Multinational Capability Development Campaign

Multinational Multi-Domain Command and Control Interoperability

MCDC December 2024

MCDC
Multinational Capability Development Campaign

Multinational Multi-Domain Command and Control Interoperability

dated December 2024

Disclaimer

This document was developed and written by the contributing nations and organizations of the Multinational Capability Development Campaign (MCDC) program community of interest. It does not necessarily reflect the views or opinions of any single nation or organization but provide recommended actions to be considered by nations and other entities. Contributor nations and organizations to this report are Australia, Austria, Canada, NATO Command and Control Centre of Excellence, Denmark, European Union – European Defence Agency, France, Germany, Italy, Joint Air Power Centre of Excellence, NATO ACT Headquarters, Netherlands, Norway, Poland, Romania, Spain, Sweden, Switzerland, United Kingdom Defence Futures, and the United States.

About

The Multinational Capability Development Campaign (MCDC) is an initiative led the by the United States Joint Staff J-7 that is designed to develop and assess non-materiel (non-weaponry) force development solutions. Developmental projects are selected and executed through collaborative multinational efforts to address current and future operational needs associated with joint multinational and coalition operations. It contributes to multinational interoperability by identifying and evaluating potential solution options on joint multinational and coalition capability gaps.

The MCDC partner-centric approach enables the teaming of a broad scope of multinational subject matter experts focused on multinational force development solution options. Contributing members can invite representatives from their national networks of public, private, and academic institutions as well as functional expertise from other centers of excellence and communities of interest.

For questions or comments contact: MCDC_Secretariat@APAN.ORG

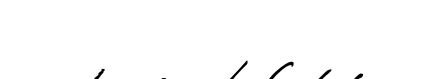
Copyright

Foreword

This report is the product of the Multinational Multi-Domain Command and Control Interoperability Project Team. The Team compiled, analyzed, and prioritized command and control (C2) modernization actions that are key for improving multinational multi-domain C2 interoperability. As part of this effort, the Team identified two modernization themes: digital transformation and readiness to participate in an event-specific federation of mission networks. These themes are foundational for improving information sharing capabilities as well as optimizing operational interoperability in a future coalition.

Overall, this project is part of the ongoing Joint Staff J-7 Multinational Capability Development Campaign to accelerate the development and implementation of capabilities interoperability among nations and partners.

Target audiences of this report are both the strategic decision-making level within national defence ministries and the national operational level that is focused on implementing C2 modernization. The report provides useful clarity for nations working to modernize their C2 capabilities and improve their ability to interoperate in the multinational multi-domain environment. It synthesizes the vast amount of information on C2 modernization into succinct and focused actionable recommendations. Nations can consider these recommendations for modernizing their national C2 capabilities and improving their ability to interoperate in the multinational multi-domain environment.



Stuart A. Whitehead, SES

Deputy Director for Command, Control, Communications and Computers/Cyber

Peter G. Bailey, Maj Gen, USAF

Deputy Director, Joint Warfighting Development

Executive summary

The specific output of this report is a prioritized listing of command and control (C2) modernization actions that will directly improve multinational multi-domain C2 interoperability. This report is targeted to both the strategic decision-making level within national defence ministries and the national operational level responsible for C2 modernization.

Challenges in the global security environment include dramatic increases in the volume of data and information and the associated handling/management problems, increased malign activity by adversaries throughout the continuum of competition, and introduction of disruptive technologies to existing C2 processes and procedures. To respond to these challenges, nations are modernizing their military capabilities and improving multinational multi-domain C2 interoperability as a critical enabler for future operational success.

As nations modernize, a significant challenge is understanding which C2 capability improvements will generate the greatest benefit for delivering C2 interoperability in future coalition operations. The report asserts that digital transformation and readiness to participate in an event-specific federation of mission networks are the two foundational themes for improving C2 interoperability. The report also provides prioritized developmental actions for nations to undertake when working to improve national C2 capabilities. Actions are grouped into four categories: technology (15 actions), structures (6 actions), people (5 actions) and processes (8 actions).

Multinational multi-domain C2 interoperability is described as the combined ability of nations to consult, coordinate, and collaborate in exercising authorities and orchestrating operations in multiple domains. Interoperable multinational C2 capabilities are needed to improve multinational data and information sharing, broaden shared situational awareness capacities and enable coherent coalition planning processes with other instruments of power.

In addition to the foundational themes, five tenets of C2 capabilities development and implementation are provided to guide national efforts and strengthen multinational coherence. They are: prioritize human performance enhancement; implement data-centric information sharing; ensure C2 resilience; posture for organizational adaptability; and monitor and incorporate technological advances.

The C2 modernization actions provide a basis for aligning C2 capabilities and are intended to facilitate achievement of the following desired operational outcomes: assured information and decision advantage; force resilience; enhanced human performance; integrated multinational targeting and fires proficiency; effective multinational planning competencies, and operational alignment in military functional areas.

Recommendations from this paper are:

- nations rapidly implement the C2 interoperability actions identified in this report;

- nations prioritize national C2 modernization in accordance with the North Atlantic Treaty Organization (NATO) standardization agreements and Federated Mission Networking spiral specifications/procedures; and

- nations prioritize C2 education and training for personnel/ leadership in accordance with NATO guidance to effectively prepare for participation in coalition operations.

Contents

Challenges in the global security environment place a premium on a coalition's ability to gain and hold information and decision advantage over adversaries throughout the continuum of competition.

Section 1 – Introduction

Challenges to achieving multinational multi-domain command and control

1. Challenges in the global security environment[1] place a premium on a coalition's ability to gain and hold information and decision advantage over adversaries throughout the continuum of competition. To assure information superiority, nations are pursuing a wide array of command and control (C2) modernization initiatives. Given the expectation that nations will be operating alongside partners in the future operational environment, a critical feature of these C2 modernization initiatives is their interoperability in a multinational multi-domain coalition force. The scope of effort to modernize C2 includes all operational domains (land, air, maritime, space, cyberspace), military functional areas, the effects dimensions, adversary actions/capability improvements, the impacts of enabling/emerging technologies,[2] and the retrofit conformance of legacy C2 capabilities (see Figure 1). This vast scope of effort is a significant obstacle for resource-constrained nations trying to improve their C2 interoperability.

1 Such challenges include: near peer adversaries' use of technologically advanced capabilities that match or exceed existing friendly capabilities; continued voluminous increase of data and information in the operational battlespace; and emergence of new technologies with potential to radically modify data and information processing, mission planning workflows, and multi-domain interactions. Detailed descriptions of the future multinational multi-domain operating environment are available in numerous documents, including the Multinational Capability Development Campaign (MCDC) report on *Multi-Domain Multinational Understanding*, November 2022, and the *Alliance Concept for Multi-Domain Operations*, 10 March 2023.

2 Technologies include: artificial intelligence/machine learning; multi/zero-trust networks; software defined networking; quantum computing; identity, credential and access management (ICAM); cloud computing and edge computing.

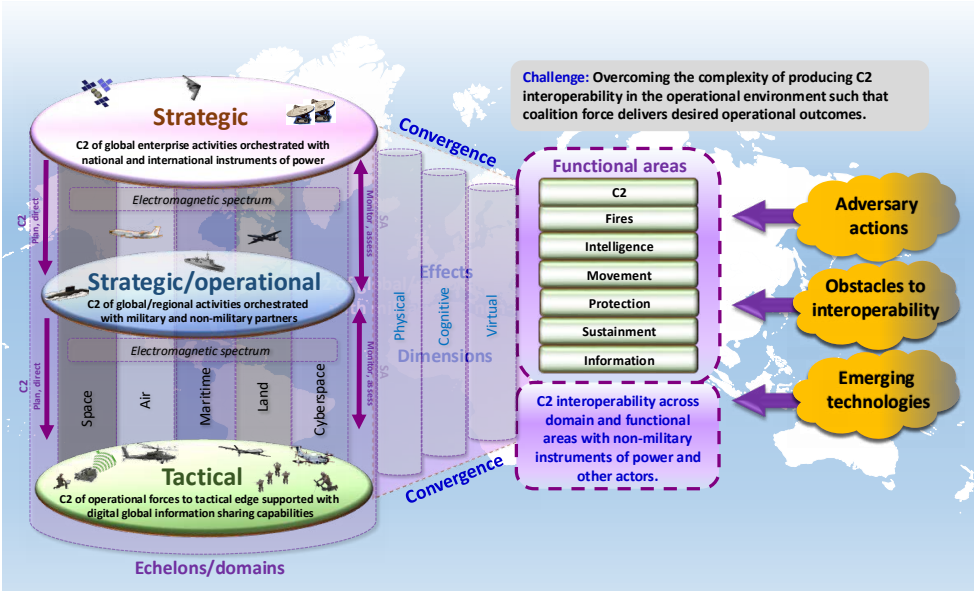


Figure 1 – Multinational multi-domain command and control interoperability

2. To address these challenges, nations are constantly balancing resource allocation options to maximize the operational benefit to their forces and simultaneously improve operational interoperability. In doing this, nations deliver a variety of capability proficiencies and varying degrees of interoperability throughout the operational domains and functional areas. These efforts to improve national forces' competencies and multinational interoperability are further complicated by rapid changes in the methods and technical specifications of data and information sharing.

Purpose

3. Provide the nations a prioritized list of C2 modernization actions to improve national C2 capabilities optimized for multinational multi-domain C2 interoperability. These actions are presented in this report.

Audience

4. Target audiences for this report are both the strategic decision-making level within national defence ministries and the national operational level that is focused on implementing C2 modernization.

Desired outcomes

5. The desired operational outcomes from this focused effort to improve multinational multi-domain C2 includes: assured information and decision advantage; force resilience; enhanced human performance; integrated multinational targeting and fires proficiency; effective multinational planning competencies, and operational alignment in military functional areas.

Alignment with other multinational multi-domain command and control improvement initiatives

6. C2 interoperability is an essential enabler for a multinational multi-domain coalition force, and most nations are modernizing their C2 capabilities to improve their C2 interoperability. Examples include the United Sates (US) Combined Joint All-Domain Command and Control (CJADC2) initiative, the UK campaign advantage, the French C2 InterArmées (C2IA) initiative, the German pCloudBw initiative, the Norwegian Militaer anvendelse av skytjenester (MAST)/Mime program, the Swiss Working Group of International Cooperation and Revision of C2 Documents, the Spanish Sistema de Mondo y Control (SC2N) and the Swedish Initiative for adaptation to the North Atlantic Treaty Organization (NATO).

7. Additionally, the C2 interoperability modernization approach described in this paper aligns with standing multinational efforts (for example, the European Union's European Defence Operational Collaborative Cloud (EDOCC), NATO's multi-domain operations (MDO) concept, and the federated mission networking (FMN)[3] initiative). These initiatives emphasize the importance of multi-domain interoperability that includes

3 FMN is a standardization framework designed to enhance information sharing and interoperability among NATO and like-minded nations. It provides common standards, specifications, processes and procedures with the aim of improving multinational interoperability.

whole-of-government coordination and activities throughout the full spectrum of the competition continuum. The recommended modernization actions in this paper are applicable to global coalitions.

Key terms

8. Whilst a full listing of terms, descriptions and definitions is at Annex A, the following lexicon is core to understanding the context of multinational multi-domain C2 interoperability.

a. **Command and control.** The authority, responsibilities, and activities of military commanders in the direction and coordination of military forces as well as the implementation of orders related to the execution of operations. (NATOTerm). As the means for orchestrating and controlling forces, C2 is an activity that occurs in every operational domain and functional area. Executing C2 involves all the systems, tools, procedures and structures that support a commander's information management and decision-making.

b. **Event-specific federation of mission networks.** The unified information network supporting an expeditionary and/or mission-focused coalition force.

c. **Federated mission networking.** FMN is the primary forum for agreeing common specifications, processes and procedures for standardizing multinational multi-domain C2.

d. **Multi-domain.** The condition where two or more domains interact with one another. The scale of interaction can be high (for example, NATO defines MDO as: the orchestration of military activities across all operational domains and environments, synchronized with non-military activities to enable the Alliance to create converging effects at the speed of relevance) or low (for example, establishment of multi-domain communications to assure force deconfliction in an operational environment).

e. **The West.** A legacy term-of-art that refers to the NATO Alliance and like-minded nations with shared governance ideals and support for a freedom-oriented rules-based international order.

Section 2 – Themes for improving command and control interoperability

9. The two overarching themes for improving multinational multi-domain C2 interoperability are:

- the use of digital transformation[4] approaches and technologies to improve information sharing, shared situational awareness and better/faster decision-making; and
- the readiness to participate in an event-specific federation of mission networks.

10. These themes are foundational for building multinational multi-domain C2 interoperability and they address the core challenges of improving C2 in the challenging arena of multi-domain operations. As depicted in Figure 2, these themes are useful for prioritizing and guiding national C2 modernization efforts.

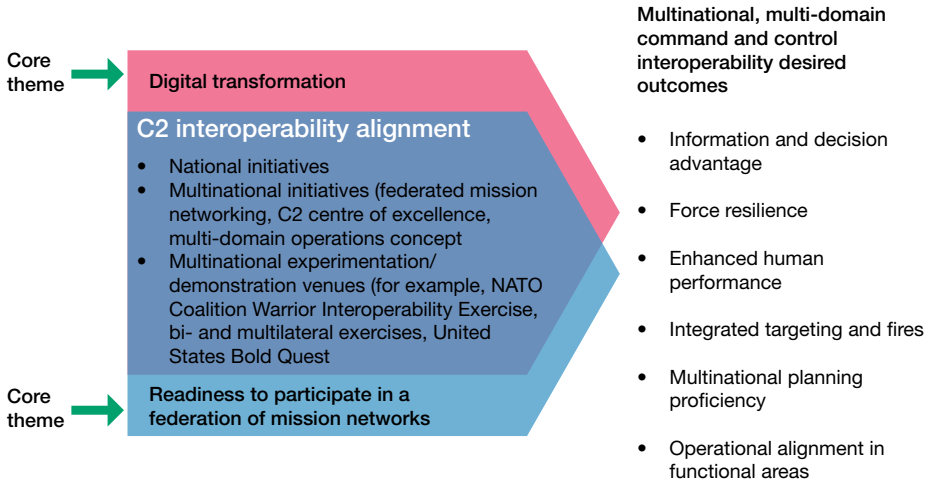


Figure 2 – Prioritizing command and control interoperability modernization

4 Digital transformation includes NATO and national data-centric approaches.

Digital transformation

11. This theme refers to the modernization, optimization and innovation of information technology using data-centric approaches for improving operational information sharing and the use of data-centric security to protect data and information. Digital transformation is a shift from 'network-centric' to 'data-centric' methodologies, and this shift is expected to yield improved information management and sharing abilities between nations and partners, thus ensuring effective multinational multi-domain C2 interoperability.[5]

Readiness to participate in an event-specific federation of mission networks

12. This theme refers to the information sharing capability used to execute C2 of a coalition force, as depicted in Figure 3.[6] Effective orchestration of activities in the multinational multi-domain environment is an aimpoint for all C2 modernization efforts. This is characterized by strengthening a coalition's operational reach and effectiveness, the ability of nations to more readily leverage collective resources to support mission objectives, and an improved collective ability to harmonize planning and decision-making processes.

5 NATO's digital transformation includes the NATO Digital Backbone (NDBB) which is the foundational initiative to accelerate effective information sharing across the Alliance. NDBB reference architecture is the guide for capability integration and sets standards for establishing mission networks including the aspiration of 'day zero' capabilities.

6 Effective coalition operations require coherent and unified C2 that is provided using a federation of mission networks to manage coalition information, planning processes and decision-making. A variety of multinational information sharing networks exist today and are represented as 'enterprise' information networks. A dedicated coalition information network is represented as 'event-specific'. Of note, the mission network is agnostic to the organizational structure/hierarchy used in a coalition headquarters. Unifying national C2 capabilities into an event-specific network will be facilitated through use of FMN standards, specifications, processes and procedures, and also the use of joining, membership and exit Instructions.

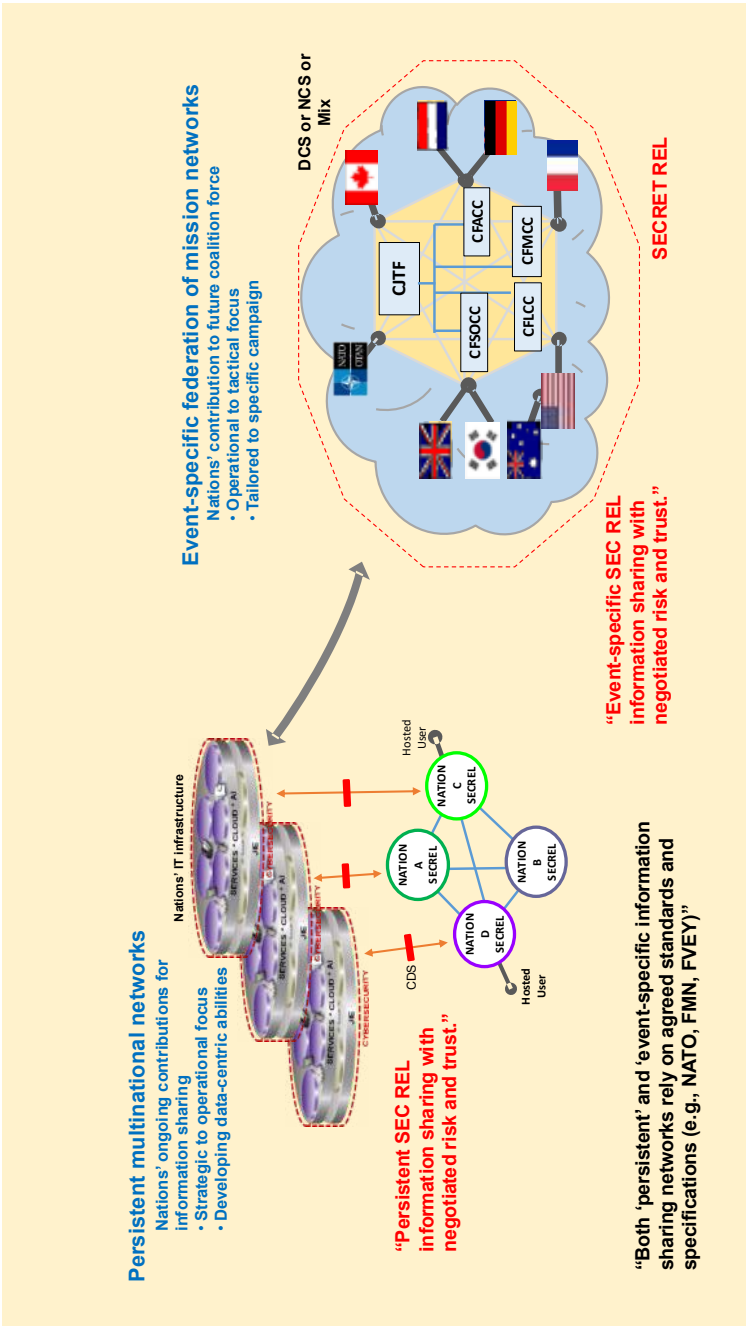


Figure 3 – Aimpoint: rapid integration of command and control capabilities within an event-specific federation of mission networks

13. When formed, an event-specific federation of mission networks integrates multiple national participants possessing different information technology standards, specifications and procedures. The primary means for establishing common approaches and technical means to enable multinational multi-domain information exchange interoperability is the FMN forum.[7] FMN promulgates Service and procedural instructions within time-bound spirals of development that define the common basis for operational interoperability. The idea of developing common standards/specifications/procedures is not new: in addition to FMN, there are numerous ongoing initiatives by nations and NATO to improve capabilities interoperability and thereby be more prepared to join a future mission network.

14. Experience shows that mission partners will 'plug-in' their force contributions into the mission network either by federating directly into the network or by being 'hosted'. There are some realities about C2 in multinational coalitions that constrain the tempo and degree of achieving interoperability: nations will retain authority[8] over the employment of their forces, will often place caveats on their use and will require clear lines of accountability; nations will bring to the coalition varying levels of C2 interoperability that will directly impact their employment options; the 'framework' mission network[9] used to support the coalition is unknown until such time the coalition activates. This unknown extends to operations planning processes, connectivity requirements/methodologies and information sharing protocols (for example, presence/type of common semantic reference model, application programming interfaces (API's), data catalogues, data services and cloud services).

7 To aid in aligning national planning processes and tools, FMN identifies four 'environments' of activity (verification and validation, collective training, operations planning and mission execution) wherein preparations must occur for the alignment of processes in coalition operations.

8 In addition to national caveats, a coalition force defines its C2 through use of agreed authorities, as expressed by type of authority/control (for example, operational command (OPCOM), operational control (OPCON), tactical command (TACOM), tactical control (TACON) and coordinating authority).

9 'Framework' nation or entity refers to the establishing entity of an event-specific mission network. This will usually be a nation or multinational entity (for example, NATO) with the ready capabilities/capacities to build a mission network.

15. These realities about a future coalition federation of mission networks make it very difficult for nations to know which preparations are best suited to deliver optimal C2 interoperability. A productive way to assess the value of capability investments is to continuously engage with other nations through C2 experimentation, exercises, demonstrations and operational deployments. Such an approach continuously aligns standards, specifications, processes and procedures, and will result in nations being more readily postured to participate in an event-specific federation of mission networks.

Section 3 – Multinational multi-domain command and control interoperability tenets

16. In addition to the two overarching themes of C2 capabilities interoperability development, the five main tenets listed below will aid nations in establishing common modernization outcomes.

a. Prioritize human performance enhancement. Nations should carefully assess the potential impact on human performance aspects of any C2 capability improvement.

b. Implement data-centric information sharing. Nations should strive to consistently adopt emerging data-centric approaches, 'need-to-share' policies, and standards into national information management systems and technologies.

c. Ensure command and control resilience. Nations should prioritize operational resilience in their C2 modernization work. This tenet assumes multiple threats (such as, contested electromagnetic spectrum and malign cyber activity) where alternative and duplicative information sharing methods/capabilities are a routine feature in the C2 suite of capabilities.

d. Posture for organizational adaptability. Nations should be prepared to adapt their organizational structures and processes to continuously improve both the 'authority to direct' and the 'actions to control'.

e. **Monitor and incorporate technological advances.** Nations should ensure application of enabling/emerging technologies to accelerate C2 interoperability.

Section 4 – Command and control interoperability modernization actions

17. C2 capabilities modernization initiatives are occurring throughout the nations in every domain, functional area, and across organizational boundaries. This paper focuses on initiatives that are core for improving multinational multi-domain C2 interoperability. The following lists, grouped into categories[10] of technology, structures, people and processes are essential actions for nations to consider and prioritize.

Technology

18. The shift to a data-centric approach prioritizes data as an asset in an information system and strives to make it simultaneously visible, accessible, understandable, linked, trustworthy, interoperable and secure.[11] In a data-centric approach, data is often stored in a single place or system and then accessed or delivered to various applications, rather than being duplicated and stored in each application. This 'ubiquity' of data access and movement can improve data quality, consistency and security.

10 These categories of interrelated activities that compose command and control as a function are identified and succinctly explained in the UK Ministry of Defence's Joint Concept Note 2/17, *Future of Command and Control*, September 2017.

11 These descriptive features of data management, summarized in acronym VAULTIS, are used by the US Department of Defense Chief Information Officer to guide data management policies and modernization implementation.

19. Nations seeking to improve their C2 interoperability in a multinational multi-domain environment should undertake the actions listed in the following tables.

Digital transformation (technology)	Readiness to participate in a federation of mission networks (technology)
T1 – Contribute to and implement emerging data-centric standards in communication and information systems (CIS)/information technology/C2 capabilities.[12] [To implement data centricity, nations must increase their conformance to common standards and specifications]. **T1.1 – Engage with multinational fora (for example, NATO, FMN) to establish common metadata.** [Standardized metadata on information products is an important element for making data shareable within a multinational multi-domain environment]. **T1.2 – Employ enterprise and community-of-interest semantic reference models and harmonize with multinational models for example, NATO's Common Cross Community-of-Interest Semantic Reference Model (CXCSRM).** [Semantic reference models are foundational for ensuring understanding between national and multinational information networks].	**T2 – Develop and implement an operational deployable CIS capability using standards and specifications detailed in FMN spirals.** [This action is focused on national preparation for participation in an event-specific federated mission network and includes the specific task of modernizing/converging SECRET-level information technology infrastructure]. As a minimum, nations should possess the six 'core services' identified in FMN Spiral 3: secure video teleconferencing (SVTC), VTC over IP, secure voice over IP (SVOIP), email with attachments, global address sharing, chat, and web browsing].

12 NATO interoperability standards and profiles, governed by NATO's Digital Policy Committee (DPC) Interoperability Profiles Capability Team (IPCaT), establishes mandatory interoperability standards and profiles for CIS in NATO, as well as candidate standards and profiles. Once approved as Allied Data Publication (ADatP)-34, *NATO Interoperability Standards and Profiles*, these standards and profiles are publicly available and continuously updated with new versions.

Digital transformation (technology)	Readiness to participate in a federation of mission networks (technology)
T1.3 – Establish and use common enterprise and mission data catalogues. [Commonly accessible data catalogues provide a means for improving staff planning and operations execution by enabling permitted access to national data].	
T1.4 – Agree on standard application programming interface (API) convergence templates. [API's provide software-to-software connectivity between respective national information systems/networks].	
T1.5 – Align with/incorporate data management services to support automated machine-to-machine multinational multi-domain information sharing. [Providing data services is already a function of all information systems/networks, but this initiative unites such services with the aim of enabling continuous data/information access and use].	
T3 – Adapt national legacy information systems to data-centric standards and specifications. [Existing C2 systems, infrastructure and processes use legacy capabilities and must be modernized to conform to data-centric standards and specifications (for example, positioning, navigation and timing services, common intelligence picture, and common operational picture)].	**T4 – Within national operational domains and functional areas, develop and implement modernized highly mobile communications capabilities in compliance to FMN spiral evolution.**

Digital transformation (technology)	Readiness to participate in a federation of mission networks (technology)
T5 – Pursue and adapt common technical standards and specifications for using cloud services for data and information management. [The introduction of cloud-native architectures is producing significant benefits to nations, including improved availability/access of information, cloud native security, application of artificial intelligence and machine learning capabilities, improved monitoring of data accessibility and use, elastic storage and compute capacities, and agile C2 service improvement. Future persistent multinational mission networks and event-specific mission networks will employ cloud services. This technological service is still formative in NATO and the nations but is expected to become a standard feature enabling C2 interoperability. Cloud-native architecture is an approach to designing and building applications that fully exploit the benefits of cloud computing. It involves using microservices, containers, development operations (DevOps) practices, and scalable infrastructure to create applications that are flexible, resilient and easily scalable].	T6 – Leverage enabling/emerging technologies (such as, artificial intelligence/machine learning) to support rapid federation of mission networks.

20. Actions T7–T9 specifically address the protection of data and information. Data-centric security is an approach that emphasizes the security of the data itself and the importance of individual identification, rather than the security of networks, servers or applications. This approach involves encrypting data at rest and in transit, managing access controls and consistently monitoring data activity to detect suspicious behaviour. The main goal is to protect data wherever it is stored or travels, ensuring that even if a breach occurs it remains inaccessible and unusable to unauthorized individuals. This approach is becoming increasingly important with the rise of cloud computing, mobile access and distributed systems where data is mobile across various locations and devices.

21. Data-centric security enables the application of automated and dynamic user attribute access and release controls that restricts access based on credentialed identity characteristics. It also minimizes the number of operational networks needed to support operational C2 and reduces the time it takes to transmit information from one federated network to another.

Digital transformation (technology)	Readiness to participate in a federation of mission networks (technology)
T7 – Establish common zero trust policy guidance, governance approaches, and methods, processes and procedures. [Zero trust is a security concept that requires all users and all information technology services, even those inside the organization's enterprise network, to be authenticated, authorized, and continuously validated before being granted or keeping access to applications and data. Key elements of a zero trust approach include: identity verification, micro-segmentation, least privilege access, multi-factor authentication, continuous monitoring and security automation. This action is complemented with simultaneous efforts to prioritize policy guidance stipulating increased willingness to share information with mission partners].	T7 – Establish common zero trust policy guidance, governance approaches, and methods, processes, and procedures. [Zero Trust is a security concept that requires all users and all information technology services, even those inside the organization's enterprise network, to be authenticated, authorized, and continuously validated before being granted or keeping access to applications and data. Key elements of a zero trust approach include: identity verification, micro-segmentation, least privilege access, multi-factor authentication, continuous monitoring and security automation. This action is complemented with simultaneous efforts to prioritize policy guidance stipulating increased willingness to share information with mission partners].
T8 – Establish common identity, credential and access management (ICAM) policies, methods, processes,and procedures in compliance with emerging standards.	T8 – Establish common ICAM policies, methods, processes and procedures in compliance with emerging standards.
T9 – Employ common attribute-based access control (ABAC) policies, methods, processes,and procedures.	T9 – Employ common ABAC policies, methods, processes and procedures.

Digital transformation (technology)	Readiness to participate in a federation of mission networks (technology)
T10 – Produce C2 reference architecture and design architecture documents. [C2 reference and design architecture documents contain detailed listings and descriptions of C2 capability systems, networks, functions and operational dependencies. These documents enable a systematic analysis of C2 capabilities, and the technical actions required to create interoperability between different systems and networks].	

Structures

22. Coalition C2 in a federation of mission networks traditionally relies on hierarchical and organizational structures that group military functions (for example, intelligence, operations, logistics, policy or C2) and facilitate information flows to the force commander. The application of C2 interoperability improvements to existing planning procedures and processes holds the promise of improving the speed and accuracy of information flow into and through the processes, and possibly altering the organizational relationships that support planning and execution.

23. Readers of this publication have likely witnessed both 'bottom-up' and 'top-down' organizational change as their organizations adjust to changes in functional abilities. Nations seeking to improve their C2 interoperability in a multinational multi-domain environment should adapt their structures as needed to develop and refine their C2 interoperability capabilities.

24. Specific actions to support C2 interoperability within national and international structures are described in the following table.

Digital transformation (structures)	Readiness to participate in a federation of mission networks (structures)
S1 – Establish a national high-level organization that can engage at the strategic and operational levels with multinational multi-domain experimentation/demonstration/exercise activities.	S2 – Continuously prepare national high readiness forces for C2 integration into an event-specific federated mission network.
S3 – Create a standing information technology service management organization that accrues and maintains proficiency in supporting C2 interoperability within enterprise and expeditionary information sharing infrastructures.	S3 – Create a standing information technology service management organization that accrues and maintains proficiency in supporting C2 interoperability within enterprise and expeditionary information sharing infrastructures.
S4 – Adapt defence capabilities development, acquisition, and implementation authorities and processes to emphasize data-centric approaches.	
S5 – Embrace development security operations (DevSecOps) methodology scoped for multinational collaborative continuous integration/continuous deployment. [DevOps as a foundation for DevSecOps is the proven methodology to rapidly produce interoperability improvements].	S6 – Maintain competencies in a recognized command structure (for example, J-code).

People

25. Human performance in C2 is critical for successful execution and a reminder that the processes, structures and technology used in C2 are enablers, but not an end in themselves. The value of any C2 capability lies in how well it enables people to perform their C2 tasks and functions. Effective C2 requires personal competence, adaptability, and collaboration skills that are able to address uncertainty and respond swiftly in fluid situations. People at every level and type (for example, military/non-military) must be educated, trained,and equipped to interpret data rapidly, create congruent shared meaning and execute decisions under time pressure and uncertainty. This can be fostered by a culture of rapid and continuous learning at national and multinational levels and continuous engagement in multinational experimentation, demonstration and exercise activities.[13]

26. Future commanders will need to possess expertise in information sharing methodologies, knowledge of the impact and use of enabling/emerging technologies within their decision-making processes. Additionally, commanders must be aware of the interdependencies within and between the operational domains, functional areas and effects dimensions, as well as understanding potential barriers to interoperability caused by socio-cultural differences within a coalition force.

27. Nations seeking to improve their C2 interoperability in a multinational multi-domain environment should develop and refine their human performance proficiencies with the actions detailed in the following tables.

13 A mindset for adaptability and an expectation for multinational collaboration is a core feature of NATO's MDO concept for future operations.

Digital transformation (people)	Readiness to participate in a federation of mission networks (people)
PE1 – Pertaining to digital transformation, incorporate multinational multi-domain C2 precepts, principles, approaches and execution methodologies into national C2 approaches, frameworks, processes,and procedures. [This effort is aided with existence of numerous NATO and national training and education resources addressing multinational multi-domain C2 interoperability. Coalition members are educated, trained, and proficient in coalition mission planning and execution].	PE1 – Pertaining to participating in a federation of mission networks, incorporate multinational multi-domain C2 precepts, principles, approaches and execution methodologies into national C2 approaches, frameworks, processes and procedures. [This effort is aided with existence of numerous NATO and national training and education resources addressing multinational multi-domain C2 interoperability. Coalition members are educated, trained, and proficient in coalition mission planning and execution].
PE2 – Develop a cultural and socio-technical understanding of C2 for leaders that is tailored for the multi-domain and information driven operating environment. ['Cultural' understanding of C2 relates to cultivating an environment of trust and empowerment. 'Socio' aspects of C2 socio-technical understanding are built upon four fundamental competencies a leader must possess: knowledge, skills, experience, and qualities. 'Technical' aspects of C2 socio-technical understanding require a working familiarity with information technology and automation within multi-domain operations].	PE2 – Develop a cultural and socio-technical understanding of C2 for leaders that is tailored for the multi-domain and information driven operating environment. ['Cultural' understanding of C2 relates to cultivating an environment of trust and empowerment. 'Socio' aspects of C2 socio-technical understanding are built upon four fundamental competencies a leader must possess: knowledge, skills, experience, and qualities. 'Technical' aspects of C2 socio-technical understanding require a working familiarity with information technology and automation within multi-domain operations].

Digital transformation (people)	Readiness to participate in a federation of mission networks (people)
PE4 – Ensure that national processes and procedures enable timely verification of security clearances that are required for personnel access to coalition SECRET classified information and systems. [Recommended guidance includes NATO documents '*Security within the North Atlantic Treaty Organization*', (C-M(2002)49-REV1) Enclosure C and '*NATO Directive on Personnel Security*' (AC/35-D/2000-REV8)].	PE3 – Incorporate multinational, multi-domain C2 proficiency as a standing requirement in the performance of national and international wargaming, exercises, experimentation and demonstrations. [Each year nations have the option of participating in select multinational exercises as well as participating in annual experimentation venues such as the NATO sponsored Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX) venue, and the US hosted Bold Quest events].
PE5 – Support further multinational multi-domain C2 doctrinal development and adapt national C2 doctrinal approaches, frameworks, processes and procedures accordingly.	PE4 – Ensure that national processes and procedures enable timely verification of security clearances that are required for personnel access to coalition SECRET classified information and systems. [Recommended guidance includes NATO documents '*Security within the North Atlantic Treaty Organization*', (C-M(2002)49-REV1) Enclosure C and '*NATO Directive on Personnel Security*' (AC/35-D/2000-REV8)].

28. In addition to the traditional methods to address human performance listed above, some nations are undertaking conceptual analyses of the human factors and organizational relationships that influence sensing and decision-making within a chaotic, confused and disconnected battlespace.[14] These approaches foresee the need to blend military, civilian and academic perspectives into operational problem-solving. Although formative, these approaches for exercising C2 in a challenging future operating environment may produce new and effective C2 methodologies.

14 For example, one approach formalizes a comprehensive and collaborative information sharing environment that more readily teams the military with other instruments of national power. It uses cross-organizational methodologies, such as emergent teaming, to leverage existing organizational structures and processes into broader analysis and problem-solving solution options.

Processes

29. A constant feature of C2 is the matching of human performance competencies with the planning, execution and decision-making processes used to direct, control and orchestrate forces. Optimally, the processes efficiently enable the multinational collaboration needed to derive and direct operational actions. Emerging technologies hold great promise of accelerating analysis and decision cycles, thus providing an advantage over an adversary.

30. C2 in an event-specific federation of mission networks relies on common planning processes and tools, and operations planning processes are likely to be either NATO standard or from the coalition 'framework' nation.

31. C2 is increasingly reliant upon cloud service models. 'Cloud' does not only refer to technology, but to agile service delivery and provisioning processes with a continuous loop of develop–test–produce– deploy–operate–measure, including all military security and safety concerns, called DevSecOps. This approach improves capability development processes by readily and continuously connecting operational users and development test teams.

32. Nations seeking to improve their C2 interoperability in a multinational multi-domain environment should develop and refine their planning, execution and decision-making processes with the actions detailed in the following table.

Digital transformation (processes)	Readiness to participate in a federation of mission networks (processes)
PR1 – Participate in FMN processes and procedures.	PR1 – Participate in FMN processes and procedures.
	PR2 – Align national operations planning and execution processes with NATO planning and execution processes (as described in NATO Allied Joint Publication (AJP)-01, AJP-3) AJP-5) and the Comprehensive Operations Planning Directive (COPD). [Nations that are likely to lead a coalition headquarters should adjust their operations planning processes to align with the NATO standard].
PR3 – Optimize connectivity between intelligence/operational dashboards such as national common intelligence picture (CIP) and common operational picture (COP) capabilities and coalition mission network capabilities. [Maximize intelligence/operational information sharing policies and procedures to achieve rapid and seamless connectivity].	PR3 – Optimize connectivity between intelligence/operational dashboards such as national CIP and COP capabilities and coalition mission network capabilities. [Maximize intelligence/operational information sharing policies and procedures to achieve rapid and seamless connectivity].
PR4 – Use agile strategies for developing and implementing multinational, multi-domain C2 interoperability capabilities. [This action mitigates the costs and unknowns of producing capabilities in a rapidly changing technological environment].	PR5 – Ensure that national operational headquarters planning and execution processes can be rapidly aligned to a coalition headquarters.

Digital transformation (processes)	Readiness to participate in a federation of mission networks (processes)
PR6 – Participate in the development of governance policies/procedures that oversee use of cloud services. [Cloud governance issues address multinational agreement on a regulatory framework, organizational relationships and technical measures for mutual cloud use. Such governance is prerequisite for entities (including coalitions) to implement information technology/cloud services in support of data and information sharing requirements].	
PR7 – Adopt DevSecOps and align procedural implementation to provide for fully interoperable, agile cloud infrastructures. [This may eventually include sharing information technology services based on shared trust of both DevSecOps processes and its applications].	PR7 – Adopt DevSecOps and align procedural implementation to provide for fully interoperable, agile cloud infrastructures. [This may eventually include sharing information technology services based on shared trust of both DevSecOps processes and its applications].
PR8 – Apply process improvements resulting from the application of enabling/ emerging technological advances.	

Conclusions

33. The challenges to improve multinational multi-domain C2 interoperability are broad and complex, and delivering improved C2 interoperability requires consistent and targeted efforts. The ability to effectively command and control forces in a multinational multi-domain environment is essential for future coalition operations. All actions identified in this report will help nations improve and align multinational multi-domain C2 interoperability.

34. Effective multinational multi-domain C2 provides numerous benefits, including: assured information and decision advantage; force resilience; enhanced human performance; integrated multinational targeting and fires proficiency; effective multinational planning competencies; and operational alignment in military functional areas.

35. The method of sharing information is shifting from a network-centric approach to a data-centric approach. This shift requires a substantial commitment of national resources to develop, test and implement new methods and policies for sharing data and information, as well as the implementation of data-centric functionality into legacy information systems and networks. Implementation of data-centric security is a forcing agent to achieve digital transformation and is foundational for C2 interoperability in coalition operations.

36. The human performance factor is essential for effective and efficient multinational multi-domain C2 interoperability. The means to collect, parse and deliver information must enhance the human ability to understand and act.

37. Despite the ‘known unknowns’ of a future coalition headquarters, nations can build high levels of C2 interoperability into their forces by aligning with NATO and FMN guidance, specifications, standards, processes and procedures.

38. Continuous engagement with multinational experimentation, demonstrations and exercises is critical to develop and implement enhanced C2 interoperability.

Recommendations

- Nations rapidly implement the C2 interoperability actions identified in this report.
- Nations prioritize national C2 modernization in accordance with NATO standardization agreements and FMN Spiral specifications/ procedures.
- Nations prioritize C2 education and training for personnel/leadership in accordance with NATO guidance to effectively prepare for participation in coalition operations.

Annex A – Project lexicon

Command and control (C2) concepts can differ amongst the nations, therefore, the Multinational Multi-Domain Command and Control (M2C2) Interoperability Project Team recognized the need to agree a common lexicon. Key terms, descriptions and definitions are provided below. Note that many of these terms are specific and relevant for this publication/ project only.

Command and control

command. The authority to direct, coordinate and control. (M2C2 Project Team)

command and control. The authority, responsibilities and activities of military commanders in the direction and coordination of military forces as well as the implementation of orders related to the execution of operations. (NATOTerm)

command and control capability. The technology, people, processes, and structures essential to plan, direct and control operations of assigned and attached forces pursuant to the missions assigned. (M2C2 Project Team)

control. The act of directing, coordinating and orchestrating forces to outcomes determined by command. (M2C2 Project Team)

Organizational relationships

C2 interoperability. The ability of multiple entities to consult, cooperate, and collaborate in exercising authorities and directing/controlling/ orchestrating operations. (M2C2 Project Team)

coalition. An arrangement between two or more nations for common action. (US Department of Defense (DOD) Dictionary)

combined. A term identifying two or more forces or agencies of two or more allies operating together. (DOD Dictionary)

domain. Activities associated within a specified physical arena (for example, NATO agreed operational domains are maritime, land, air, space and cyberspace). (M2C2 Project Team)

emergent teaming. A collaborative methodology to accelerate analysis and problem-solving efforts within or alongside traditional processes/organizational structures. (M2C2 Project Team)

event-specific federation of mission networks. The unified information network supporting an expeditionary and/or mission-focused coalition force. (M2C2 Project Team)

'framework' nation or entity. Refers to the establishing entity of an event-specific mission network. This will usually be a nation or multinational entity (for example, NATO) with the ready capabilities/capacities to build a mission network. (M2C2 Project Team)

functional areas. A grouping of activities by type. (M2C2 Project Team)

interagency. Anything pertaining to the agencies and departments of a single government. (M2C2 Project Team)

joint. Anything pertaining to the military services. (M2C2 Project Team)

multi-domain. The condition where two or more domains interact with one another. (M2C2 Project Team)

Interoperability actions

cloud-native architecture. Cloud-native architecture is an approach to designing and building applications that fully exploit the benefits of cloud computing. It involves using microservices, containers, DevSecOps practices, and scalable infrastructure to create applications that are flexible, resilient and easily scalable. (M2C2 Project Team)

coherent. Logically connected/consistent. (Dictionary.com)

collaboration. The act or process of working together or cooperating. (Dictionary.com)

cooperation. Occurs when states or non-state actors work together to achieve the same objectives. (NATO AJP-01)

coordination. Harmonious combination or interaction, as of functions or parts. (Dictionary.com)

coordination. The act of making parts of something (for example, groups of people) work together in an efficient and organized way. (Oxford Dictionary)

deconfliction. The act or process of removing or preventing conflict. (Dictionary.com)

development, security and operations. A framework that integrates security into all phases of the software development life cycle. Organizations adopt this approach to reduce the risk of releasing code with security vulnerabilities. Through collaboration, automation,and transparent processes, teams share responsibility for security in development, rather than at implementation when issues are usually more difficult and costly to address. Development, security and operations (DevSecOps) is a critical component of a multi-cloud security strategy. (M2C2 Project Team)

doctrine. Fundamental principles by which military forces guide their actions in support of objectives. It is authoritative but requires judgement in application. (NATOTerm)

federated mission networking. Federated mission networking (FMN) is the primary forum for agreeing common specifications, processes and procedures for standardizing multinational multi-domain C2. (M2C2 Project Team)

harmonization. To combine or meld together. (Dictionary.com)

integrate. To combine capabilities, assets and/or methodologies. (M2C2 Project Team)

interoperability. The ability of entities to act together to achieve common objectives. (M2C2 Project Team)

- Technical Interoperability concerns systems and equipment, such as communication and information systems, and their ability to operate together. (M2C2 Project Team)

- Procedural interoperability is based on measures such as common doctrine, procedures and terminology. (M2C2 Project Team)

- Human interoperability concerns mutual trust and understanding achieved by strengthening relationships in training and on operations. (M2C2 Project Team)

metadata. Data about data. Metadata describes attributes of data or information products and is important in enabling the flow of data-centric information between different information systems/networks. (M2C2 Project Team)

orchestrate. To arrange, organize and manage activities to accomplish a common purpose, especially by means of planning or manoeuvring. (M2C2 Project Team)

Annex B – Project methodology

The Project Team examined and agreed the project objectives, refined the scope of effort and created a framework (technology, structures, people and processes) for grouping and organizing modernization actions. Derived from ongoing capability development and implementation efforts within various nations, the groupings provide a means of clarifying key improvement actions and cross-group dependencies. Additionally, the Project Team identified two C2 modernization themes:

- digital transformation; and
- readiness to participate in an event-specific federation of mission networks.

All analysis and compilation of C2 interoperability initiatives are unclassified. The Project Team agreed on a common lexicon for describing the C2 capability development and implementation environment, as well as terms pertaining to C2 interoperability in the operational environment. The Project Team identified and prioritized C2 modernization actions that are believed critical for improving multinational multi-domain C2 interoperability. These actions are already progressing in many nations, NATO and FMN, and are transforming how nations execute C2. The Project Team developed the list of C2 modernization actions with intent that nations could use the listing as a template for modernization choices and to self-assess national posture on multinational multi-domain C2 interoperability.

Notes

For more information, contact: MCDCsecretariat@apan.org