?
- How will information be exchanged between security domains?
- How will certification and accreditation of the coalition MPE be conducted and by whom? How will the certification and accreditation of the troop contributing nations communications and information systems be incorporated into the coalition's certification and accreditation process?
- How will the coalition report on, investigate, and recover from incidents involving security, information, or cryptographic compromise?
- What is the physical security plan for coalition headquarters, mobile assets, information infrastructure, remote radio frequency rebroadcast, and repeater sites?
- Has a vulnerability and threat assessment of critical friendly nodes and systems been conducted and are protection measures recommended and executed?
- How will security actions affect continuity of operations?

Notes. Bullet three asks about exchanging information between security domains. For information on how to exchange between security domains, refer to DA Pam 25-2-1. Bullet four asks about certification and accreditation; the Risk Management Framework in DA Pam 25-2-14 uses the term "authorization" instead of "certification and accreditation."

INFORMATION SECURITY AND DISCLOSURE

A-17. The following are considerations for information security and disclosure:

- What are the information access, authorization and accounting, and disclosure policies for the coalition?
- Are the information handling policies of the coalition partners equivalent to or acceptable for these classifications and caveats?

Note. Disclosure authorities are delegated from the national level by country, category of information, and classification level. It is likely that the disclosure authorities are not the same for all mission partners. In addition, the United States uses the term "cybersecurity" instead of "information security."

COMMON SERVICES

A-18. The following are considerations for common services:

- What services are required for the coalition? What services will be provided by the CSHub to partner nations?
- What are the roles and responsibilities for managing the CSHub and all other services?
- What is the domain name server architecture for the mission network?
- What is the email exchange architecture between supporting nations (if needed)?
- What is the voice and video architecture between supporting nations? Who is responsible for developing and managing the voice and video architecture for all phases?
- How will the coalition directory and global address list be maintained and disseminated?
- How will domain trusts between supporting nations be set up and maintained within the mission network?
- What coalition collaboration tools will be used (for example, SharePoint, web portals, file sharing)?
- What is the chat architecture?
- How will radio over internet protocol be transported over the mission network?

Note. Planners also consider how the common services are assessed, authorized, patched, and configured.

Appendix B

Architecture Database Products, Reports, and Returns

This appendix provides a list of products, reports, and returns.

B-1. Table B-1 is a list of high-priority command and control information exchange products, reports, and returns that may be exchanged between the multinational force and subordinate headquarters. Mission partners agree to and implement these products as voice and/or structured message templates for use in a division headquarters or below. Refer to ABCANZ Standard 2100 for information exchange products, reports, and returns.

Note. Neither NATO nor ABCANZ have developed information exchange requirements for fires information products.

Table B-1. High-priority information exchange products, reports, and returns

Information Product
Arrest Report (ARRESTREP)
Aviation Logistics Coordination Report (ALCREP)
Barrier Report (BARREP)
Battle Damage Assessment Report (BDAR)
Bomb Report (BOMBREP)
Casualty Notification (Stage 1) (NOTICS1)
Chemical, Biological, Radiological and Nuclear Situation Report (CBRN SITREP)
Collateral Damage Report (COLATDAMREP)
Combat Services Support Demand (CSSDEM)
Command, Control, and Information System Status Report (CCISSTATREP)
Commanders Assessment Report (ASSESSREP)
Commanders Medical Report (COMMEDREP)
Common Capture Report (COMCAPREP)
Daily Replenishment Implementation Program (DRIP)
Electromagnetic Warfare or Interference Jamming Report (EWJAMREP)
Emergency Burial Report (EMBUREP)
Enemy Contact Report (ENEMY CONTRACT REP)
Enemy Sighting Report (LAND) (SPORTERLAND)
Engagement of Hostile Aircraft (ENGRDATAREP)
Explosive Ordnance (EO) Report (EOREP)
Forward Line of Own Troops (FLOT)
Fragmentary order (FRAGORD)
Human Intelligence Report (HUMINTREP)

Table B-1. High priority information exchange requirements (continued)

Information Product
Incident Report (INCREP)
Incident Spot Report (INCSPOTREP)
Intelligence Report (INTREP)
Intelligence Summary (INTSUM)
Isolated Soldier Guidance (ISG)
Key Leader Engagement (KLE)
Location and Status Report (LOCSTAT)
Logistics Assessment Report (LOGASSESSREP)
Logistics Assistance Request (LOGASREQ)
Logistics Assistance Response (LOGASRESP)
Logistics Deficiency Report (LOGDEFREP)
Logistics Situation Land (LOGSITLAND)
Logistics Surplus Report (LOGSURPLUS)
Logistics Update (LOGUPDATE)
Mechanism, Injury, Symptoms, Treatment Age & Time (MISTAT)
Medical Evacuation Request (MEDVAC)
Movement Request (MOVREQ)
Movement Situation Report (MOVSITREP)
Obstacle Report (OBSREP)
Own Situation Report (OWNSITREP)
Patrol Report (PTLREP)
Patrol Tasking Forecast (PLTASKFOR)
Public Information Situation Report (PISITREP)
Recovery Evacuation Report (RECEVACFORM)
Request for Information (RFI)
Situation Report (LAND) (SITREPLAND)
SLANT Report (SLANTREP)
Source Report (SOURCEREP)
Threat Warning (THREATWARN)
Unit Positioning Request (UNITPOSREQ)
Unit Position Response (UNITPOSRESP)

Appendix C

Change Management

This appendix provides guidance on conducting change management on the MPN. It outlines the requirement for, and function of, a multinational force change advisory board and articulates its role in the change management process and the structure of the board.

BACKGROUND

C-1. According to the ITIL®, change is the addition, modification of, or removal of anything that could have effect on information technology services. Change management is a process that seeks to minimize the risk associated with changes to information technology services. Essentially, the process acts as a gate keeper, ensuring that changes are made only after planners carefully consider risks and potential side effects. A typical change management process is outlined in Figure C-1 on page C-2.

Note. Providing information on ITIL® does not constitute the Army's endorsement of the product.

C-2. ITIL® identifies three different types of changes:

- Standard changes are pre-authorized, low-risk changes that follow a well-known procedure.
- Emergency changes are changes that must be implemented immediately.
- Normal changes are all other changes that are not standard changes or emergency changes.

C-3. Normal changes are often sub-categorized as major, significant, or minor depending on the level of risk involved. The multinational force headquarters defines these types of changes and the required change authorities in their change policy or change management SOP.

C-4. Nonstandard changes require the submission of a request for change-to-change management. A request for change is a formal request for a change to be implemented specifying the details of the proposed change.

C-5. The following actions may result from a request for change:

- Approve.
- Reject (the reason for the rejection must be documented).
- Approve with changes.
- Approve for future implementation or baseline.
- Defer (the reason for the deferral must be documented).
- Recommend approval (this is the change advisory board's recommendation to a higher, national, or host-nation change advisory board when the change impacts higher, national, or host-nation baseline).

C-6. A release plan is developed for each approved change. Each implementation plan includes a recovery plan. A recovery plan contains specific instructions for returning specific services, systems, or both to a working state.

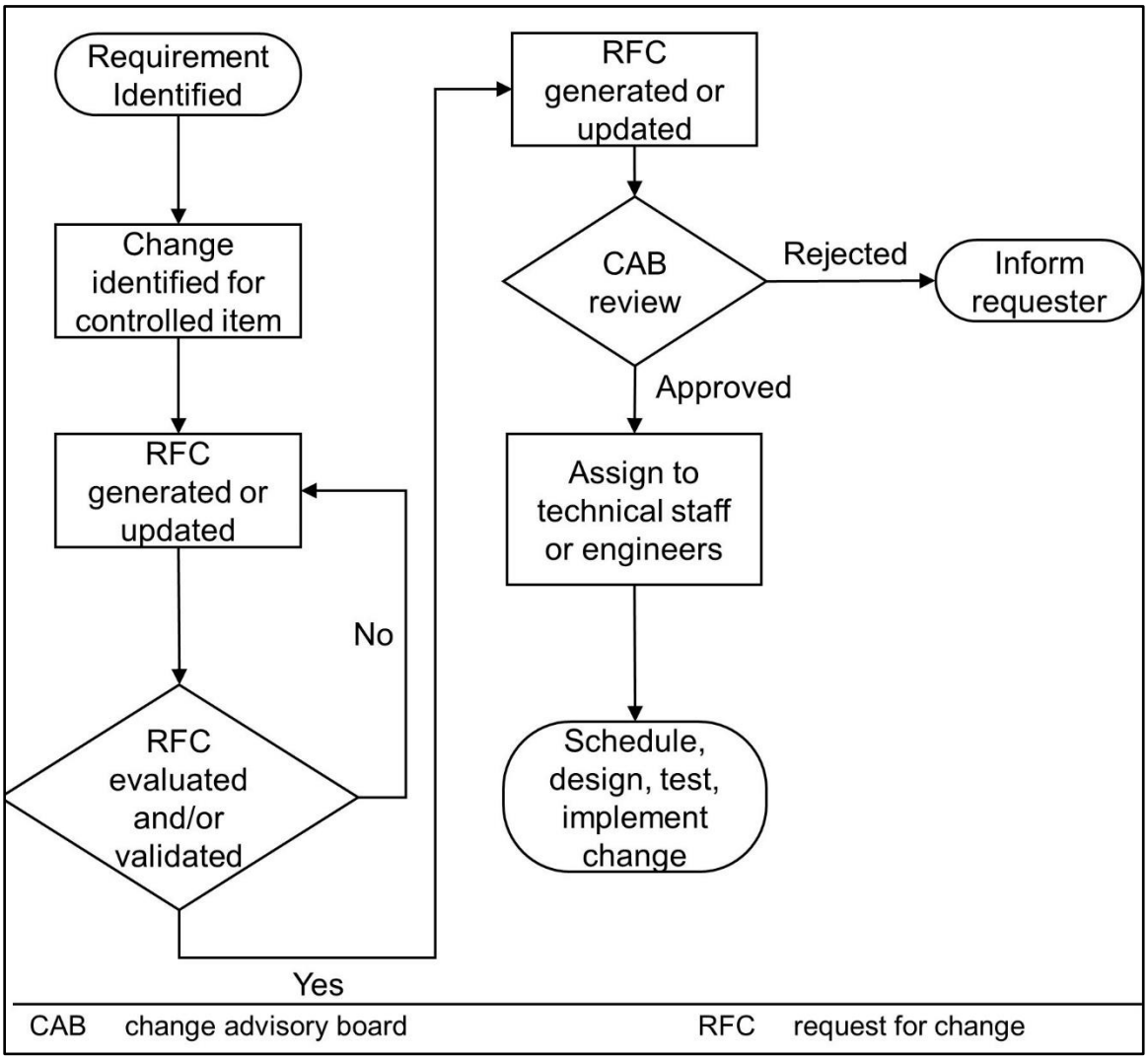

Figure C-1. Example change management process

C-7. A change manager and a change advisory board are required for a change. The change manager is the multinational force technical authority. The change advisory board advises the change manager on the assessment, prioritization, and scheduling of changes. A change manager and a change advisory board ensure the overarching intention and policies of change management are employed throughout the service management lifecycle and with specific considerations for every aspect of the complete service.

CHANGE ADVISORY BOARD SCOPE

C-8. The change advisory board has a limited scope. The board is responsible for maintaining and controlling the system baseline on behalf of the network operational authority. Staffs call on the change advisory board to examine operational, technical, security, and design issues associated with changes that have a system-wide impact.

RESPONSIBILITIES

C-9. The change advisory board is responsible for, but not limited to, the following:

- Managing change to the network baseline during the in-service lifecycle of the network within the scope identified in paragraph C-8.

- Forwarding changes to the respective national-level authorities where potential changes may impact national networks.
- Tracking and recording changes to the baseline.
- Resolving issues through coordination with other change advisory boards (subordinate or higher).
- Providing all stakeholders a forum for the discussion of operational, technical, cost, schedule, or benefits issues.
- Providing DODIN operations priorities and guidance on changes to the baseline on the MPN.
- Ensuring all approved changes are tracked, documented, implemented, and verified.
- Developing a change advisory board charter and maintaining its currency throughout the lifecycle of the network. This charter outlines the delegation of authority, procedures, and dispute resolution strategies.
- Assessing the impact to cyberspace security for all changes to the MPN.

PROPOSED LIST OF PARTICIPANTS

C-10. Paragraphs C-11 through C-16 is a proposed list of change advisory board participants.

Chair

C-11. The multinational force technical authority is the change advisory board chair. This technical authority has responsibility to adjudicate proposed changes presented to the change advisory board, assign action items as necessary, approve change advisory board operating procedures, and designate change advisory board permanent and ad hoc members.

Executive Members

C-12. The following are a list of executive members of the change advisory board:

- Multinational force G-6 operations officer.
- Multinational force G-6 plans officer.
- Multinational force P-ISSM.
- CNOSC director or officer in charge (OIC).
- Subordinate NOSC OIC, technical authority, or representative.
- Network engineers.

Secretary

C-13. The secretary is a member of the CNOSC. This person has responsibility to determine the change requests and potential requirements that are ready for disposition at the change advisory board, schedule meetings (in-coordination with the executive members), prepare and distribute the agenda, and maintain a record of discussions.

C-14. The change advisory board secretary provides change processing and status accounting services to the board, pending change requests, and action items assigned at the change advisory board.

Ad Hoc Members

C-15. Ad hoc members represent organizations or special skills that are not permanent members of the change advisory board, which may be impacted by changes being reviewed by the board. Their function is to ensure that proposed changes are consistent with the technical and policy positions of their organizations.

Technical Advisors

C-16. Technical advisors are personnel invited, as required, to attend the change advisory board meetings to provide specialized technical or program management information.

CHANGE AUTHORITY

C-17. Formal authorization at the multinational force headquarters level is obtained for each change from the multinational force technical authority. The levels of authorization for change are articulated in Figure C-2 on page C-4.

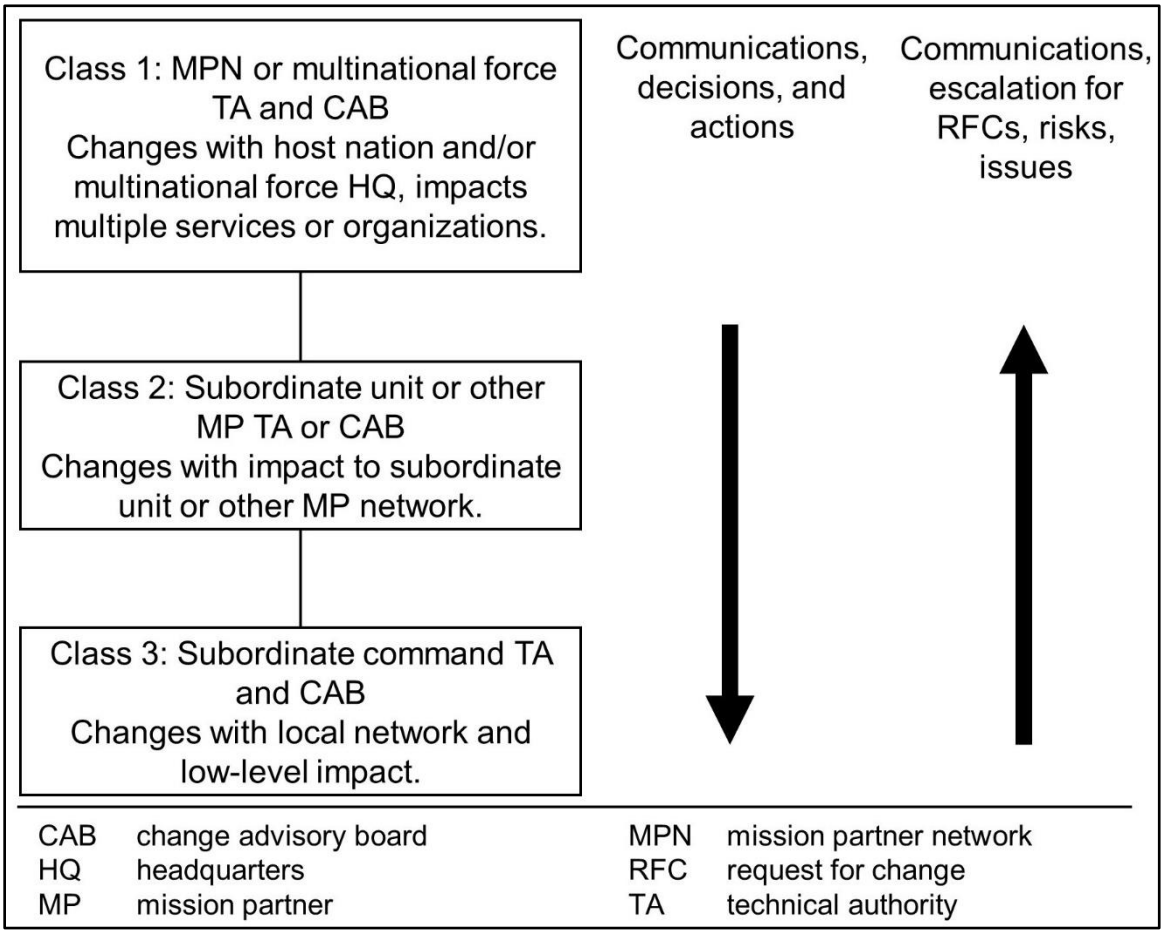

Figure C-2. Change authority hierarchy

Appendix D

Service Desk Management

This appendix discusses the processes and procedures required to operate a service desk in a CNOSC or subordinate NOSC. These processes and procedures are tailorable to meet mission requirements.

OVERVIEW

D-1. During day-to-day operations in an operational environment, the signal staff—at all echelons—deals with various incidents and outages in which communication systems fail, security incidents are detected, users request information, and events are sent automatically from devices. To address these incidents, the signal staff uses the service desk to provide a single location within a unit to which these requests, incidents, and events are reported, tracked, and resolved. The service desk provides support for—

- Requests which normally result from a user asking for information or assistance from a service desk.
- Incidents which are considered unplanned interruptions in service.
- Events which are automated notifications sent relating to the status or health of a device or system.

D-2. Each unit operates its own service desk to resolve incidents in its portion of the MPN. Units escalate incidents that impact the MPN to the CNOSC from the subordinate NOSC for resolution, and staffs notify any affected units. For example, if the United States has an issue that affects its ability to conduct voice calls over the MPN, it creates a local trouble ticket at the subordinate NOSC. Signal staff then escalate it to the CNOSC for assistance and ensure all other units are notified about an issue impacting their ability to communicate with the United States.

SERVICE DESK

D-3. The service desk is the central interface for request, incident, and event resolution. The service desk is expected to provide immediate resolution for basic incidents according to the complexity and service desk staff's experience with the specific issue. The more incidents the service desk resolves without escalating to a technician or another service provider, the quicker the resolution process. This is known as first contact resolution.

D-4. The service desk creates a ticket detailing an issue and annotates the ticket as completely and as accurately as possible to capture basic information in addition to the issue. During the collection process, the service desk evaluates the severity of the issue as well as the priority of the incident to determine the response objective. This ensures the issue is addressed in a timely manner, in accordance with leader guidance, and per criticality of the issue. No matter to what tier the ticket may be escalated, the originating service desk maintains ownership of the incident until full resolution.

D-5. The signal staff can develop customized service desk templates for specific types of incidents to capture additional information that may be useful in solving the problem.

D-6. The G-6 or the S-6 ensures the ongoing operation, administration, support, and stability of the local service desk. This is necessary in this support model and mission critical to the service desk, local technicians, and other service providers.

USERS

D-7. Users are expected to understand and follow the defined process, so resources are appropriately allocated and problem resolutions are reached expeditiously. They also read and follow instructions,

frequently ask questions, and access websites and other supporting processes when available to garner information prior to calling the service desk or engaging any service providers.

D-8. Users must understand the methods for communicating with the service desk. The most common methods for a user to submit incidents to the service desk include, but are not restricted to, the following:

- Walk-in.
- Call (telephone).
- Web page.
- Email.

LOCAL TECHNICIANS AND SERVICE PROVIDERS

D-9. Every person in the signal staff, regardless of the echelon, has some responsibility for problem management. The local service desk provides tier 1 and sometimes tier 2 support. Most often, the local technicians are the next step in the resolution process. While the service desk and the technicians on the signal staff strive to resolve as many problems as possible, sometimes other organizations outside the service desk need to address problems in specific areas.

LEADERS

D-10. At times incidents arise that require the involvement of leaders to address problems. Incidents that involve leaders often address command priorities, commander's critical information requirements, operation orders, and fragmentary orders. Such incidents normally include incidents related to security, extended outages, and mission critical applications. To address these incidents, leaders may be required to initiate an investigation, validate reports that are sent to higher, and adjust the mission based upon extended outages.

EXTERNAL SERVICE PROVIDERS

D-11. Service providers follow an approach similar to the ITIL® approach to service operations and use the service desk appropriately so all problems are handled in a consistent, repeatable, and predictable manner. To ensure an effective relationship in resolving incidents, the local service desk ensures the external service providers—

- Acknowledge a service request assigned by the service desk entry person and provide a reference as required.
- Notify the appropriate service desk with the status of the assigned trouble tickets.
- Notify the appropriate service desk upon completion to describe the resolution. This provides a knowledge base of information that can be used by local support personnel and is sent to the knowledge base if applicable.
- Provide the service desk with technical information and problem-solving techniques when requested. When the service desk continuously receives problem calls on certain incidents, staff may request updates to or developments of additional training, frequently asked questions, information websites, and documentation to reflect the types of calls received.
- Assist the G-6 and S-6 to resolve escalated problems. The G-6 or S-6 is responsible for assessing the criticality of a given situation or user and appropriately escalating any special situation to an internal service provider.
- Form emergency response teams to correct large- or wide-scale problems.

Note. Providing information on ITIL® does not constitute the Army's endorsement.

D-12. The service desk exercises discretion in the escalation of any situation but should expect that the service provider follows through with any escalated service desk trouble tickets. This follow through frequently involves upset users, very important person users, or critical infrastructure and application failures. Such escalated trouble tickets constitute a high volume of service desk trouble tickets.

D-13. Any changes made are noted on the service request for that call. Information concerning these changes is shared with all technicians and affected users, with the work order number referenced should technicians need additional information.

CONCEPT OF SERVICE DESK OPERATIONS

D-14. Request, incident, and event management are processes that start at the identification of an issue through the reporting, tracking, resolution, and documenting of the issue. These processes, while universal in the need to resolve the issue, are not always performed, documented, and tracked in the same manner. As tools become more standardized and the systems become more integrated, the need for a standardized process becomes more critical because of the cascading affect that these incidents may cause or the affect upon a larger population of users. Figure D-1 illustrates the concept of service desk operations.

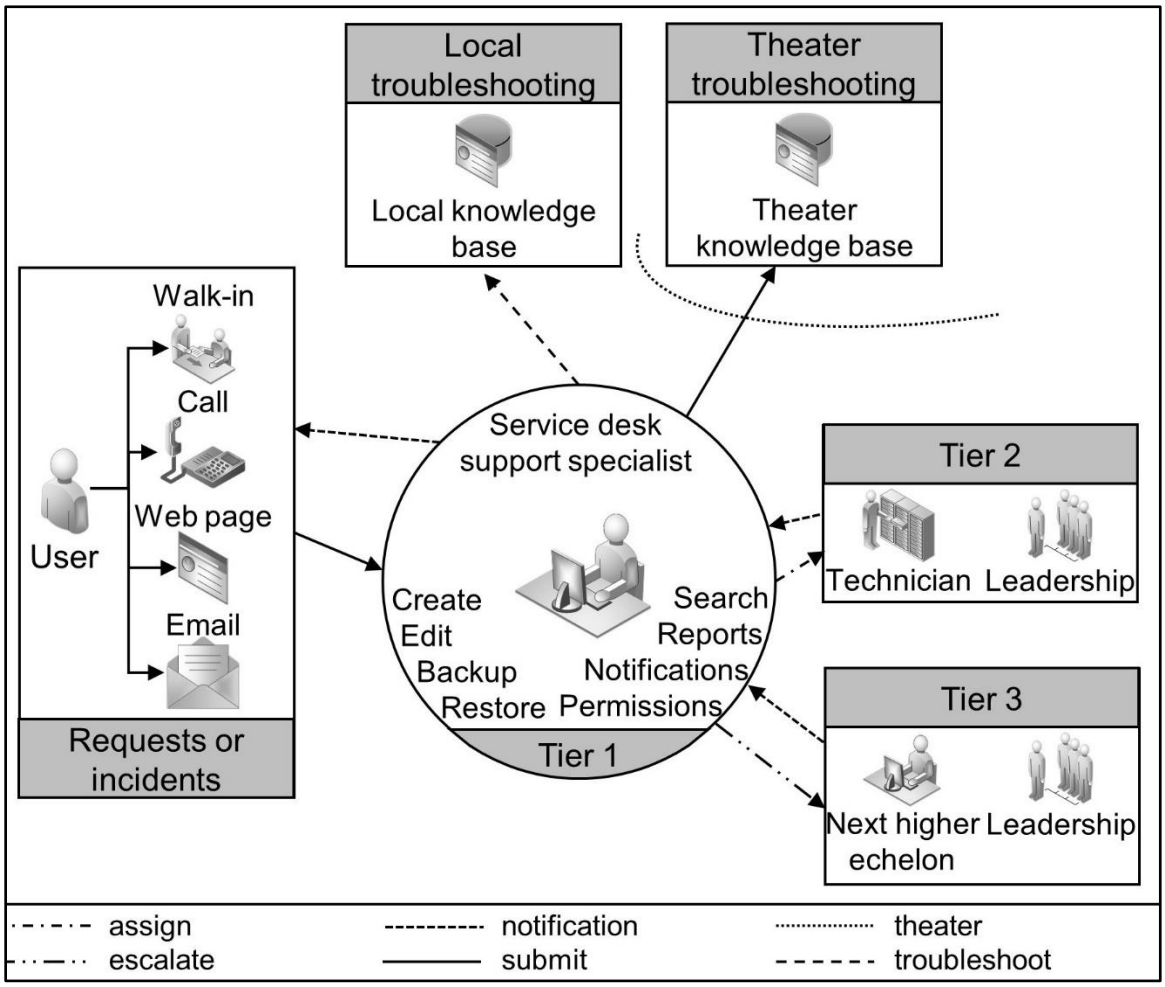

Figure D-1. Concept of service desk operations

D-15. During normal operations, the signal staff provides a means to submit and track requests and incidents relating to signal operations within the headquarters. The service desk is the primary location and is the central point of contact for handling user and other communications or service-related incidents. Although the primary focus is on communications and services, staffs often use the service desk to track various incidents within the headquarters.

D-16. The service desk receives, troubleshoots, and responds to end-user requests, incidents, and events. The service desk logs and tracks all reported incidents and determines the best manner to address them. One of

the top priorities of the service desk is to ensure a consistent response to problem resolution, service requests, status reporting, escalation, and notification of changes related to the communication systems.

SERVICE DESK SUPPORT TIERS

D-17. Paragraphs D-18 through D-23 list the tiers of support from a service desk.

Tier 0

D-18. This tier is typically a web self-service portal known as "self help." Examples include frequently asked questions and how-to guides. Incidents that fail to be dealt with at this tier filter to tier 1.

Tier 1

D-19. This is the basic tier of support where incidents are logged into the service desk, triaged, and troubleshot. The staff resolves elementary problems at this tier. Examples of this include basic how-to questions, hardware diagnostics, password resets, and account creation.

D-20. The service desk support specialist generally handles these tier 1 incidents relatively quickly. The service desk support specialist walks a user through an application issue, or a service desk support specialist activates a disabled account.

Tier 2

D-21. This tier of support involves incoming user phone calls, emails, and requests logged into the service desk. Staffs obtain the relevant details and route an issue to an appropriate local support resource. These incidents are normally identified through tier 1 troubleshooting, or the service desk support specialist determines a higher tier of support is necessary.

D-22. The support personnel at this tier may be required to make changes to the infrastructure or systems that support the entire unit. For example, changes can include group policy changes, email service changes, routing or network changes, and security policy changes which require G-6, S-6, or leader approval. In a deployed environment, change management is completed in a scaled down decision process that is less formal than the change management process within the strategic environment. The G-6 and S-6 or leaders at each echelon normally give approval for changes where the change is required.

Tier 3

D-23. The service desk does not generally provide this tier of support. However, the service desk receives the issue, logs the issue, and then directs the issue to the appropriate resource. The issue requires escalation to an external service provider, such as contract support, a higher echelon service desk, or a tier resource. These problems usually involve advanced tiers of support that require specialized technical or application expertise, support for systems that are outside the control of the unit, or possible outside vendor assistance.

ESCALATION

D-24. Escalation is the act of notifying the next higher service desk when the local service desk is unable to address an issue. Escalation also includes incidents routed to system support representatives and external service providers. If the service desk cannot resolve an issue, it escalates the problem to the next appropriate location for resolution. When the service desk escalates an incident, it hands the ticket over to the next higher service desk for continued troubleshooting, processing, or resolution. The original service desk still maintains ownership of the ticket and all actions until full resolution.

D-25. If the issue is related to a system or service with its own dedicated service desk, the issue is escalated to that service desk. The trouble ticket number provided is annotated locally and the issue tracked until resolved as defined in the unit service desk SOP. The escalation process continues until the issue is escalated to the location where the issue is addressed, or it is determined the issue cannot be resolved within the specified resolution time. Either conclusion requires certain actions at each tier to ensure all service desks involved understand the findings and functions as required by unit SOP.

D-26. If the service desk is required to escalate an incident report to another service provider, service desk staff collect any additional pertinent data, such as a higher echelon reference number, service provider reference number, return merchandise authorization, and any other pertinent information. Then staff enter the data into the incident report to continue to track the status.

D-27. Operationally, a hierarchical relationship exists between each echelon (command channels) and the same holds true for the trouble ticketing process. For the trouble ticketing process to work properly, the service desk staff and callers need to adhere to the escalation hierarchy. This escalation policy ensures any incidents needing to be addressed by additional resources is tracked appropriately and all echelons involved are informed of status or resolution of the issue. This is critical when the G-6 and S-6 are reporting operational statuses.

D-28. The tier of service desk support is not always formalized within all unit levels. Units may not be manned or qualified to stand up a service desk. The first tier of support is normally the local signal support personnel. Figure D-2 illustrates the process of service desk escalation.

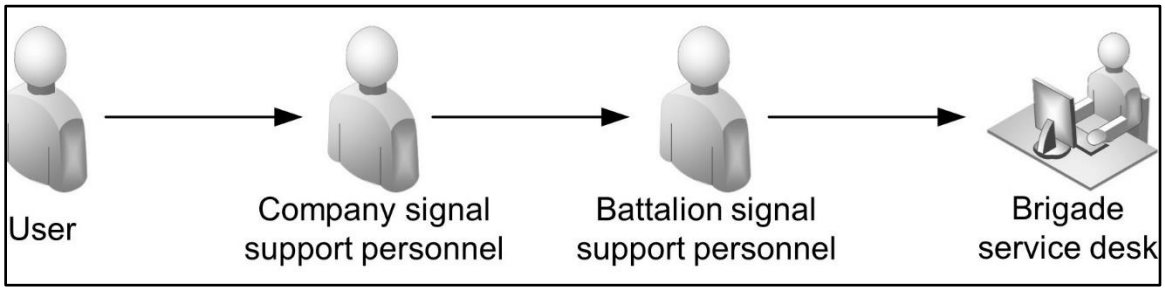

Figure D-2. Service desk escalation

D-29. In other words, a user at company level reports an issue to local signal support personnel. The company signal support personnel create a trouble ticket. If the company support personnel cannot resolve the incident, they request help from the battalion support personnel. The battalion support personnel create a trouble ticket. If the battalion support personnel cannot resolve the incident, they notify the brigade service desk, develop a trouble ticket for the issue, and identify the service provider based upon the nature of the issue. If the brigade-level service provider cannot resolve the issue, the process continues until a resolution or a decision is made concerning the issue.

D-30. It is important that a trouble ticket is created at each involved level to properly document all incidents to develop lessons learned and identify problems.

METHODS FOR MANAGING INCIDENTS

D-31. Managing incidents is commonly performed manually, using a software tool, or the combination of both. Whether entering and logging requests, incidents, and events via a paper form or via an online web form, the process essentially remains the same. Paragraphs D-32 through D-41 are not all encompassing and only represent the most common methods of issue submission and tracking.

Manual

D-32. Manual issue submission is normally via a paper form that a user fills out and submits to the service desk. The service desk then tracks the submission manually via a consolidated paper list or though data entered to a spreadsheet or database for improved tracking. The manual method focuses on tracking and responding to the incidents to ensure mission accomplishment.

D-33. Manual management of incidents does not lend itself to local analysis and event correlation because of the time and effort required to manually analyze the incidents and the time-sensitive nature of many events.

Automated

D-34. Automated issue submission is normally via a software tool that uses a web-based data entry form or template. The service desk enters the issue as data into a database or equivalent that automatically works other processes. The database provides a means to quickly track, analyze, and report on submitted incidents. The automated issue submission method focuses on tracking and responding to incidents and provides a more proactive approach while enabling significantly better analysis and reporting of statuses. An automated method for submission must support all the environments that the unit could be placed in.

Systems and Tools

D-35. Although submitting and tracking incidents can be performed manually, the recommended method is via an automated means. Using an automated tool allows for the quick submission, tracking, escalation, resolution, and analysis of incidents. In addition, it enables the submission of solutions for review and further inclusion into a knowledge base of authoritative fixes to common incidents. Paragraphs D-36 through D-41 discuss the recommended tools the service desk support specialist or technician and users within a headquarters need access to for incidents management and submission. Tools should be International Organization for Standardization/International Electrotechnical Commission 20000-1 compliant.

Service Desk Support Specialist or Technician Web Interface

D-36. The service desk support specialist or technician web interface is a web-based problem management solution. It enables the streamlining and reporting of the many complex processes required to support the users. It provides the capability for any service desk specialist and technician to access, review, update, and close trouble tickets from any location with web access to their server. It provides the ability to view the history of the submitted trouble tickets and perform analysis across all the incidents submitted for their organization.

Service Desk User Web Interface

D-37. The service desk user web interface is a web interface that allows users to enter incidents directly into the system from their desktop and allows them to check the status of their open trouble tickets.

Local Knowledge Base

D-38. A local knowledge base is a local nonauthoritative collection of data that contains incidents and resolutions for incidents that are troubleshot and resolved locally. Users can access the knowledge base to locate resolutions to recurring incidents and incidents that may require detailed steps required for analysis.

Consolidated Knowledge Base

D-39. The consolidated knowledge base is normally, but not restricted to, a wide collection of authoritative data containing incidents and resolutions consolidated from lower echelons and across a large area of operations. It provides a unified location to locate approved resolutions to identified incidents with documented solutions. This knowledge is provided from various sources, including—

- Fixes submitted and validated from a service desk.
- Unit tactics, techniques, and procedures.
- Official Army publications.
- Knowledge provided with a system or service.
- Knowledge purchased from a vendor or service provider.

D-40. Authoritative knowledge must go through a thorough technical review and be categorized as an authoritative means to fix defined incidents.

D-41. The relationships between all the personnel and organizations are clearly defined. This ensures no ambiguity in the resolution process and the service desk knows to whom they must escalate specific incidents. Normal escalation follows the typical command hierarchy.

REPORTING

D-42. The most important components in the management of a service desk are the ability to generate and report statuses. Reporting is critical in evaluating the health of the unit and the communications systems. Reporting combined with notifications ensures all the personnel involved in the resolution process are kept informed.

D-43. Reporting requirements between a unit and its higher command are normally defined in the operation order and further refined in subsequent fragmentary orders based on changes to an operational environment. Reporting requirements are also in unit SOPs; directives; and tactics, techniques, and procedures. Examples of the reporting requirements include—

- Commander's critical information requirements.
- Type of reports.
- Frequency of reporting and whether the type of issue influences the frequency.
- Reporting format and method of reporting.
- Trend analysis.

D-44. Many reports and the status information is used during commanders' update briefings that are held on a regular basis.

NOTIFICATIONS

D-45. Notifications are a method of reporting where statuses are sent, or when changes or updates are made, to the status of a trouble ticket. Changes considered for generating a notification are based upon SOPs; tactics, techniques, and procedures; and leader guidance.

D-46. Reasons for notifications include, but are not limited to—

- Creation of a trouble ticket.
- Update of a trouble ticket.
- Changes to the priority of a trouble ticket.
- Requests for additional information.
- Escalation of a ticket.
- Assignment of a trouble ticket.
- Closure of a trouble ticket.

SERVICE DESK MANAGEMENT MODEL

D-47. The service desk enables the review and addressing of incidents. Often the number of trouble tickets outweighs the number of available or qualified personnel to address the trouble tickets. The service desk implements a process to evaluate the incident on priority and severity to ensure the most important incidents are addressed in the correct order.

PRIORITY CODES AND SEVERITY LEVELS

D-48. An incident is an unplanned interruption to an information technology service or reduction in the quality of an information technology service. A problem is a cause of one or more incidents. Priority codes and severity levels document the prioritization and resolution order of problem types. All service desk personnel communicate with and use these meanings consistently when dealing with commonly shared incidents, requests, and changes.

D-49. Priority codes are designed to work in conjunction with severity levels. Priority codes offer a way to capture the business situation or requirements on a personal level whereas severity levels identify the pure business impact of a problem or request. Service desk personnel assess and capture both the priority code and severity level on the service desk trouble ticket. The use of these criteria is designed to assist in workflow prioritization and resolution based on common definitions.

Priority Codes

D-50. A priority code is a code that allows the service desk to document and consider a user's unique mission-dependent situation, title, or system when prioritizing workflow. This code allows the support personnel to respond appropriately with the proper resources in an acceptable timeframe. See Table D-1 for priority code definitions.

Table D-1. Priority code definitions

Priority 1	Very important person, general officer, or member of the senior staff is experiencing an impact to productivity or requires special attention. Individual is experiencing significant lack of productivity. User is completely inoperable.
Priority 2	Individual is requesting faster than average response based on actual need. Individual is requesting scheduled service that has a hard deadline for resolution.
Priority 3	Individual is experiencing average operational impact from problem or request and does not have above average or extenuating circumstances.
Priority 4	Individual has made a service request in advance of need that is easily handled within required timeframe. Usually a severity 4 request. User agrees that this is a priority 4 item.

D-51. The service desk provides user priorities to the entire organization. A numeric priority is given to ensure an issue is handled based upon the importance of the issue or user. In each organization, there are categories of users who customarily receive a higher priority of service because of their rank or importance. See Table D-2 for a sample priority chart. The colors in Table D-2 correspond with colors in D-4 on page D-10.

Table D-2. Example priority chart

Priority Listing			
Priority 1			
People			
Assistant chief of staff, signal (G-6) staff section Division (DIV) assistant chief of staff, operations (G-3)	DIV chief of staff DIV command sergeant major (CSM) DIV commander	DIV deputy commander DIV operations sergeant major (SGM) DIV secretary of the general staff	
Incidents			
User cannot log on or account locked out. Email Issues. Account creation.			
Priority 2			
People			
DIV air liaison officer DIV assistant chief of staff, intelligence (G-2) DIV assistant chief of staff, logistics (G-4) DIV assistant chief of staff, personnel (G-1) DIV assistant chief of staff, plans (G-5) DIV aviation officer	DIV deputy fire support coordinator DIV engineer DIV engineer SGM DIV fire support coordinator DIV G-1 SGM DIV G-2 SGM DIV G-3 plans DIV G-4 SGM DIV G-5 SGM	DIV knowledge management officer DIV staff judge advocate SGM DIV surgeon Headquarters and headquarters battalion (HHBN) CSM HHBN commander Program information system security manager	
Incidents			
Cannot print or scan. Software installs. Telephone work orders.			
Priority 3			
People			
Command drivers DIV chaplain DIV chaplain assistant DIV chemical officer DIV deputy G-4	DIV chemical, biological, radiological, and nuclear (CBRN) officer/ or CBRN noncommissioned officer DIV equal opportunity DIV master gunner	HHBN executive officer HHBN prescribed load list clerk HHBN supply sergeant	
Incidents			
System alerts. Hardware installs.			
Priority 4			
People			
Air force detachment Fire support element	G-1 shop G-2 shop	G-3 shop G-4 shop	staff judge advocate
Incidents			
Image or re-image computer.			
Key When trying to determine the trouble ticket priority, look at the person submitting the trouble ticket and then look at the problem they are experiencing. The higher of the two determines the trouble ticket priority.			

Severity Level

D-52. The severity level is a code that identifies a technology failure which has a direct impact to the unit. The code allows the service desk to respond appropriately with the proper resources within a predefined

timeframe. It is not based on the emotions or circumstances of the user. A primary criterion for severity is the number of personnel impacted when evaluating an incident. The more personnel impacted, the more severe the incident. See Table D-3 for severity level definitions.

Table D-3. Severity level definitions

Severity Level – 1		
Who	***How***	***What***
A major outage, performance degradation, or instability causing significant impact to the unit.	Many or most users are unable to function. Mission critical systems down. Mission critical application down. Mission critical server and/or circuit down.	Email, firewall, router.
Severity Level – 2		
Large number of users are impacted. Entire section or sections are experiencing a similar problem. Small number of users cannot use a mission-critical application.	Multiple users unable to function. Major performance incidents. Multiple users running on contingencies or a work-around. Backup failure of mission-critical application.	Network switch affecting areas in the headquarters.
Severity Level – 3		
Individual unable to use non-mission critical application. Users can work with minimal impact to their productivity.	Users having difficulty, but basically operational. Users unable to carry out their necessary tasks.	
Severity Level – 4		
Individual request or problem that does not impact mission.	User needs information or a standard service. User has simple question or problem. User has how-to or procedural questions.	

D-53. The routine user often provides a “first alert” when reporting incidents, especially with infrastructure applications or with network connectivity. The first few calls may indicate a much larger problem such as an “application down” or “system down.” Additional levels of reporting and documentation may be required based upon the issue, priority, severity, or the class of user. Unit policy or SOPs determine if any additional steps are required.

Situation Level Response Objective Matrix Based Upon Priority Code and Severity Level

D-54. These situation level response objectives are intended as general guidelines of expectations for providing service to users. The situation level response objective considers the priority and severity of an incident to determine response times and to ensure timely response and resolution of reported incidents. The matrix serves only as a baseline, and specific leader guidance takes precedence over these guidelines. Additionally, the response times may be used to set notification thresholds for technicians or for the internal escalation of incidents that are not resolved within the designated time. See Table D-4 for an example situation level response objective matrix. The colors in Table D-4 correspond with colors in D-2 on page D-8.

Table D-4. Situation level response objective matrix

		Severity Level			
		1	2	3	4
Priority Code	1	1	1	1	1
	2	1	2	2	2
	3	2	2	3	4
	4	3	3	4	4

D-55. To determine the situation level response objective level, the service desk personnel trace the priority code across to the severity level. For example, if an incident has a priority code of 3 and a severity level of 2, then the situation level response objective level is 2. See Table D-5 for an example response parameter prime time.

Table D-5. Example response parameter prime time

Response Objective	*Response Parameter*	*Prime Time*
Level 1	• Acknowledge and accept trouble ticket. • Initial situation response. • Status notification interval. • Maximum resolution time goal.	• 10 minutes. • 30 minutes. • 1 hour.
Level 2	• Acknowledge and accept trouble ticket. • Initial situation response. • Status notification interval. • Maximum resolution time goal. • Escalate condition if not resolved.	• 10 minutes. • 1 hour. • 2 hours. • 4 hours. • 6 hours.
Level 3	• Acknowledge and accept trouble ticket. • Initial situation response. • Status notification interval. • Maximum resolution time goal. • Escalate condition if not resolved.	• 10 minutes. • 30 minutes. • 10 hours. • 18 hours.
Level 4	• Acknowledge and accept trouble ticket. • Initial situation response. • Status notification interval. • Maximum resolution time goal. • Escalate condition if not resolved.	• 10 minutes. • 30 minutes. • 18–24 hours. • 36 hours.

Situation Level Response Definitions

D-56. Paragraphs D-57 through D-61 discuss the types and meanings for the situation level responses parameters.

Acknowledge and Accept Trouble Ticket

D-57. When the service desk personnel are contacted with an incident, they collect as much information as possible to expedite the resolution process. Once the service desk personnel dispatch a trouble ticket to a local technician or an external service provider, a support representative from that provider acknowledges and accepts the ticket and accountability for resolution. The service provider contacts the user within the required timeframe to verify assignment, receipt of the trouble ticket, and acceptance. The service provider may request the service desk to deliver a general response or outage notification to all affected users for situation level response level 1 and 2 trouble tickets.

Initial Situation Response

D-58. Situation level response level 1 and 2 trouble tickets require service providers to develop an initial response that outlines the situation and responses plan of action. This outline includes items such as response checklist and notification list. Determining the situation response and the resulting plan of action is important to the resolution of an incident. Collecting the required information and understanding the incident is critical to the situation response and determines the estimated resolution time, who is accountable for the resolution, and which users are affected. An initial situation response provides immediate notification of a major outage or problem so all parties are aware of the problem. With that knowledge, all parties can immediately assist with the resolution rather than passing the problem sequentially from group to group.

Status Notification Interval

D-59. The current owner of the trouble ticket provides updated information of the trouble ticket resolution to the service desk personnel. Updated information includes updated status and last update time and date. Sharing updated information allows the service desk to provide updated status information to users who call to check the status of a trouble ticket. It also allows all service providers to understand the status of a trouble ticket.

Maximum Resolution Time Goal

D-60. The maximum allowable time to resolve a trouble ticket is a target and service goal. The maximum resolution time goal may vary depending on the complexity of the problem or request.

Escalate Condition If Not Resolved

D-61. The service desk personnel move the priority code to the next higher level when the resolution time limit threshold is passed based on the situation level resolution objective. If the priority code is escalated, the information technology service provider is accountable for and has discretion over the escalation procedure.

INCIDENT SYNCHRONIZATION FOR TREND ANALYSIS

D-62. Incidents provide significant information on the health and security of the network and associated systems using the network. Certain types of incidents are used for analysis at higher echelons. The most important topics include security, network outage, and equipment-related incidents. Proactive organizations analyze these incidents to prevent further incidents and provide better visibility of the overall network health across a large area.

CONCLUSION

D-63. The service desk can receive, track, and resolve incidents with critical capabilities in an operational environment. Users and support personnel become supportive members in the process and assist in the overall reduction of incidents by understanding the overall process, components, and use of those components.

PROCESS CHART

D-65. Figure D-3 illustrates the trouble ticket process on the next two pages.

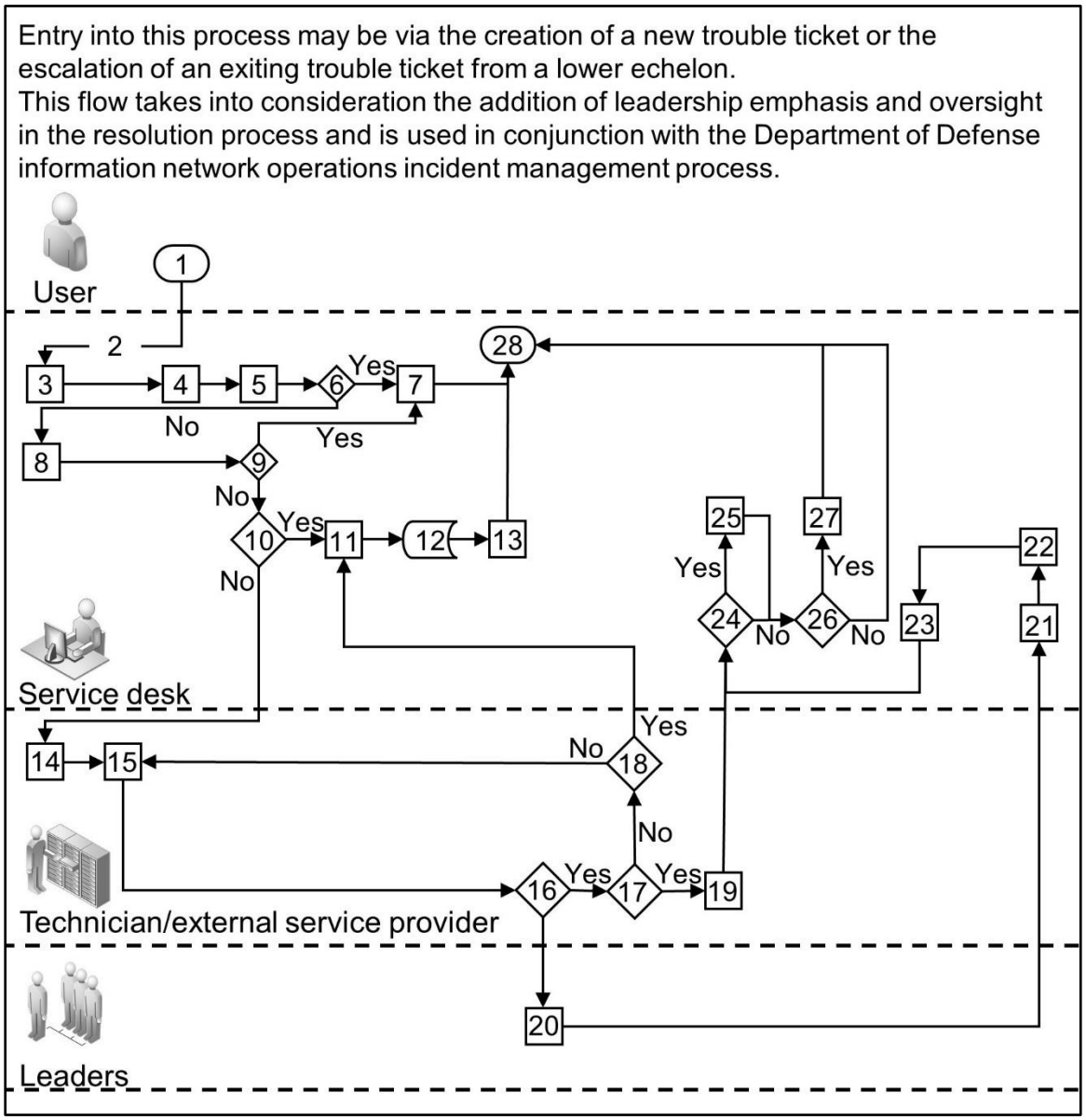

Figure D-3. Trouble ticket process

1. User initiates service desk request, incident (automated event such as device incident).
2. Walk-in, phone call, email, or web page.
3. Service desk support specialist enters incident and user information.
4. Incident is evaluated and given a priority, severity level, and ticket number.
5. Search incident in the consolidated knowledge base.
6. Is a resolution available?
7. Resolve incident.
8. Search incident in the consolidated knowledge base.
9. Is a resolution available?
10. High priority requiring immediate escalation?
11. Ticket annotated and sent to service desk for escalation.
12. Service desk notifies the user and tracks the status until incident resolved.
13. Incident resolved.
14. Ticket is assigned to a local technician and addressed based upon priority.
15. Technician troubleshoots incident.
16. Does incident need to go to leaders?
17. Incident resolved?
18. Does incident need to be escalated?
19. Ticket annotated and returned to service desk.
20. Notify leaders and receive guidance based upon the commander's critical information requirements.
21. Annotated ticket and continued as directed by leaders.
22. Service desk tracks the status until incident is resolved.
23. Incident resolved.
24. Update local knowledge base?
25. Incident and resolution information added to the local knowledge base.
26. Update consolidated knowledge base?
27. Incident and resolution information added to the consolidated knowledge base.
28. Ticket annotated, closed, and notification sent to user.

Figure D-3. Trouble ticket process (continued)

Appendix E

Common Operational Picture Coordination Cell

This appendix provides an overview of the COP coordination cell. Section I discusses the COP coordination cell. Section II illustrates a SOP for the COP coordination cell.

SECTION I – COMMON OPERATIONAL PICTURE COORDINATION CELL OVERVIEW

E-1. It is difficult to create a digital multinational force COP that seamlessly exchanges information for commanders and staffs to plan operations. The COP coordination cell overcomes these difficulties. The COP coordination cell is a group of operational and technical personnel from the multinational force led by the G-3, enabled by the G-6, and guided by knowledge management and information management plans to meet the commander's information requirements.

E-2. The COP coordination cell ensures that operational information is timely, accurate, complete, relevant, and shared to the chief of operations. It provides 24 hours a day, seven days a week monitoring of network and system links of COP exchange for the command and control information systems. The COP coordination cell—

- Confirms trends proactively in subordinate digital operational pictures and sustains systems by monitoring backend systems to facilitate the multinational force COP.
- Continuously monitors the multinational force headquarters and subordinate units' operational pictures to verify the COP is consistent across the multinational force.
- Continuously assesses the multinational force headquarters and subordinate units' operational pictures side-by-side in accordance with SOPs and the battle rhythm to verify knowledge management and information management processes and procedures.
- Confirms the multinational force headquarters and subordinate units' data integrity and secure available network connectivity to verify technical interoperability standards and procedures.
- Conducts COP coordination cell synchronization, data validation, data inconsistency battle drills, and layer discrepancy battle drills to facilitate the COP.

ARCHITECTURE AND DESIGN

E-3. Subordinate units provide operational and technical personnel with the skills, COP application, and COP management tools. These personnel enable the exchange of information and resources that resolve COP exchange issues.

E-4. The COP coordination cell physically co-locates all multinational force COP applications requiring subordinate units' network segment extensions into the multinational force headquarters command post. The multinational force G-3, G-6, information management officer, and knowledge management officer, collectively determine the location of the COP coordination cell at the multinational force headquarters command post. Units establish the COP coordination cell with, or near, the G-3 current operations integration cell.

E-5. The multinational force Multilateral Interoperability Program gateway, or other exchange mechanism, resides in the CNOSC. Figure E-1 on page E-2 shows the COP coordination cell. The multinational force headquarters manages subordinate units' connections via the applicable command and control gateway and exchange mechanism.

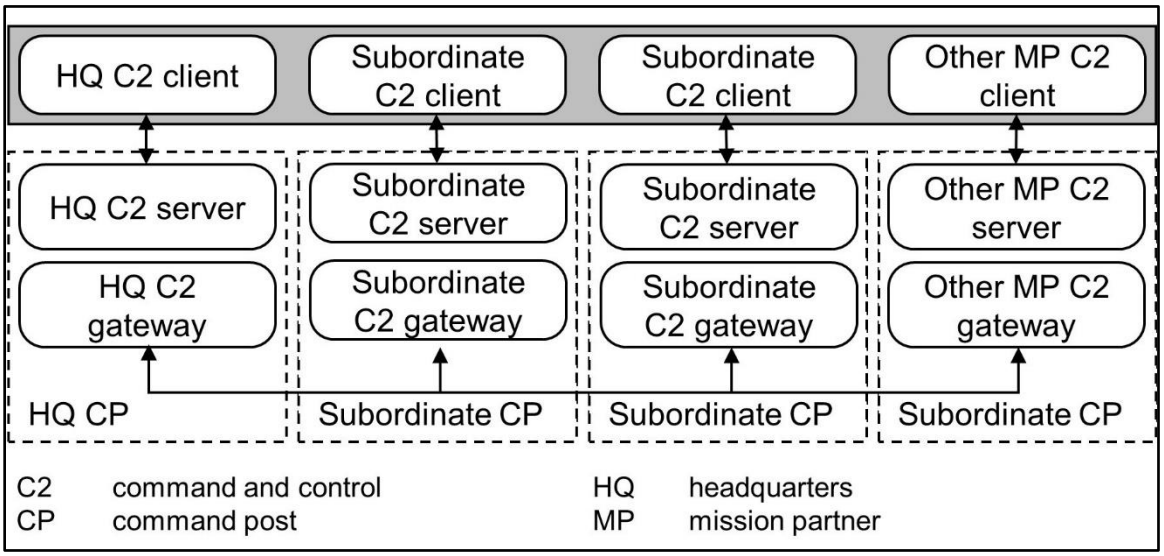

Figure E-1. Common operational picture coordination cell

PLANNING

E-6. Coalition planners have several considerations when planning for the COP coordination cell. Paragraphs E-7 through E-10 discuss these considerations.

INTEGRATION

E-7. The integration of subordinate units' operational picture systems is complex and requires active monitoring to enable a COP within the multinational force. Coalition planners consider location, manning, and equipment in the multinational planning phase and included in the JMEI to support the COP coordination cell within the multinational force headquarters command post.

INFORMATION EXCHANGE REQUIREMENTS

E-8. An *information exchange requirement* is a set of characteristics that define who exchanges what information with whom, why the information exchange is necessary, and how the information exchange must occur to support an operational process or function (JP 3-33). IERs are finalized during the multinational planning phase to completely achieve a robust MPN incorporated to confirm information flows to enable the multinational force COP.

NETWORK AND FIREWALLS

E-9. Subordinate units liaise with the multinational force G-6 engineers to introduce their network systems into the multinational force command post.

EMBEDDED PERSONNEL AND EQUIPMENT

E-10. Beyond workspace for people and equipment, planners consider who is responsible for billeting, feeding, and moving of the personnel manning the COP coordination cell. Planners also consider if there is a translator requirement for COP coordination cell personnel.

TECHNOLOGY

E-11. The COP coordination cell requires the following technology:

- COP assurance tools.
- Network monitoring tools.
- Packet inspection software.
- Command and control information systems.
- Display capability per command and control information system.

Coordination among the multinational force headquarters and subordinate units occurs to connect operational picture systems and establish a COP primary, alternate, contingency, and emergency plan.

ORGANIZATION

E-12. The COP coordination cell is organized to provide 24-hour operations. Figure E-2 shows the COP coordination cell manning.

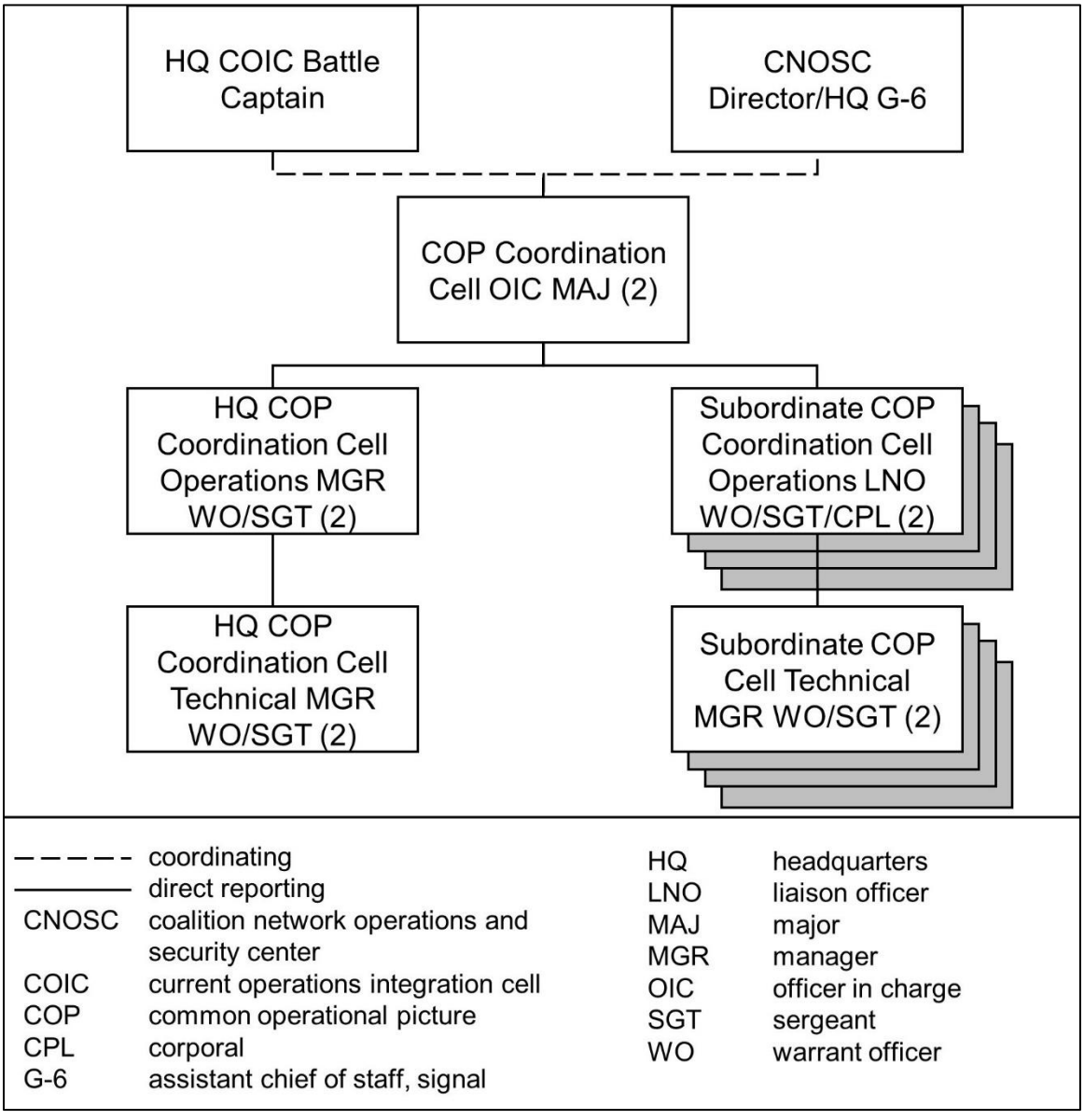

Figure E-2. Common operational picture coordination cell manning

E-13. The COP coordination cell works as a team to correct issues with the COP. When issues are operational, the COP coordination cell OIC, operations manager, and the operations LNO work with the multinational force battle captain and subordinate unit battle captain to solve the issue. When the issue is technical, the COP coordination cell OIC, technical manager, and the technical LNO work with the CNOSC director and subordinate network operations center to solve the issue.

E-14. Paragraphs E-15 through E-19 describe the billets for the COP coordination cell.

COMMON OPERATIONAL PICTURE COORDINATION CELL OFFICER IN CHARGE

E-15. The billet is provided by the multinational force headquarters or subordinate unit as agreed to during the planning phase. The OIC understands and knows how to use the multinational force command and control information system. The OIC informs and interfaces with the CNOSC, subordinate NOSCs, and commanders as necessary.

COALITION FORCE OPERATIONS MANAGER

E-16. The billet is provided by the multinational force headquarters current operations integration cell. The operations manager understands and knows how to use a multinational force command and control information system.

COALITION FORCE TECHNICAL MANAGER

E-17. The billet is provided by the multinational force headquarters G-6. The technical manager understands how the multinational force headquarters command and control information system server works, can troubleshoot, and access the server.

SUBORDINATE COMMON OPERATIONAL PICTURE COORDINATION CELL OPERATIONS LIAISON OFFICER

E-18. The operations LNO billets are provided by each subordinate unit current operations integration cell. The operations LNO understands and knows how to use the COP application and tools.

SUBORDINATE COMMON OPERATIONAL PICTURE TECHNICAL LIAISON OFFICER

E-19. The technical LNO billets are provided by each subordinate unit G-6 or S-6. The technical LNO understands and knows how their COP applications, tools, and server works and can troubleshoot and access the server.

SECTION II – COMMON OPERATIONAL PICTURE COORDINATION CELL STANDARD OPERATING PROCEDURE

E-20. This section provides an example SOP for the COP coordination cell.

OBJECTIVES

E-21. The following are the COP coordination cell objectives:

- Integrate the multinational force COP.
- Ensure integrity of COP data.
- Help achieve the commander’s trust in the COP.

BATTLE DRILLS AND STANDARD PROCEDURES

E-22. Paragraphs E-23 through E-30 outline battle rhythm events standard procedures for the COP coordination cell.

RHYTHM

E-23. The COP coordination cell battle rhythm is as follows:

- Conduct COP coordination cell synchronization on even hours.
- Conduct COP coordination cell communication status twice daily.
- Conduct COP coordination cell data validation on odd hours.

Synchronization

E-24. The following outlines the COP coordination cell synchronization:

- Ensure all maps and layers are up and displayed.
- Cross-check each common layer by nation for count, knowledge management input of priority layers.
- Cross-check common layers to include—
  - Routes.
  - Objectives.
  - Fire support control measures.
  - Phase lines.
  - Air space control measures.
  - Obstacles.
  - Significant activities (2-way sharing).
  - Command post locations.
  - Friendly units.
- Note deviations under each display and—
  - Resolve deviations.
  - Mark issue complete.

E-25. Record COP coordination cell synchronization on "COP Coordination Cell Layer Sync Slant Report" and send report to G-3, CNOSC, and knowledge management officer.

Communications Status

E-26. Record communications status and send to the CNOSC twice daily.

Data Validation

E-27. The following should be accounted for when validating data:

- Perform time synchronization or time hack to match present time on server with present time on systems.
- Confirm data is in correct layer.
- Note last update time for position location information.

BATTLE DRILLS

E-28. Paragraphs E-29 and E-30 are the battle drills for the COP coordination cell.

Layer Discrepancy

E-29. The following are steps in the layer discrepancy battle drill:

- Identify a layer that is blank, duplicate, or stale.
- Confirm layer status with the command post operations or input from user or author.
- Note COP coordination cell changes or deleted layer.

Data Inconsistency

E-30. The following are steps in the data inconsistency battle drill:

- Identify inconsistencies.
- Mark or document under display (issue, layer, time, or fix owner).
- Track until complete.

COMMON OPERATIONAL PICTURE COORDINATION CELL LAYOUT AND EQUIPMENT

E-31. Figure E-3 is the recommended layout and equipment for the COP coordination cell.

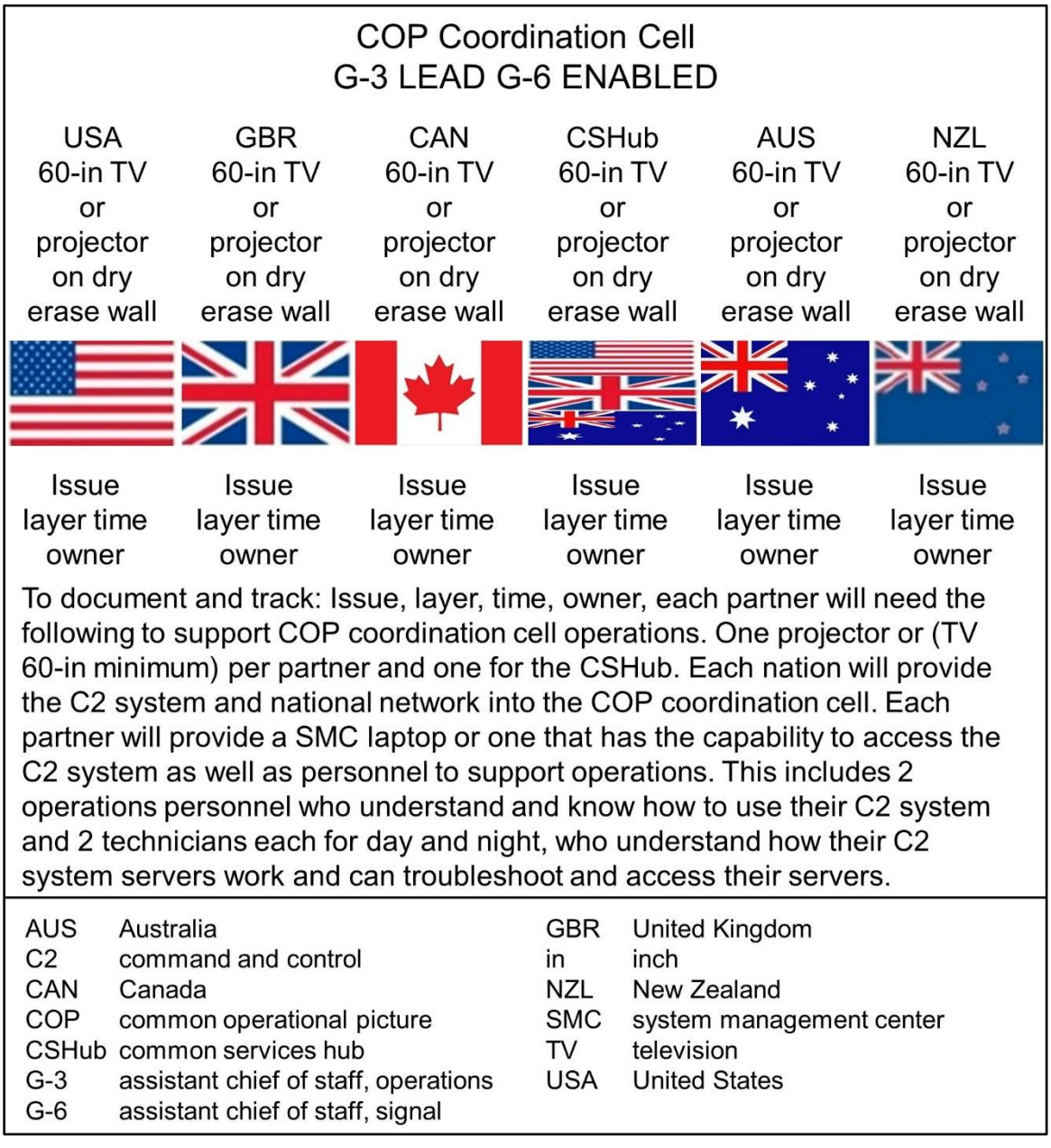

Figure E-3. Proposed common operational picture coordination cell layout

This page intentionally left blank.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. The proponent publication for terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ABCANZ	American, British, Canadian, Australian, and New Zealand
ADP	Army doctrine publication
ATP	Army techniques publication
CNOSC	coalition network operations and security center
COMSEC	communications security
COP	common operational picture
CSHub	common services hub
DA	Department of the Army
DODI	Department of Defense instruction
DODIN	Department of Defense information network
FM	field manual
G-3	assistant chief of staff, operations
G-6	assistant chief of staff, signal
IER	information exchange requirement
JMEI	joining, membership, and exiting instructions
JP	joint publication
LNO	liaison officer
MPE	mission partner environment
MPN	mission partner network
NIST	National Institute of Standards and Technology
NOSC	network operations and security center
OIC	officer in charge
Pam	pamphlet
P-ISSM	program information systems security manager
S-6	brigade or battalion signal staff officer
SATCOM	satellite communications
SMO	spectrum management operations
SOP	standard operating procedures
U.S.	United States
VTC	video teleconference
WAN	wide area network

SECTION II – TERMS

common operational picture

(Army) A display of relevant information within a commander's area of interest tailored to the user's requirements and based on common data and information shared by more than one command. (ADP 6-0)

Department of Defense information network operations

Operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense information network. (JP 3-12)

information exchange requirement

A set of characteristics that define who exchanges what information with whom, why the information exchange is necessary, and how the information exchange must occur to support an operational process or function. (JP 3-33)

spectrum management operations

The interrelated functions of spectrum management, frequency assignment, host nation coordination, and policy that together enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations. (FM 6-02)

References

All URLs accessed on 5 July 2023.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

ATP 6-02.62. *Expeditionary Mission Partner Network Techniques for Joining, Membership, and Exiting Instructions*. 06 December 2023.

DOD Dictionary of Military and Associated Terms. 15 September 2023.

FM 1-02.1. *Operational Terms*. 09 March 2021.

RELATED PUBLICATIONS

This publication cites these documents that contain relevant supplemental information.

JOINT PUBLICATIONS

Most joint publications are available at https://www.jcs.mil/Doctrine/.

DODI 8110.01. *Mission Partner Environment Information Sharing Capability Implementation for the DOD.* 30 June 2021.

JP 3-12. *Joint Cyberspace Operations*. 19 December 2022.

JP 3-33. *Joint Force Headquarters.* 09 June 2022.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online at https://armypubs.army.mil/.

ADP 1. *The Army*. 31 July 2019.

ADP 3-0. *Operations*. 31 July 2019.

ADP 6-0. *Mission Command: Command and Control of Army Forces*. 31 July 2019.

ATP 6-02.12. *Department of Defense Information Network-Army Planning Techniques.* 17 November 2021.

ATP 6-02.60. *Tactical Networking Techniques for Corps and Below*. 09 August 2019.

ATP 6-02.70. *Techniques for Spectrum Management Operations.* 16 October 2019.

DA Pam 25-2-1. *Army Cross Domain Solution and Data Transfer Management*. 12 April 2019.

DA Pam 25-2-14. *Risk Management Framework for Army Information Technology.* 08 April 2019.

FM 3-0. *Operations*. 01 October 2022.

FM 3-16. *The Army in Multinational Operations*. 08 April 2014.

FM 6-02. *Signal Support to Operations.* 13 September 2019.

FM 6-27/MCTP 11-10C. *The Commander's Handbook on the Law of Land Warfare.* 07 August 2019.

OTHER PUBLICATIONS

Most ABCANZ publications are available online at https://www.apan.org/. Most NIST publications are available online at https://www.nist.gov/.

ABCANZ Publication 332 Edition 7. *Coalition Operations Handbook*. 15 September 2021.

ABCANZ Standard 2100 Edition 4. *ABCANZ Coalition Wide Area Network and Network Operations Policy and Planning Standard*. 07 January 2020.

ISO/IEC 20000-1. *Information Technology–Service Management–Part 1: Service Management System Requirements.* 2018. Available online at https://www.iso.org/standard/70636.html.

NIST *Cybersecurity Framework*, version 1.1. 16 April 2018.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA Forms are available on the Army Publishing Directorate (APD) website: https://armypubs.army.mil.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

Index

Entries are by paragraph number.

Entries are by paragraph number.

Entries are by paragraph number.

T–U

V

W–X–Y–Z

This page intentionally left blank.

ATP 6-02.61
06 December 2023

By Order of the Secretary of the Army:

RANDY A. GEORGE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant
to the Secretary of the Army
2332101

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve. Distributed in electronic media only(EMO).

This page intentionally left blank.

PIN: 216605-000