Multinational Capability Development Campaign

Multi-Domain Multinational Understanding

MCDC November 2022

Multi-Domain Multinational Understanding

dated November 2022

Authorisation

Questions or comments about this publication should be referred to MCDC Secretariat via email at: mcdc_secretariat@apan.org

Copyright

Front cover image copyright as detailed below.

Top row	© Blackboard / Shutterstock.com
	© sdecoret / Shutterstock.com
	© Kutsenko Volodymyr / Shutterstock.com
Middle row	© Art of Life / Shutterstock.com
	© Blue Planet Studio / Shutterstock.com
	© Chesky / Shutterstock.com
Bottom row	© Golden Dayz / Shutterstock.com
	© Scharfsinn / Shutterstock.com
	© UK MOD / Crown copyright

Participants and roles

Project leads: GBR and NATO/ACT

Contributing nations and organizations: AUT, CAN, CHE, DEU, DNK, ESP, FRA, HUN, ITA, KOR, NLD, POL, SWE and USA

Observer nations and organizations: EU, JPN, NOR and ROU

Executive summary

The global security environment has become increasingly complex, dynamic and uncertain. Greater numbers of state and non-state actors are competing for power and influence, often in innovative ways that defy the traditional threshold between peace and war. Rapid advances in technology, the processing, management and exploitation of information is changing the character of military operations while also increasing the requirement to synchronize with non-military activities. The people, processes and organizations which deliver these operations must evolve to ensure an integrated effort, this is being termed a 'multi-domain' approach.

This project was initiated to develop a common understanding of how military forces can maintain advantage over their adversaries in a multi-domain way.

A multinational perspective is developing, and this report helps by proposing agreeable multi-domain terms and foundational principles. The principles were conceived as adjuncts to, not replacements for, existing ideas such as the principles of war. The following principles were agreed and helped inform specific recommendations:

- shared understanding;
- unity of effort;
- dynamic posture;
- agility; and
- innovation.

In reaching this project view, 20 contributing nations and entities have referenced their own progress and this is also expected to enable further discussion around alignment and shared perspectives. Individual nation approaches can be found in Annex A, which exists outside of this report.[1]

Finally, this report closes by recommending follow-on projects to further enhance subject understanding and better preparedness to face the challenges of the global security environment.

1 Access to Annex A can be requested via email at: mcdc_secretariat@apan.org

Contents

* Both annexes are held separately to this publication. Access to Annex A and Annex B can be requested via email at: mcdc_secretariat@apan.org

> The global security environment continues to change. While there are exceptions, a key aspect is the willingness of adversaries to target national systems and assets while remaining below the threshold of armed conflict.

Introduction

1. The global security environment continues to change. While there are exceptions, a key aspect is the willingness of adversaries to target national systems and assets while remaining below the threshold of armed conflict. Nations and alliances find themselves in a constant state of adaptation to meet evolving threats and risks, such as:

- the rise of technologically advanced actors with malign intent to disrupt the existing rules-based international order and the supporting multinational security arrangements;
- the use of cyberattacks committed by both state and non-state adversaries to disrupt, damage and extort critical infrastructure;
- the inability of existing security systems to manage the exponential increases in data and information in the global security environment; and
- the increased lethality and volume of adversary weaponry and technological capabilities, including an array of emerging and disruptive technologies.

2. To successfully meet these challenges, nations and organizations are increasingly pursuing a 'multi-domain' approach. This approach seeks not only the further integration of the military instrument of power through operational domains[1] (for example, land, maritime, air, space and cyber) but also integration with the other instruments of power (diplomatic, information, economic).

3. For the purpose of this report, a multi-domain approach includes operations in a combined, joint, inter-agency, intergovernmental and multinational (CJIIM) construct.[2]

1 There are variations amongst nations of what they consider to be the operational domains. Section 4 of this report lists recognized operational domains by specific nations.

2 Similar constructs to CJIIM can be found in NATO's comprehensive approach, UK Ministry of Defence, *Integrated Operating Concept* and the United States (US), Joint Publication 3-08, *Interorganizational Cooperation*.

Project initiation statement

4. A need to develop a common understanding of how military forces can maintain advantage over their adversaries in a multi-domain way.

Objectives and aims

5. The Multinational Capability Development Campaign (MCDC), *Multi-Domain Multinational Understanding* project plan provided a number of high-level objectives and aims that are stated below.

a. The project objectives were to:

- develop a common multinational understanding of the idea of domains (working description), and describe what multi-domain means; and
- propose a set of broad foundational principles for conducting multi-domain activity.

b. The project aims to:

- lay out a common understanding and working description of multi-domain; and
- provide a foundation for developing multi-domain approaches within member nations.

c. The project does not aim to:

- define a detailed concept for multi-domain or operationalize the idea;
- define a concept for integrating the military instrument with other instruments of power; or
- detail capability solutions for multi-domain activity.

Project approach

6. The project was collaborative and maintained a loyal intent to be multinational and not champion any single nation's perspective. Thorough information sharing of national approaches was structured into the discussions; and national and organizational presentations were allocated throughout the 18-month project cycle as part of vital information exchange.

7. Perspectives of multi-domain are evolving and are reflected in the complexity of generating a common multinational perspective. To deliver a baseline of agreement across the project, the report was structured in the following way.

- Section 1 describes relevant aspects of the global security environment that are increasingly demanding cross-domain solutions.
- Section 2 introduces and explains specific terms needed to achieve understanding of multi-domain.
- Section 3 describes the principles of multi-domain.
- Section 4 provides project conclusions.
- Section 5 provides recommendations for further multi-domain study.
- Enclosure 1 is an excerpt of the NATO sponsored SAS-050 study that identified nine variables to achieving a robust level of shared understanding, one of the multi-domain principles identified in Section 3 of this report.
- Annex A has a compilation of individual national multi-domain approaches from contributor/observer nations and entities.[3]
- Annex B is the project plan and project terms of reference.[4]

3 Access to Annex A can be requested via email at: mcdc_secretariat@apan.org
4 Access to Annex B can be requested via email at: mcdc_secretariat@apan.org

> A changing character of war is creating the need for nations, partnerships and alliances to organize and operate in new adaptable ways.

Section 1 – Global security environment

8. The rules-based international order is increasingly being challenged and is causing rapid change to the global security environment. Increased ambiguity, due to various factors, is also adding opportunity for those able to exploit it. The result is often seen through state and non-state competition, which generates a mix of unpredictable threats and dilemmas for leaders. This brings greater demand for timely coordination within and between nations, across all instruments of power and specifically where the military operates. Add a changing character of warfare, and the consequence for nations, partnerships and alliances is the need to organize and operate in new adaptable ways.

9. These trends are expected to continue into the foreseeable future and reinforced the project's view to highlight two significant cross-cutting themes. The first is the pursuit of 'advantage' by an entity within the context of competition and the second is the demand for 'security.' Both have multi-faceted consequence across the instruments of power and levels of operations. Due to their prevailing extent, they will not be discussed exclusively, but are considered an enduring backdrop to the global security environment and arm the notion for new adaptable ways.

10. Nations, partnerships and alliances will continue to find themselves in continuous competition with potentially more challenging adversaries. This continuum of competition, shown in Figure 1, ranges from cooperation, through rivalry and confrontation to armed conflict.[5]

5 Allied Joint Publication (AJP)-01, *Allied Joint Doctrine,* Edition F, Version 1, 2022, Chapter 1, Section 3.

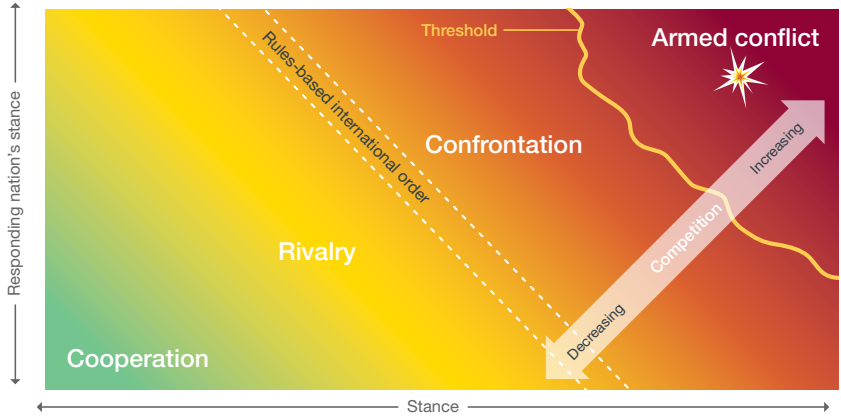

Figure 1 – The continuum of competition

11. To enable relative success, militaries will require a diverse set of capabilities and operational approaches that can be applied across the security environment and in tandem with other instruments of power.[6]

12. Democratic nations, with pluralistic societies, are vulnerable to exploitation; one aspect of which is based on their adherence to the rules-based international order. These vulnerabilities often manifest in the physical and non-physical seams between nations, instruments of power and operational domains. For military forces to be effective in contributing to mitigation they must learn, innovate and adapt to a more complex security environment, particularly as the distinction between peace and war increasingly blurs or overlaps. However, the changing circumstances brought forward by competition and the changing character of warfare offer opportunities to shape the security environment for advantage.

13. One such circumstance to highlight is the use of cyberattacks to disrupt, sideline and weaken national capabilities across the instruments of power. Such activity often occurs through untraceable means between the seams introduced above and are designed to avoid an armed response. Thus, all instruments of power, including military, must be prepared to coordinate against adversary actions throughout the continuum of competition. Increased use of multi-domain approaches and

6 US *Joint Operating Environment 2035*, 2016, pages ii, iii, 21, 24, 41, 51 and 52.

a complementary national security posture is an effective way to counter such malign activity.

14. In response to this competitive mix, there is a need to develop a common understanding of how military forces could operate in a multi-domain way above and below the threshold of armed conflict. Importantly, how to gain advantage through synchronizing domain effects in new and novel ways, including with other national and international agencies, will ensure maximum utility of the military instrument of power. An expected benefit would be to transition from a traditionally reactive posture, to one that affords appropriate pre-emptive posturing that suppresses or shapes adversarial intent.

15. The next section discusses key themes of the security environment using a framework based on combining the model for programme blueprints (process, organization, technology, information),[7] with the command and control system of analysis (people, processes, structures and technology),[8] shown in Figure 2. This blended framework was judged to bring forward aspects of change, competition, vulnerability and opportunity relevant for this project.

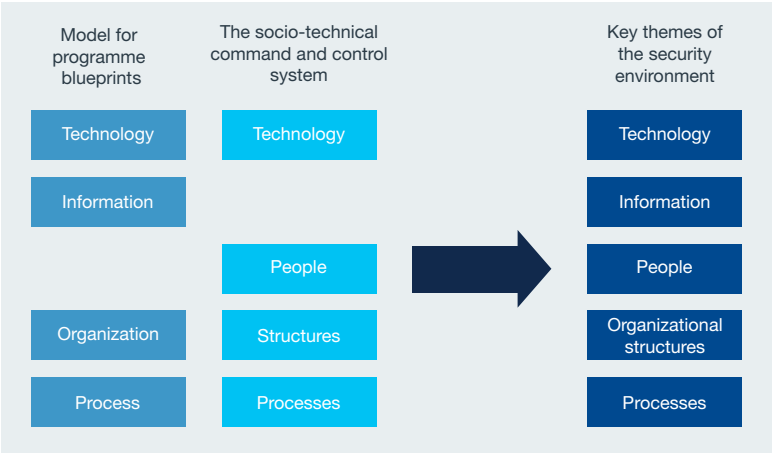

Figure 2 – Framework of themes: the derivation of models

7 Totally Optimized Projects, 'TOP & MSP: The Blueprint', last updated 3 April, 2020.
8 UK Joint Concept Note 2/17, *Future of Command and Control*, 2017, pages iii, 30 and 31.

Technology

16. Advances in technology provide opportunities to state and non-state actors that better enable them to create, challenge and erode competitive advantage. This is compounded by emerging and disruptive technologies, which are expected to enable novel approaches and improved military performance across all domains. Good examples are directed energy weapons, hypersonic platforms, artificial intelligence and machine learning, all of which represent a step-change to today's character of warfare. Military technology is currently caught in a cycle of balancing physical presence with high-cost Industrial Age means and is not best suited to meet the more subtle aspects of competition. Focused innovation on key technologies with maximum utility must be pursued and will enhance the ability to restore, sustain or extend advantage across the domains. However, access to this technology is not a given and it is important to note heavy dependence the military has on others for research and development across a wide spectrum of possibilities; this may require increased tolerance of high-cost research and development failure while exploring the decisive technological edge.

Processing power, the volume and variety of data, algorithms, data analytics, connectivity and scientific advancement continue to grow exponentially.

Information

17. Processing power, the volume and variety of data, algorithms, data analytics, connectivity and technological advancement continue to grow exponentially.[9] Recent innovations, including a shift from network-centric to data-centric information management and the use of validated identity information processes to protect data access, are foundational for improved multi-domain information sharing. Such activities support the achievement of information and decisive advantage for military forces, as well as mitigate the challenges of operating in a contested electromagnetic environment.

18. These technological advantages are accelerating both pervasiveness and persuasion of information, even if it is not based on fact, and herein lies a further aspect of competition. Furthermore, the narratives that flow are having increased influence on populations worldwide and have demonstrated the ability to mobilize significant change; both positive and negative. Also, social media helps inform competing narratives that seek to influence attitudes and gain support for objectives. As a result, society, industry and governments are spending more time conducting activities across all forms of media. Some actors choose to base narratives on disinformation and invariably, it is the triumph of the narrative over audiences that is decisive, not necessarily the facts, or even the truth. Further, for the sophisticated practitioner the ability to shape these narratives and base them on real artifacts within the physical world allows maximum influence. This can help prevent efforts to undermine the rules-based international order, while also enabling better military outcomes across nations, partners and alliances.

9 AJP-01, *Allied Joint Doctrine,* Edition F, Version 1, paragraph 1.29.

People

19. There is an increase in the number and variety of actors, including revisionist powers, who seek to challenge the status quo; their aim of altering the balance of global, regional or national power.[10] These potentially malign actors now have additional means and capabilities to pursue their goals and cause harm in ways that avoid confrontation or outright conflict. At the same time, nations and alliances struggle to obtain the human resources necessary to fulfil commitments and meet aspirations, partially due to societal and demographic changes in populations.[11] These trends may limit the ability to recruit essential personnel with the necessary skills, knowledge and experience to effectively deal with the complex situations actors may face.[12] This is typified within the military instrument of power in western nations who can be slow to respond, limited in action and constrained by the availability of domain specific skills. Also relevant is the necessity to adapt military leadership as discussed in the MCDC Project: *Future Leadership*.[13]

10 *National Security Strategy of the United States of America*, December 2017, page 25. See also: Michael J. Mazarr et al., 'Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives', RAND Research Report, 2018.
11 NATO Allied Command Transformation, *Strategic Foresight Analysis*, 2017 Report, page 36-37.
12 Ibid.
13 MCDC Project: *Future Leadership*, 2020.

There may also be radical policy and procedural changes required to authorize specific military actions in the more nuanced 'cooperation' and 'rivalry' stages of competition.

20. An increasing trend towards multi-domain approaches requires nations to examine the impact on human cognition and behavior at both national and multinational levels. Such impact stems from both the incorporation of new technology (for example, artificial intelligence and machine learning) and organizational alignments needed to create a coherent multi-domain force. Changes in force education and training will help and should be expected to support collaboration towards a competent multi-domain force. There may also be radical policy and procedural changes required to authorize specific military actions in the more nuanced 'cooperation' and 'rivalry' stages of competition.

Structures, organizations and processes

21. Existing organizational structures and processes are insufficient to adequately manage effective multi-domain activities, and successfully expand traditional military actions and mission sets to the 'cooperation' and 'rivalry' stages of competition.[14] Evolving these organizations and processes, while also developing new ones, may require both to be dynamically changeable or adaptable to the demands of the security environment.[15] [16]

22. Current structures do not align with evolving perspectives of operational domains and associated missions. Optimal competing may have extended, and introduced as yet unknown authority chains,

14 The continuum of competition introduces a sharper requirement to understand, decide and be clear on the intent for management of relationships; specifically, where interoperability is required: deconflict, cooperate, coordinate, synchronize and integrate.
15 US *Joint Operating Environment 2035*, 2016, pages iii, 7 and 8.
16 Ibid. See also: NATO, 'NATO's Approach to Space', last updated 2 December, 2021 and NATO Cooperative Cyber Defence Centre of Excellence, 'NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit', last accessed 7 November 2022.

with some authorities not integrated within existing military structures. Developing agile organizational structures[17] enables the sharing of information and should assist with authorities, while also allowing innovative best-practice across nations, partners and allies. Moreover, it facilitates burden-sharing by design through pooling of resources or niche domain-specific capabilities.

23. There are many relevant processes to consider. Command and control and civil-military cooperation are derived from the list of joint functions. It is recommended that a comprehensive review of all the joint functions and their related processes is undertaken in the future.

24. Command and control demands are changing because of the rapidly evolving security environment. These changes stress current command and control architectures and processes. Extant hierarchical, fixed and vulnerable processes lack agility[18] and system redundancy, leading to critical dependencies. There is therefore, a need for improved command and control agility to out-pace, out-think and out-fight the adversary.[19]

25. A further example is increasing civil-military cooperation. This stems from better understanding of the security environment and the recognized benefits of complementary activities across the instruments of power. As nations pursue a multi-domain approach to operations, they must be inclusive of these benefits and not inadvertently design-in approaches that are closed to broader leverage. This also brings forward the specific requirement to significantly improve cross-ministerial, cross-domain processes throughout the continuum of competition. As an example, threats of predatory financing, supply chain control and cyberattacks demand clarity over respective authorities and responsibilities.

17 See NATO's System Analysis and Studies (SAS) on command and control agility, for example, STO-TR-SAS-085, *C2 Agility*, 2014, (*Executive Overview: Task Group SAS-085 Final Report on C2 Agility*) and STO-TR-SAS-143, *Agile Multi-Domain C2*, 2020, including harmonization (*NATO STO SAS-143 Agile Multi Domain C2*).
18 NATO, STO-TR-SAS-085, *C2 Agility*, 2014, Chapter 2, pages 29–48.
19 *NATO Warfighting Capstone Concept* (NWCC): Building the Alliance's Decisive Advantage, military letter to the NWCC virtual conference, June 2020, 3–4.

Section 2 – Terminology

26. The following are agreed project definitions, with expanded comments, essential for a multinational understanding of multi-domain. These terms provide a working baseline and when framing them, consideration was given to the strategic, operational and tactical levels, as well as the CJIIM context.

27. **Domain.** A defined sphere where distinct groups of specific activities are undertaken. Contained within a domain are specific activities, and their effects, orientated to achieve specific objectives (activities within a domain could include planning, execution, sustainment and redeployment). Table 1 lists the operational domains by project nation or organization.

Nation or organization	Recognised operational domains						
Austria	Maritime	Land	Air	Space	Cyberspace		Information
Canada	Maritime	Land	Air	Space	Cyberspace		
European Union	Maritime	Land	Air	Space	Cyber		
France	Maritime	Land	Air	Space	Cyberspace	Electromagnetic	Information
Germany	Maritime	Land	Air	Space	Cyber		
Italy	Maritime	Land	Air	Space	Cyberspace		
Korea	Maritime	Land	Air	Space	Cyberspace	Electromagnetic	
NATO	Maritime	Land	Air	Space	Cyberspace		
Netherlands	Maritime	Land	Air	Space	Cyberspace		
Norway	Maritime	Land	Air	Space	Cyberspace		
Poland	Maritime	Land	Air	Space	Cyber	Cognitive	
Romania	Maritime	Land	Air	Space	Cyberspace		
Spain	Maritime	Land	Aerospace		Cyberspace	Cognitive	
Sweden	Maritime	Land	Air	Space	Cyber		
Switzerland	Maritime	Land	Air	Space	Cyber	Electromagnetic	Information
UK	Maritime	Land	Air	Space	Cyber and electromagnetic		
US	Maritime	Land	Air	Space	Cyberspace		

Table 1 – National operational domains

29. Across the project nations, there are varying perspectives on how relevant multi-domain approaches are to each of the instruments of power. Some nations have orientated their multi-domain narrative to be focused within the military instrument of power. Other nations are explicit that multi-domain approaches need to be integrated with the other instruments of power (diplomatic, information, and economic). For the purposes of this project, it is enough to know that these different perspectives exist and that the multi-domain principles identified in the next section are applicable regardless of scope.

30. Multi-domain. The condition where two or more domains interact with one another. While this term accounts for more than one domain, multi-domain does not necessarily require the interaction of all domains all the time.

31. Environment. The surroundings and conditions, physical and non-physical, that may influence domain activities over time and space. Physical surroundings or conditions include, but are not limited to, natural phenomena/elements, people, geography and resources. Non-physical surroundings or conditions may include mentality, culture, society, or virtual/digital landscape. These factors exist independently and may fluctuate.

32. Operating environment. The specific surroundings, conditions, actors and their objectives, which affect operational actions including understanding, planning, decision-making, and operating. Examples of operational actions include the following.

- Understanding: intelligence, assessment/analysis, common strategic/operational picture.
- Planning: critical vulnerabilities, critical requirements, critical factors, logistics, resources.
- Decision-making: authorities, command and control, legalities, doctrine, organizational structure, cohesion.
- Operating: capabilities, capability employment, timing, distance.

33. **Multi-domain operations.** The orchestration of activities in multiple domains to achieve a desired end-state. The term multi-domain operations (MDO) accounts for the interaction of multi-domain activities beyond joint service employment. It requires more than simple coordination between domains. MDO focuses on more than conflict alone and considers the full continuum of competition. MDO requires sophisticated understanding of the operating environment.

Section 3 – Principles

34. The multi-domain principles that follow provide guidance for integrating across multiple domains. They are not intended to replace, critique or conflict with existing principles such as the principles of war or joint operations.

35. The collective judgement of subject matter experts from across the project nations and organizations are the foundation for these principles. These judgments were informed by conceptual, doctrinal and emerging academic thoughts blended with a diverse cohort of experience. The project plan called for:

'A set of broad foundational principles for conducting multi-domain activity. These principles should encompass the design, planning and execution of multi-domain activity across the strategic, operational and tactical levels and within a CJIIM context.' (Annex B)

36. Throughout the project and extended discussion, twelve themes were identified and interrogated for meaning within a multi-domain context. These themes were then transitioned into seven principles. During the analysis, it was apparent that two, security and advantage, had overarching meaning and were best covered as implicit detail within the global security environment section.

37. The remaining five principles were then further described. These were:

- shared understanding;
- unity of effort;
- dynamic posture;
- agility; and
- innovation.

38. The principles are explained in three parts: **aim**, **attributes** (which are not exhaustive) and **description**, with the latter broken down into sub-sections of:

- **importance and risk** – a judgement on the principle's contribution to success when effectively applied, as well as potential negative consequences should the principle not be considered.

- **elements** – describes how the attributes work together for the principle to be successfully embedded; and

- **enablers** – the material and non-material resources that need to be in place or be available for the principle to be successful.

39. The principles are listed in the order shown due to interdependencies. For instance, within multi-domain activities, shared understanding is key to executing the tenets of unity of effort, dynamic posture and agility. While the fifth, innovation, is more stand-alone.

Shared understanding

40. **Aim.** To foster comprehension of the global security environment by sharing data and information while incorporating feedback. This will lead to better decision-making throughout a diverse network of stakeholders. This allows challenges to be addressed and opportunities to be realized in a timely fashion across domains.

The complexity of the military challenge in multi-domain operations demands an array of expertise to understand the problem.

41. **Attributes.** Accuracy, accessibility, collaboration, common conceptual understanding, data-centric methodologies, relevance and security.

42. **Description – importance and risk.** Shared understanding enables the timely execution of orchestrated activities across domains and levels of command. In the past, coordinated planning and general situational awareness was sufficient, with each component commander focused primarily on their area of responsibility. Now, more robust and dynamic interdependencies in multi-domain operations render this mindset lacking. The complexity of the military challenge in multi-domain operations demands an array of expertise to understand the problem, as well as to formulate pre-emptive actions or timely responses. It is through shared understanding and mission command[20] that objectives can be more effectively achieved. Lack of shared understanding risks incoherent pursuit of goals and offers exploitable opportunities to adversaries.

43. **Description – elements.** Timely access to relevant and accurate information within appropriate security protocols. This exists across all levels of command and in every aspect of the competition. A standardized data-centric approach simplifies sharing, accessibility and security allowing more collaborative and timely decision-making based on a holistic understanding of friendly and adversary capabilities.

44. **Description – enablers.** Shared understanding requires sophisticated technological infrastructures and decision-making processes to connect a diverse community of stakeholders. Artificial intelligence and machine learning, and other emerging and disruptive technologies will present even more opportunities for shared understanding. To meet these opportunities, there is a requirement

20 US Army Doctrine Publication-06, *Mission Command: Command and Control of Army Forces*, 2019.

for continuous education of leaders across domains and disciplines. These leaders will benefit from a mindset that promotes awareness and feedback, persistent consideration of how actions affect other stakeholders and organizational relationships across instruments of power.

45. Shared understanding within a multi-participant endeavor is examined as a key component of decision-making in the NATO sponsored SAS-050 study *Exploring New Command and Control Concepts and Capabilities*.[21] Enclosure 1 has an overview of the relevant parts of the study and identified nine shared understanding variables.

Recommendations

- Establish a standardized data-centric approach towards information.
- Establish a continuous program of education and training across domains and disciplines.
- Increase data, information and knowledge management skills across the force to enable shared understanding.
- Enhance real-time information sharing between mission partners and stakeholders, and to be able to do so in a contested electromagnetic environment.
- Connect a diverse community of stakeholders through sophisticated technological infrastructures and decision-making processes.
- Ensure timely access to relevant and accurate information within appropriate security protocols.
- Implement identity of credentialed information access management with appropriate security protocols.

21 SAS-050 Final Report, *Exploring New Command and Control Concepts and Capabilities*, 2006.

Unity of effort

> Unity of effort requires qualified trust, shared understanding, and common intent.

46. **Aim.** To harmonize capabilities and activities across multiple nations, organizations and stakeholders. This will enable commanders to plan operations, burden share and deliver maximum economy of force towards shared objectives.

47. **Attributes.** Collaboration, economy of force, harmonization, interoperability, shared intent and unity of command.

48. **Description – importance and risk.** Unity of effort enables the orchestration of activities and coordinated effects across domains to achieve shared goals with a broad range of stakeholders. It prevents organizations from working at cross-purposes and the unnecessary duplication of effort. A high degree of unity of effort avoids the risk of underperforming activities, the creation of conflicting effects and a degradation in presenting multiple dilemmas towards adversaries.

49. **Description – elements.** The start point must be a willingness to collaborate amongst stakeholders with the aim of optimizing interoperability. This harmonization should manage interests across a CJIIM context. Within the military instrument of power and the specific conduct of operations, unity of command will be critical to achieving synchronized efforts and attainment of shared objectives. Applying a multi-domain approach demands a high degree of interoperability across contributing nations. The reasons for this are various but include the management of multiple interrelated activities across domains, throughout the levels of command, and the opportunity of emerging technology. A dynamic operating environment, where adversaries are seeking to subvert or confront our design for competitive advantage, further reinforces the need for forces to function seamlessly. This demands a sophisticated level

of interoperability, and must include integration of doctrine, capabilities and training.

50. **Description – enablers.** Unity of effort requires qualified trust, shared understanding and common intent. This is achieved through engagement, experimentation, education and training. Military commanders cannot force trust amongst stakeholders in moments of crisis or conflict without introducing unquantified additional risk.

Recommendations

- Establish an active collaborative network of intelligence, knowledge and command centers across a broad range of stakeholders.
- Integrate doctrine, capabilities and training for forces to interoperate as seamlessly as possible.

Dynamic posture

> Without the appropriate capabilities and forces being in-place or available at the right time, in a state of persistent readiness, national decision makers face potential strategic shock with limited means to respond effectively, and risk loss of advantage.

51. **Aim.** To have the appropriate combination of capabilities and scale of forces ready for employment in the right place, at the right time, and able to converge effects decisively in concert with other stakeholders across the domains.

52. **Attributes.** Persistence, readiness, resilience and responsiveness.

53. **Description – importance and risk.** Dynamic posture influences the operating environment across the continuum of competition, acts as a deterrent, provides the capability to respond decisively to general crises, and provides the means to prevail in periods of armed conflict. Without the appropriate capabilities and forces being in place or available at the

right time, in a state of persistent readiness, national decision-makers face potential strategic shock with limited means to respond effectively, and risk loss of advantage. This dynamic will likely also cause an overbearing demand to regain initial advantage.

54. **Description – elements.** Dynamic posture includes the appropriate mix of interoperable forces, the necessary blend of capabilities (for example, cyber and space), at the appropriate level of readiness. Therefore, this must include access to required transportation, corresponding infrastructure, prepositioned materiel, and other enablers. A globally distributed network of available forces will enhance resilience, mitigating first mover advantage and minimizing the potential impact of strategic shock. In support of this network, a family of adaptable plans plus the requisite permissions and authorities would prime both readiness and responsiveness.

55. **Description – enablers.** Essential to delivering a dynamic posture, will be an effective, coordinated force generation mechanism across stakeholders. This should deliver a network of sustainment options across the area of interest that draws on burden sharing where appropriate. Complementary to this is a robust exercise program using tried and tested doctrine that delivers relevant and adaptive processes. It is equally important to test communication and information systems to assure confidence, trust and interoperable 'day zero' readiness.

Recommendations

- Establish a family of plans to support a globally distributed network of available forces with the requisite permissions and authorities in place.
- Increase coordination of force generation across partners and allies.
- Test communication and information systems to assure confidence, trust and interoperable 'day zero' readiness.

Agility

> Agility enables the creation and exploitation of opportunities, at speed and scale across domains

56. **Aim.** To orchestrate dynamic activities, be responsive to changes, and quickly shift focus to establish or re-establish advantage in a rapidly changing operating environment.

57. **Attributes.** Adaptability, anticipation, prioritization and speed.

58. **Description – importance and risk.** Agility enables the creation and exploitation of opportunities, at speed and scale across domains. This will both gain and sustain advantage, especially in response to changes in the operating environment. Forces lacking agility become reactive instead of proactive, surrendering initiative and advantage to the adversary.

59. **Description – elements.** Multi-domain operations require an alertness to changes in the operating environment and understanding of both the impact and opportunity this presents across domains. Anticipation is the ability to foresee those changes, generate influence and shape actions to build advantage before an unwanted situation manifests. Equal to this is the ability to respond to change, reacting and adapting to maintain or regain advantage. In both cases, the ability to take opportunities will require rapid prioritization and apportionment of available resources to achieve desired effects.

60. **Description – enablers.** Effective doctrine and comprehensive exercising will help embed the necessary agility within forces. However, this alone is insufficient and will need to be supported by rapid operational learning and energized feedback throughout the continuum of competition. The character of multi-domain operations, including diverse participation of partners and allies, strengthens the requirement for achieving common situational understanding. This will only be delivered through effective sensor coverage and a culture of trustworthy intelligence

sharing. With these enablers in place, the benefits of agility can be realized; the ability to both anticipate and respond.

Recommendations

- Increased focus on multi-domain situational awareness.
- Develop a culture of trustworthy intelligence sharing.
- Embed agility within forces through rapid operational learning and energized feedback.
- Improve cross-domain capabilities for rapid prioritization and dynamic apportionment of available resources to achieve desired effects.

Innovation

> Failure to innovate risks losing competitive advantage and increases the number and range of vulnerabilities available to the adversary.

61. **Aim.** To have a creative and adaptive approach to change. Innovation requires deliberate and coordinated investment. It will deliver the acceleration and flexibility needed to outpace and overmatch the adversary.

62. **Attributes.** Adaptability, asymmetry, creativity, learning culture, novelty, and research and development.

63. **Description – importance and risk.** Innovation leverages emerging and disruptive technologies, processes, organizational structures and information plus their novel recombination to produce new ways and means. It is the ability to do new things or do old things in new ways; this is especially important in a rapidly changing environment. Failure to innovate risks losing competitive advantage and increases the number and range of vulnerabilities available to the adversary.

64. **Description – elements.** Innovation must be resourced. In the short-term it includes the creative and novel use of existing capabilities and the adaptation of strategic, operational and tactical ways. In the long-term it should consider force design, force development, organization, process and technology opportunities that focus advantage through a multi-domain lens. Asymmetry, or the ability to consider novel approaches to challenges, is a central feature of innovation.

65. **Description – enablers.** Good connection from the operational user to innovation networks, both within and outside of the military enterprise, complements the rapid learning required for multi-domain approaches. To ensure focus is retained on successful operational outcomes, learning and experimentation must be shared, and critically must include best practice across partners and allies. Alongside this, innovation must be resourced throughout the levels of operations, the supporting acquisition cycles, and within the policy decisions made against force ambition and design. For innovation to be compelling, balance must be struck between starting small and being prepared to scale, with the acceptance that controlled fast-failure is important to healthy learning. This could indicate complete cultural change of both innovation and learning. However, it should not be seen as the first step, but more the cumulative benefit of delivering now, against real initiatives in support of the operational user.

Recommendations

- Allow fast-failure as part of healthy learning.
- Harmonize and resource capability innovation (investment of money, people, time, and research and development).
- Implement multi-domain standardization mechanisms between stakeholders (for example, modernization conforms to multi-domain standards and specifications).
- Establish common procedures among stakeholders to deny the easy access to high-tech products for potential adversaries.

Section 4 – Conclusion

66. In addition to the recommendations in Section 3, below are general conclusive comments.

67. Multi-domain approaches require information and intelligence to manage knowledge and perception across affected domains (**shared understanding**). This understanding will propel a timely decision-making process and harmonization of efforts to achieve objectives (**unity of effort**). Planning, force preparation, readiness and staging are critical to maximizing opportunities generated by common understanding (**dynamic posture**). To respond effectively, multi-domain efforts must be flexible, timely and adaptive to overcome the challenges within the operational environment (**agility**). The promotion of creative thinking and exploitation of emerging technologies are vital to navigating constant changes in the operating environment (**innovation**).

68. Therefore, nations, partners and alliances must organize and operate in new agile and flexible ways and continuously learn, innovate and adapt to a more complex security environment. This includes developing a diverse set of capabilities and operational approaches that can be applied cross-domain and cross-ministerial in tandem with other instruments of power, including pre-emptive posturing that suppresses or shapes adversarial intent. Increased tolerance of high-cost research and development 'failure' (or learning) while exploring a decisive technological edge are prerequisites.

69. Nations, partners and alliances must establish multi-domain doctrine, built from extant doctrine and standardized terminology, to develop a common understanding of how military forces could operate across the full continuum of competition. In parallel, it is necessary to identify and implement policy and procedural changes required to authorize related military actions during the more nuanced aspects of competition (cooperation and rivalry).

Section 5 – Recommendations for further multi-domain study

- Translate principles (Section 3) into operational requirements to support capability development.

- Review existing joint functions from a multi-domain perspective and identify potential gaps (such as doctrine, organization, training, materiel, leadership and education, personnel, facilities, and interoperability) including a specific focus on command and control.

- Validate the agreed multi-domain principles through a program of wargaming and experimentation (specifically challenge how the scientific community can assist).

- Develop the principles and elements into a deliverable road map (such as generic templates, maturity models and appropriate metrics linked to interoperability).

- Study the utility of the military instrument of power across the continuum of competition with a focus below the threshold of armed conflict.

- Develop a deeper understanding of the civil military balance within a CJIIM context.

- Develop a practical operational model to prioritize capabilities and resources across domains.

- Develop an effective force generation model across stakeholders that takes account of the broad character of CJIIM and enables dynamic posture.

- Establish the baseline for and develop effective doctrine that considers multi-domain force design, force development, organization, process and technology opportunities.

- Develop a mechanism to share the concepts and principles across multinational instruments of power, agencies, entities and organizations.

Enclosure 1 – Shared understanding variables

E1. A finding of the SAS-050 report on *Exploring New Command and Control Concepts and Capabilities* was, 'the quality of decision-making ultimately depends upon the quality of shared understanding … regarding the capabilities, environment, forces/actors, intentions, and the nature of the mission.'[22]

E2. Shared understanding is not a binary state of being achieved or not, but rather like a grey scale ranging from white (none) to dark grey (robust) with absolute shared understanding likely not ever being fully obtained.

E3. Where dynamic interdependencies exist amongst stakeholders, it is necessary to have in place the systems, processes, lexicon, and relationships necessary to obtain the highest level of shared understanding.

E4. The SAS-050 report listed nine variables related to shared understanding. They are provided here to give context to the challenges of a multi-domain approach that by its nature involve multiple stakeholders. The variables highlight the need for robust communication systems and feedback loops to reach the highest degrees of shared understanding.

- Accuracy – appropriateness of precision of shared understanding for a particular use.
- Completeness – extent to which relevant shared understanding is obtained.
- Consistency – extent to which shared understanding is consistent within and across communities of interest.

22 SAS-050 Final Report, *Exploring New Command and Control Concepts and Capabilities*, 2006.

- Correctness – extent to which shared understanding is consistent with ground truth.
- Currency – time lag of shared understanding.
- Precision – level of granularity of shared understanding.
- Relevance – proportion of shared understanding that is related to the task at hand.
- Timeliness – extent to which currency of shared understanding is suitable to its use.
- Uncertainty – subjective assessment of confidence in shared understanding.

For more information, contact: MCDCsecretariat@apan.org