Joint Air & Space Power20Conference19

8-10 OCTOBER 2019 READAHEAD



Joint Air Power Competence Centre

Shaping NATO for Multi-Domain Operations of the Future





Shaping NATO for **Multi-Domain Operations**

of the Future

Joint Air and Space Power Conference 2019



Joint Air Power Competence Centre

© This work is copyrighted. All inquiries should be made to: The Editor, Joint Air Power Competence Centre (JAPCC), contact@japcc.org.

Acknowledgements

This read ahead is a JAPCC product realized in collaboration with the authors of the essays contained herein. The JAPCC would like to thank the numerous authors who took the time to contribute to this product in an effort to advance this topic for discussion within NATO.

Disclaimer

This publication is a product of the JAPCC. The views expressed in this work are those of the authors. It does not represent the opinions or policies of the North Atlantic Treaty Organization (NATO), and is designed to provide an independent overview, analysis and food for thought regarding possible ways ahead on this subject.

Release

This document is releasable to the Public. Portions of the document may be guoted without permission, provided a standard source credit is included.

Published and distributed by

The Joint Air Power Competence Centre von-Seydlitz-Kaserne Römerstraße 140 47546 Kalkar Germany



M Denotes images digitally manipulated

Moderator's Foreword

Esteemed Colleagues,

It is my privilege and pleasure to serve as your moderator for this year's JAPCC Conference.

As in previous years, the panels for this conference follow a logical progression. Panel one has the clear task of establishing a working definition of what we actually mean by the term 'Multi-Domain Operations' (MDO). It would not be too dramatic to say that the rest of this conference (and, certainly, the remaining three panels) depends on the outcome of panel one. Therefore, panel one members have what is perhaps the most onerous task. Fortunately for all of us, the JAPCC has already done much of the 'heavy lifting' for this and you are about to go on and read a set of carefully selected, and carefully curated essays and articles that should lay firm foundations for our understanding of MDO.

Three articles are particularly relevant to panel one, and I would like to spend a little time discussing them here. It is also gratifying to note that two of these articles are written by JAPCC SMEs. As the first article in this read ahead suggests, each of the three traditional components – Land, Maritime and Air – may have their own understanding of what they mean when they use the term MDO. In many cases, each of these understandings may be subtly (and, often, not so subtly) different. The article also suggests that it is easier to explain what an MDO isn't rather than to define what an MDO actually is.

Dr Reilly from the US Defense Technical Information Center takes us further and suggests that one of the drivers for MDO is the 'global proliferation of advanced information technology'. However, whilst the concluding paragraph says that what is needed is 'a clear and common understanding of simultaneous manoeuvre in multiple domains beyond air, space, and cyberspace,' I am not sure whether we have quite reached that point by the end of the article.

The article by Lieutenant Colonel Canovas sheds considerable light on why the air component is particularly engaged by the concept of MDO. It is here that, I think, we find our first working definition of MDO as 'simultaneous, cross-domain operations that take into consideration the interdependency of different domains to exploit limited windows of opportunity.' This is a good start, but we may need to do better if we are to reach a common understanding of the MDO concept. However, the members of panel one may find this a useful place to start their work.

I have been part of many JAPCC conferences now, both as a JAPCC SME in the past and, more recently, as a member of academia in the audience. One of the great things about the JAPCC conference is that, whilst we hear from the smart people on the platform (and, by the way, I don't number myself amongst them), we also get to hear from some of the smartest people in the room. By that I mean those of you sitting further back in the conference room. One of my most important roles as the moderator is to ensure that there is sufficient time to hear from you as well. So, without being impolite to the panellists, I will make sure that there is ample time in each session for questions, opinions and rigorous debate put forward by the conference audience. Please feel free to challenge me – over coffee and cake – if you feel I am not doing this well enough.

Military people (and I write this as one who, in my RAF service, used to number amongst you) are, for the most part, highly pragmatic. One of the (perhaps slightly cynical) unwritten adages of UK Staff College was 'no lead, no read'. However, the concept of MDO is one where in-depth read-ing is a necessity – if we are going to be able to take the debate forward.

I therefore urge you to read what follows with your full attention. Engage with it – scribble on it, highlight it, insert exclamation marks and write 'YES' or 'NO' in big letters where you strongly agree or disagree with what you are about to read. Much of what you are about to read is contentious – and quite rightly so. New ideas and new concepts must be robustly debated before they can be accepted or rejected – and the JAPCC Conference gives us the ideal opportunity to do this.

I look forward to meeting you all, and hearing from many of you, in October.

Yours aye,

Bruce Hargrave MBA

Military Postgraduate Programmes Leader University of Lincoln

Table of Contents

| | Moderator's ForewordV |
|-----|--|
| 1 | What is a Multi-Domain Operation? |
| 11 | Defining the 'Domain' in Multi-Domain7 Dr. J. Donnelly, Lt Cdr J. Farley Over the Horizon Online Journal |
| 111 | Multi-Domain Operations |
| IV | Accelerating Multi-Domain Operations |
| V | The Complexity of Multi-Domain Operations33 Gen (ret.) H. J. Carlisle National Defense Industrial Association |
| V1 | Is Fluidity the Key to Effective Multi-Domain Operations? |

Multi-Domain Operations and Challenges to Air Power..47 Lt Col J. Canovas Joint Air Power Competence Centre

Training Joint Forces for Multi-Domain Operations57 Lt Col E. Wijninga Joint Air Power Competence Centre

1X

Doolittle Series 18 Multi-Domain Operations......65 US Air Force Lessons Learned/Air University Lemay Center for Doctrine Development and Education

X

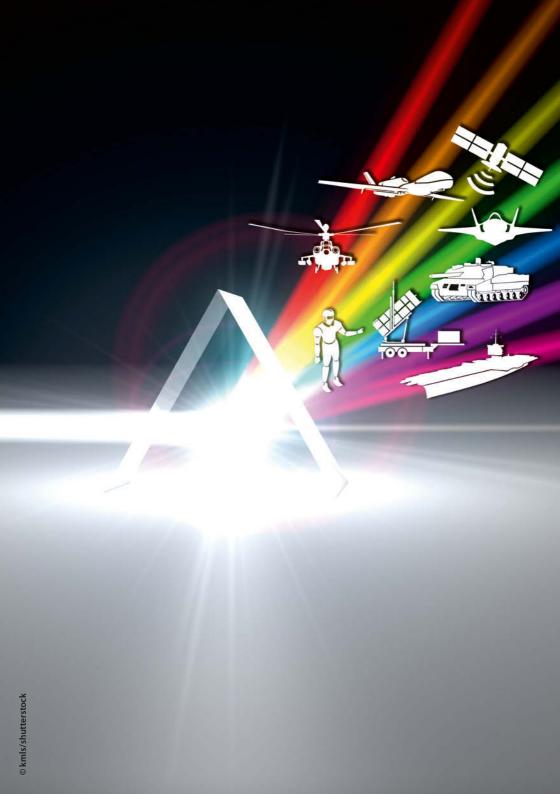
Multi-Domain Operations and Counter-Space73 Maj R. W. Gibson Small Wars Journal

XI

Cyberspace and Multi-Domain Operations......85 Lt Col P. MacKenzie Joint Air Power Competence Centre

Tracing Opinio Juris in National Cyber Security Strategy Documents91 Ms A. Väljataga NATO Cooperative Cyber Defence Centre of Excellence

Conference Itinerary 102



What is a Multi-Domain Operation?

By Lieutenant Colonel Heiner Grest, DEU, Air Force By Lieutenant Colonel Henry Heren, USA, Air Force Joint Air Power Competence Centre

A Look at Differing Views on a Developing Concept

The use of the term Multi-Domain Operations (MDO) has increased in popularity over the past decade as military services, those of the United States, in particular, have sought to codify their approach to warfare beyond the traditional confines of land, sea, and air. The term is new enough that, while many in military circles within the US and NATO have heard and even used the term themselves, the term is yet undefined by most nations and by NATO. Moreover, much of what has been written in the past few years concerning MDO bypasses elaborating on or clearly defining MDO, instead focusing on Multi-Domain Command and Control (MDC2). This paper will break from that approach and focus on addressing what can currently be said about MDO, from officially published guidance, and how it differs from previous concepts; notably Joint Operations.

As previously mentioned, neither NATO nor any of its member nations, specifically the US, has published a single unifying definition for Multi-Domain Operations. However, the official NATO Terminology Database,

published by the NATO Standardization Office (NSO), does offer a definition for 'domain'. Yet this definition is specific to the field of Information Technology, and defines 'domain' as 'that part of a computer network in which the data processing resources are under common control' and 'the set of possible values of an attribute.'¹ This IT specific definition is of little assistance in gaining a clear understanding of what is meant by MDO, at least within NATO. While NATO has not published a definition for the term 'domain' (within its Glossary of Terms and Definitions), it does have a definition for 'environment'² which seems to be used interchangeably with domain in numerous NATO publications. Moreover, NATO also clearly defines an 'operational environment'³. However, its definition seems to be more along the lines of conditions and factors than the closer environment term which aligns with the various recognised operational domains within NATO (land, sea, air, and cyberspace).

Without clear, concrete definitions within NATO, the Alliance is forced to look to its member nations. Most (not all) of what is being written and discussed concerning MDO is emanating from the US In 2018 the US Army Training and Doctrine Command defined MDO as 'how the US Army, as part of the joint force, can counter and defeat a near-peer adversary capable of contesting the US in all domains, in both competition and armed conflict. The concept describes how US ground forces, as part of the joint and multinational team, deters adversaries and defeats highly capable near-peer enemies in the 2025–2050 timeframe.'4 This US Army-centric definition lacks a clear description of MDO usable by services and nations, as it only clarifies the US Army's approach to MDO. It is important to note the U.S Army's MDO definition is actually a transition from 'Multi-Domain Battle' which is 'more inclusive of the type of competition that is now underway between the US and other nations' and takes into account a global competition that doesn't always involve fighting and battles, and 'Winning battle is not necessarily winning the competition.'5

The US Air Force offers another national service-focused definition for MDO in the form of MDC2, as 'the coordinated execution of authority and direction to gain, fuse, and exploit information from any source to integrate planning and synchronize execution of Multi-Domain Operations in time, space and purpose to meet the commander's objectives.'⁶ However, this definition is caveated to include the ability to 'effectively command and control (C2) Multi-Domain Operations to converge air, space, and cyber capabilities to meet the challenges of these contested domains.'⁷ While this definition begins to detail the intention of MDO, it stops short of discussing all of the various recognised operational domains within the US (or within NATO) and the reader is left to infer a definition of MDO from a definition of MDC2 ... a definition new and distinct from Joint Operations.

Joint within NATO is a term used to describe those 'activities, operations and organizations in which elements of at least two services participate.⁸ This definition is generally agreed to mean that two or more services work together and does not necessarily require they do so in an integrated manner. MDO, on the other hand, is seen as a step beyond joint. Indeed, for some, MDO requires 'coordination beyond just campaign planning to where individual effects are combined at the tactical edge.⁹ The specific degree to which MDO moves beyond joint seems to be focused on both the level of integration (within a body with requisite authorities) and expertise in capabilities employed through multiple domains. However, the degree to which MDO moves beyond joint is open to interpretation without clear delineation within NATO or its member nations.

A pessimistic and dismissive view of MDO, as a term, could be as a mere buzzword, synonymous with joint operations. And without clear definitions, it will be difficult to dispel naysayers. In the interim, time and resources are being expended on examining MDO and how NATO, and its member nations, can utilise the concepts contained therein. The discussions and research from these investigations are driving changes in capability development and will have repercussions within the Alliance for years to come. In the short-term, it is imperative that the 29 members of NATO arrive at a clear definition so they can move forward together.

Lieutenant Colonel Heiner Grest (DEU AF) is currently serving in the C4ISR+S Branch as a Space SME. In previous appointments he has been working in various positions in the area of Surface-Based Air and Missile Defence as well as in different national staff positions.

Lieutenant Colonel Henry Heren (USAF) is the NATO Space & Cyberspace Strategist assigned to the JAPCC. He is a Master Space Operator and a Fully Qualified Joint Staff Officer with more than 26 years' active duty experience in the US Air Force.

Endnotes

- 1. https://nso.nato.int/nso/, assessed 24 Apr. 2019.
- The surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans, and their interrelations. AAP-06, NATO Glossary of Terms and Definitions 2018.
- 'A composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.' AAP-06, NATO Glossary of Terms and Definitions 2018.
- https://www.tradoc.army.mil/Publications-and-Resources/Article-display/Article/1655556/multi-domain-operations/, assesses 24. Apr. 2019.
- 5. https://www.ausa.org/news/multi-domain-battle-gets-new-operational-name, assessed 24. Apr. 2019.
- Doolittle Series 18: Multi-Domain Operations, Air Force Leeson Learned, Air University Press, Maxwell Air Force Base, Alabama 2019. page 3, Footnote 1, https://media.defense.gov/2019/Feb/15/2002090437/-1/-1/0/lp_0003_multi_domain_operations.pdf, assessed 24. Apr. 2019.
- 7. See footnote # 6, page 3.
- 8. AAP-06, NATO Glossary of Terms and Definitions 2018.
- Chapman, Capt Matthew B. and Dalman, Lt Col Gerrit H. Joint Mission Control' Air & Space Power Journal, Spring 2019, page 51. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-33_lssue-1/V-Chapman_Dalman.pdf, assessed 24. Apr. 2018.



Defining the 'Domain' in Multi-Domain

'First, if the concept [Multi-Domain] is to be truly joint and multiservice, we need clarity and alignment in how we talk.'

General Stephen Townsend Commander US Army Training and Doctrine Center

By Dr. Jared Donnelly and Lieutenant Commander Jon Farley Courtesy of Over the Horizon – Multi-Domain Operations & Strategy

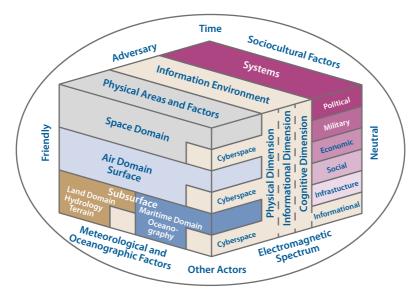
While there are plenty of philosophical discussions on the future of warfare, the important dialogue regarding the definition of domains have been largely untouched. There are a lot of smart people trying to wrap their heads around what this means for the employment of forces, but much of this churn is currently wasted, as the defence community does not have a basic definition for the word 'domain.' Until we understand what constitutes a domain, and just as importantly what does NOT, we cannot move forward with the paradigm shift that is Multi-Domain.

Doctrine does not help us with the definition of a domain. Joint Publication 3-0 does not define the term, though it uses the word from time to time. The closest it gets is in describing the Operating Environment (OE). Conceptually this is similar, but the notion of an operating environment is not the same as a domain. By the JP 3-0 definition, an OE can encompass some or all domains depending on where the commander needs to operate. This is much closer to the Multi-Domain concept as a whole where the commander will utilize a variety of domains to achieve their operational and strategic goals.

Where joint doctrine does discuss domains it often uses the term in ways that provide little clarity as to what resides in the domain or where the boundaries lie between domains. For example, in JP 3-0 cyberspace is defined as a ' ... global domain within the information environment' (JP 3-0, IV-2) while the information environment is described as '... the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information' (JP 3-0, IV-1). To further complicate things, JP 6-0 states that the Electromagnetic spectrum (EMS)' ... transcends all physical domains and the information environment and extends beyond defined borders and boundaries' (JP 6-0, I-6). This leaves warfighters with a domain (cyberspace) that exists within a milieu of individuals, organizations, and systems (information environment) that is transcended by the electromagnetic spectrum. Finally the warfighter is asked to fight and win in an Operating Environment (OE) that ' ... encompasses physical areas of the air, land, maritime, and space domains: the information environment (which includes cyberspace); the electromagnetic spectrum; and other factors' (JP 3-0, XIV).

JP 5-0 offers the diagram on the next page as an example of the OE, comprised of the stated domains: Land, Air, Maritime, Space, and Cyberspace. This graphic is an attempt to visually depict the interrelationships of domains, however it still does not inform the actual definition of the term.

The US Army's Training and Doctrine Center (TRADOC) also dances around the term with respect to Multi-Domain battle by stating: 'all domains are contested – land, air, maritime, space and cyberspace, and across the electromagnetic spectrum.'



Holistic View of the Operational Environment

The physical domains of land, air, maritime, and space are generally well understood conceptually – to the extent that joint doctrine does not feel the need to define them, but the non-physical areas of cyberspace, information environment, and the electromagnetic spectrum are much more difficult to conceptualize and bound within a constructive definition. That often leads us to situations where operations in these nonphysical domains are ill-defined, ineffectual, or non-existent, opening critical vulnerabilities to adversaries. As an example, electromagnetic interference (EMI) is rapidly becoming the Achilles heel of military operations. Manoeuvre within the electromagnetic spectrum is required by most warfighters, from basic radio operators to electronic warfare assets to satellite sensors. The sheer number of electronic devices on the battlefield, which travel through an ill-defined and coordinated EMS, are leading to routine blue-on-blue EMI fratricide. This could only be compounded if our opponents actively attempt to deny access.

This discussion is even more challenging when working with the North Atlantic Treaty Organization (NATO) partners because NATO doctrine uses the term domain to mean something else entirely. The NATO Combined Operations Planning Directive (COPD) uses the term domain in reference to the Political, Military, Economic, Social, Infrastructure, and Information Systems (PMESII), which the JP 5-0 refers to as systems. NATO doctrine looks at the concept of domains as dimensions of an operation environment'... including its land, air/space, maritime dimensions, as well as the PMESII systems of main adversaries ... ' (COPD 4-7). Therefore, with no doctrinal definition of a domain, we are forced to look to other thinkers for insight.

William Dries in a War on the Rocks commentary used the Miriam Webster definition for domain: 'a region distinctively marked by some physical or virtual feature(s).' This is a good foundation for the term, but is more refined by Peter Garretson: 'A domain is a space in which forces can manoeuvre to create effects.' This definition is closer, but we would argue that it still misses some salient points.

Other researchers working in the field of information operations, Patrick D. Allen and Dennis P. Gilbert, have suggested a definition for domain as 'The sphere of influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects' (Allen and Gilbert, 133). The latter part of this definition addresses the relation of the domain to the

operational requirements. This is an important distinction to make because the purpose for the existence of the domain concept is to provide a framework for focusing action in pursuit of strategic aims, however this definition does not fully encapsulate what we believe to be the full scope of a domain.

We offer the following definition of a domain, first proposed by Jeffrey Reilly, as a 'Critical macro manoeuvre space whose access or control is vital to the freedom of action and superiority required by the mission.'

The first segment of this definition is a 'critical macro manoeuvre space'. This phrase begins by implying that a domain starts with manoeuvre. As one of the Joint Functions, movement and manoeuvre is ... disposition of joint forces to conduct operations by securing positional advantages before or during execution. This function includes moving or deploying forces into an operational area and manoeuvring them within the timeline and to the operational depth necessary to achieve objectives. JP 1-0, I-19

The manoeuvre in a domain is often a unique, defining feature that separates domains from one another. But manoeuvre alone is not sufficient for a domain. The term macro helps simplify the definition by imposing some level of constraint. Without macro, one could argue that any distinctive feature would constitute a new domain, such as the difference in manoeuvre at 1k feet versus 50k feet, or the difference in manoeuvre in the infrared (IR) spectrum versus the radio frequency (RF) spectrum. This is the most difficult part of the definition, but one which must be clearly understood in order to be effective. The tension is simplicity versus specificity, and there are compromises with each.

The next segment is 'whose access or control is vital.' This segment implies that we need access or control of a medium in order for it to be a domain. For example, prior to the launch of Sputnik in 1957, the space domain physically existed, but was not operationally accessible. If the ability to manoeuvre through, access, or control, a medium is vital to the mission, then it meets the definition of a domain.

The final segment of the definition is 'freedom of action and superiority required by the mission.'This segment refers to the mission, and the ability to freely act and gain superiority in a domain. This closely ties to the definition of a centre of gravity in JP 5-0: 'The source of power that provides moral or physical strength, freedom of action, or will to act.' Superiority may come in the form of dominance, such as air superiority, or denial, such as in the electromagnetic spectrum. Ultimately, this ties the definition back to the mission, providing an anchor to the true purpose of manoeuvre through domains.

In the end, terms matter. The military is actively pursuing a Multi-Domain concept, with no understanding of the term domain. This attempt to provide a foundational definition is the beginning of that conversation. Until we understand the building blocks on which we are depending, the Multi-Domain concept cannot be explored to the level it deserves.

Dr. Jared Donnelly is an Assistant Professor at the Air Command and Staff College. He teaches in the Multi-Domain Operations Strategists program for the Department of Future Security Studies.

Lieutenant Commander Jon 'Tike' Farley is an instructor at the Air Command and Staff College who teaches in the Multi-Domain Operational Strategist program. He is an F-18 Pilot with multiple deployments to the 5th Fleet AOR, supporting operations in Iraq and Afghanistan.



Multi-Domain Operations

111

By Dr. Jeffrey M. Reilly

Defense Technical Information Center, US Department of Defense Courtesy of Air University Press

Note: This essay is an abridged version of the article 'Multi-Domain Operations – A Subtle but Significant Transition in Military Thought,' published in The Air and Space Power Journal, Spring 2016.

A Subtle but Significant Transition in Military Thought

n 17 November 2011, Gen Martin Dempsey, chairman of the Joint Chiefs of Staff, asked the Military Education Coordination Council the prophetic question, 'What's after joint?' After more than four years, that question remains ostensibly unanswered. The answer, however, may reside in the notion of Multi-Domain Operations. General Dempsey's inquiry was spurred by the fact that historical approaches to achieving superiority in the air, land, and sea domains may no longer be valid. The principal factor driving this phenomenon is a global proliferation of advanced information technology. Although the United States has undergone dramatic changes in technology in the past, we are in only the nascent stages of understanding this era's

monumental impact on future military operations. The worldwide flood of powerful, inexpensive, and readily available commercial technology is mandating a much more sophisticated approach to military affairs. The exponential growth associated with Moore's Law (states that processor speeds, or overall processing power for computers will double every two years (www.mooreslaw.org)) has created a security environment where the pace of cyber, directed energy, nanotechnology, robotics, and biotechnology advancements is far beyond the normal capacity to predict their effects. Advanced information technology is also changing our perspectives of Multi-Domain interdependence. America's ability to project conventional power abroad is eroding swiftly as state and non-state actors acquire advanced capabilities to offset the US military's strengths across all operating domains – air, land, sea, space, and cyberspace.¹ Additionally, the requirement to think across domains is occurring at increasingly lower levels and will be essential in the future to generating the tempo critical to exploiting fleeting local opportunities for disrupting an enemy system.² These changes in the operational environment, combined with 'new' fiscal realities, are rapidly transforming how we need to think about threats, the battlespace, and the conceptual underpinnings of Air Power.

Multi-Domain Operations Are an Enduring Characteristic of Warfare

The concept of cross-domain operations is not new. It has been an inherent part of military thought since antiquity. The disastrous Athenian campaign to conquer Sicily during the Peloponnesian War provides just one example. In 415 BC, Athens launched an ill-advised expedition to subdue Sicily's strongest state, Syracuse. The Athenian force led by Nicias consisted of approximately 6,400 men and 134 ships. The Athenians enjoyed early successes; however, in 414 BC during the siege of Syracuse,

the Spartan strategist Gylippus intervened and turned the tide of battle in favour of the Syracusan forces. Gylippus focused initially on the human domain, inspiring the Syracusan forces and galvanizing the support of their allies. He then embarked upon simultaneous attacks of the Athenian troops on the land and at sea. By 413 BC, the Athenians had been defeated.³

This defeat signalled the beginning of the end for the Athenian empire. However, the lesson of this historical example goes far beyond the collapse of Athens. It highlights the importance of understanding multiple domains and the necessity of shifting local superiority between domains. Gylippus concentrated on what is now becoming a crucial idea embedded in the Joint Operational Access Concept – specifically, that superiority in any domain may not be widespread or permanent but more often local and temporary.⁴ The lesson from Gylippus is that establishing superiority in a combination of domains offers the freedom of action necessary to attain mission success.

Challenges of Future Technological Threats

Unable to compete with US forces directly, adversaries are leveraging technological advances to create their own asymmetric advantages in countering US military superiority.⁵ Russia, Iran, North Korea, and China have invested in a number of ballistic and supersonic cruise missiles designed to challenge the United States' conventional superiority. At least nine countries are involved in the development and production of land attack cruise missiles, and many of these weapons will be available for export within the next decade.⁶ Innovations in cruise missile technology have created supersonic threats that can engage targets 300 km away and be delivered by a variety of systems such as aircraft, submarines, ships, or even trucks.⁷ Furthermore, modern cruise missiles

can be programmed to approach and attack a target in the most efficient manner. Newer missiles are incorporating stealth features to make them even less visible to radars and infrared detectors. In addition to threats from advanced missile technology, between 2004 and 2012, the number of countries having acquired remotely piloted vehicles increased from 41 to at least 76.8 Many of them are seeking to enhance not only their intelligence acquisition but also armed strike capabilities. Furthermore, numerous countries are working on highpowered microwave (HPM), directed-energy, and electromagnetic pulse (EMP) weapons. A 2005 declassified intelligence report on the bio-effects of Chinese EMP and HPM weapons indicated that China could detonate a low-yield, low-altitude strategic nuclear warhead to destroy electronic systems while minimizing the effects to the Chinese mainland.⁹ The significance of this intelligence is that it sheds light on using weapons systems to deny multiple domains simultaneously. EMP damages unhardened electrical circuits and electronics by generating a surge in the current and voltage beyond normal functioning capacity. A 1-megaton nuclear blast detonated 400 km above the centre of the United States can have continental-wide terrestrial effects in seconds, as well as a significant impact on space capabilities.¹⁰ One should also note that adversaries can deliver effects from EMP through a multitude of nonnuclear modes that produce a wide array of outcomes ranging from temporary interference to system destruction. These modes include ballistic missiles, submarines, aircraft, and satellites as well as man-packed systems.¹¹ Advances in technology are also affecting an adversary's ability to defend itself. Integrated air defence systems are becoming increasingly resistant to electronic suppression through the use of passive sensor technologies. Potential adversaries are also investing in inexpensive low-power jammers to inhibit the positioning, navigation, and timing necessary for effective strike operations.12

Changes in Adversarial Concepts and Strategies

Although the military modernization of possible enemies is disconcerting, it is only part of the future threat equation. Prospective foes are combining advances in technology with operational concepts and strategies designed to deny the US military asymmetric manoeuvre in multiple domains. The People's Republic of China (PRC) is aggressively pursuing this path, combining what it refers to as shashoujian (trump card or assassin's mace) technology with the concept of unrestricted warfare and an information warfare strategy. Shashoujian refers to a set of military capabilities that enables the technologically inferior to defeat the technologically superior. These capabilities include advanced integrated air defence systems, ballistic and cruise missiles, advanced strike aircraft, attack submarines, and counter-space capabilities.¹³ The PRC's well publicized cyber capabilities go far beyond collecting and exploiting intelligence data. The difference between cyber exploitation and attack is as simple as a keystroke. The PLA (People's Liberation Army) is actively creating the strategic guidance, tools, and trained personnel necessary to employ computer network operations in support of traditional warfighting disciplines.¹⁴ Cyberspace offers the PRC and other state and non-state actors the capacity to delay an adversary's response to a kinetic attack by implanting malicious code in advance on the enemy's networks.15

In spite of the significant advantages that China enjoys from cyberspace, it is not the focal point of the PRC's information warfare strategy. The PLA's assessments of current and future conflicts note that campaigns will be conducted in all domains simultaneously but that its emphasis on the electromagnetic spectrum has driven the PLA to adopt a much more comprehensive approach.¹⁶ In 2002 the PLA's Maj Gen Dai Qingmin characterized electronic warfare as an intangible power necessary for success. He pointed out that whichever side loses in an electronic

war will be reduced to blindness and deafness, so its weapons will be disabled, and it will lose its initiative in a battle, campaign, or even an entire strategic situation.¹⁷ This type of warfare also stresses that the electromagnetic spectrum is a vital fourth dimension equally as important as traditional ground, sea, and air forces.¹⁸ The implications of this phenomenon are numerous and serious enough to mandate another look at how we educate future Air Force leaders to develop, coordinate, and execute air operations.

Implications for the Concept of the Battlespace

Advances in technology have subtly nudged the entire globe into a realm where all previous notions of the battlespace have been radically altered by domain interdependence driven by a combination of factors ranging from advanced technology efficiency to fiscal constraints. These factors are creating an environment where failure in one domain has cascading effects in one or more of the others. Postmodern technology is guickly fusing a continuum of integrated and interdependent domains. Hypothetically, if an opponent attacks or manipulates the use of radio frequencies within the EMS (the electromagnetic spectrum), through cyber or other means, he could deny access to vital satellites that we rely on for intelligence, surveillance, and reconnaissance; communications; early warning; and navigation. The consequences would severely affect a joint force air component commander's planning, decision, and execution cycle and could render operations in the air, on land, and at sea ineffective. Future Airmen must be sufficiently cognizant of this integrated operational environment to ensure that enough local superiority in the right combination of domains fosters the conditions necessary for operational success. It is also important to emphasize that the transformation of the battlespace is much more significant than challenges related to operating in a highly contested EMS within a

designated joint operations area. For the first time since the end of the Cold War, the United States faces the threat of a catastrophic attack on the homeland beyond the scale of the terrorist strikes of 11 September 2001 The historical barriers of the Atlantic and Pacific oceans are no longer effective means to negate an enemy's operational reach. The continuing growth of networked systems, devices, and platforms offers prospective state and non-state foes a plethora of vulnerabilities to threaten US national security that go well beyond military targets. Another significant change in battlespace is space. Since 1991 the United States has become more reliant on space-based capabilities to support military operations. Space assets provide the means to communicate globally; conduct the positioning, navigation, and timing necessary for precision strikes; and empower enhanced intelligence, surveillance, and reconnaissance. Further, space furnishes virtually unimpeded overflight access to conduct the monitoring essential for missile-launch detection, missile tracking, and early warning. A satellite system consists of three basic components: the satellite itself, the ground stations used to command and control it, and the communication links between the components. All of the latter have varying degrees of vulnerabilities. Adversaries can employ a variety of attack options, including kinetically striking the ground stations, jamming or spoofing links, and using directed energy to dazzle or partially blind the satellite.¹⁹ Like space, the EMS is exceedingly complex. One of the key constraints of this battlespace is that only one percent of the spectrum accounts for 90 percent of its military and civilian use. The effectiveness of the EMS is also complicated by electromagnetic interference between systems, EMP, competition between military and civilian use, and natural phenomena such as lightning, solar flares, and precipitation. Additionally, it is important to emphasize that our adversaries know and understand the EMS and that they will aggressively contest our access to it. The spectrum transcends all physical domains, has no specific or internationally recognized boundaries, and can create a wide array of unintended collateral effects ranging from the

annoyance of a communication disruption to a deadly collision on a civilian railway transit system. Accordingly, approval to use electromagnetic-dependent systems for military operations calls for extensive coordination with multinational allies and host nations.

How Does This Change in Operational Environment Affect Air Power?

The dramatic alterations now occurring across the operational environment will affect Air Power in innumerable ways, including air superiority, strategic attack, counter-land, counter-maritime, and support to special operations forces. However, the two most significant effects will involve planning, decision, and execution cycles and domain superiority. In the future, these cycles will be compressed, reach-back capabilities will be limited, and forward commanders will have to rely on mission type orders because the EMS will be vigorously contested and because both terrestrial and space-based communications will suffer degradation or disruption. Consequently, Air Power's foundational principle of centralized control/decentralized execution will be forced to shift to a distributed-control approach that adapts to operational changes by having preplanned bandwidth allocations and a vision for manoeuvring between gateways.

The impending operational environment will also influence the concept of domain superiority. As advanced technology continues to proliferate, domain superiority will be much harder to achieve. In fact, such superiority will most likely remain localized and temporary. Moreover, it is important to point out that success may not depend upon the traditional quest for domain superiority. Instead, success may reside in precision access in a single domain that enables a combination of actions in other domains. Airmen must become much more attuned to forms of manoeuvre in all of these realms, and until they develop an appreciation for and understanding of Multi-Domain manoeuvre, true innovation in Air Power, unfortunately, will be lacking.

Conclusion

When General Dempsey asked, 'What's after joint?' he was emphasizing that at some point in time, the focus on joint operations will not be adequate to address the challenges of our emerging operational environment. During the past two decades, Air Power has given the joint force unrivalled dominance in the air. However, quantum advances in technology and the realities of fiscal constraints are driving a dynamic era of evolutionary adaptation. This evolution must be deliberately shaped to ensure that domain interdependence does not inadvertently risk a single point of failure. More than ever before, Airmen must have a clear and common understanding of simultaneous manoeuvre in multiple domains beyond air, space, and cyberspace.

Endnotes

- 1. Mark Gunzinger with Chris Dougherty, Changing the Game: The Promise of Directed-Energy Weapons (Washington, DC: Center for Strategic and Budgetary Assessments, 2012), ix.
- 2. Department of Defense, Joint Operational Access Concept, version 1.0 (Washington, DC: Department of Defense, 2012), 16.
- 3. Thucydides, History of the Peloponnesian War, trans. Rex Warner (New York: Penguin Books, 1954).
- 4. Department of Defense, Joint Operational Access Concept, 15.
- Office of the US Air Force Chief Scientist, Technology Horizons: A Vision for Air Force Science and Technology, 2010–2030 (Maxwell AFB, AL: Air University Press, Air Force Research Institute, 2011), 19.
- National Air and Space Intelligence Center, Ballistic and Cruise Missile Threat, NASIC-1031-0985-09 (Wright Patterson AFB, OH: National Air and Space Intelligence Center, Apr. 2009), 3.
- 7. Victor N. Corpus, 'America's Acupuncture Points, Part 2: The Assassin's Mace,' Asia Times, 20 Oct. 2006, http://www.atimes.com/ atimes/China/HJ20Ad01.html.
- US Government Accountability Office, Nonproliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports, GAO-12-536 (Washington, DC: US Government Accountability Office, Jul. 2012), 9.
- 9. 17. National Ground Intelligence Center, China Research on Bio-Effects of Electromagnetic Pulse and High-Power Microwave Radiation (Charlottesville, VA: National Ground Intelligence Center, 17 Aug. 2005). Unclassified.

- Headquarters Department of the US Army, Nuclear Environment Survivability (US Army White Sands Missile Range, NM: US Army Test and Evaluation Command, 15 Apr. 1994), appendix D.
- 11. See Jim Wilson, 'E-Bombs and Terrorists,' Popular Mechanics 178, no. 9 (Sep. 2001): 51; and Frederic P. Miller, Agnes F. Vandome, and John McBrewster, Explosively Pumped Flux Compression Generator (Mauritius: Alphascript Publishing, 24 Nov. 2009).
- 12. Department of Defense, Joint Operational Access Concept, 13.
- Andrew F. Krepinevich, 7 Deadly Scenarios: A Military Futurist Explores War in the 21st Century (New York: Bantam Dell, 2009), 187.
- 14. Deepak Sharma, 'China's Cyber Warfare Capability and India's Concerns,' Journal of Defence Studies 5, no. 2 (Apr. 2011): 66.
- Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2013 (Washington, DC: Office of the Secretary of Defense, 2013), 36.
- Deepak Sharma, 'Integrated Network Electronic Warfare: China's New Concept of Information Warfare,' Journal of Defence Studies 4, no 2 (Apr. 2010): 37–38.
- 17. Bruzdzinski, 'Demystifying Sha Shou Jian,' 346.
- 18. Office of the Secretary of Defense, People's Republic of China, 2013, 37.
- 19. David Wright, Laura Grego, and Lisbeth Gronlund, The Physics of Space Security: A Reference Manual (Cambridge, MA: American Academy of Arts and Sciences, 2005), 109



© iamseki/shutter<u>stock</u>

Accelerating Multi– Domain Operations: Evolution of an Idea

1V

By General Stephen Townsend, USA, Army Courtesy of Modern War Institute at West Point

White the second second

For Multi-Domain Battle there are two things driving the need to evolve the concept.

First, ideas must evolve to ensure alignment with the strategic direction of the enterprise they serve. The 2018 National Defense Strategy lays out the missions, emerging operational environments, advances in technology, and anticipated enemy, threat, and adversary capabilities that the Department of Defense envisions for the foreseeable future. It provides direction for how the joint force must evolve to compete, deter, and win in future armed conflict. To this end, Multi-Domain Battle must reflect this strategy.

Second, when I took the reins of US Army Training and Doctrine Command, I was specifically directed to 'operationalize Multi-Domain Battle' by building upon the foundation created by my predecessor and accelerating its application. And what I found was an incredible foundation. Gen. Dave Perkins brought together partners across the joint force, driving development of the concept to an articulated idea and a vision of how the army fits into it. The key players are all here and are committed to building and improving the concept and finding real solutions. The concept is ready to grow.

But for that to happen, we need to confront some of the problems others have noted. Over the last eighteen months that Multi-Domain Battle has been out there for debate, there have been four consistent critiques. Some noted that the idea was 'old wine in a new bottle.' I think the iPhone analogy articulates why that just isn't true. What the original iPhone did wasn't all that new, but how the iPhone did it fundamentally changed not just a market, but people's behaviour. This is exactly what we seek to achieve with this new concept. Though the domains of warfare (air, land, sea, space, and cyberspace) are not new, how the US armed forces will rapidly and continuously integrate them in the future is new.

Another critique is that this is an Army-only concept. However the Air Force and Marine Corps have been part of MDB from the start and recent reporting from numerous forums has made clear the Army's desire to listen, learn, and include our joint and multinational partners in the development of this idea. Recently the Navy and the Joint Staff have also joined the discussion. Albert Palazzo's series of articles in the fall of 2017 laid out a clear argument. To be successful, Multi-Domain Battle must translate into radical effects on the US military's culture. The concept must force us to reconsider fundamental tenets, like our industrial-age means of promoting, training, and educating leaders. It must also pull us from the comfort of our tactical-level trenches to develop capabilities that inform up to the strategic level of war. Putting 'battle' into the name both confines the possibilities and limits the result.

In battles, combatants can win time and space and they allow one side to take ground but they do not win wars. The world we operate in today is not defined by battles, but by persistent competition that cycles through varying rates in and out of armed conflict. Winning in competition is not accomplished by winning battles, but through executing integrated operations and campaigning. Operations are more encompassing, bringing together varied tactical actions with a common purpose or unifying themes. They are the bridge between the tactical and the strategic.

In my first months of command at Training and Doctrine Command, it became clear that the use of the word 'battle' was stifling conversation and growth of the concept. There are three concrete reasons why Multi-Domain Battle evolved to Multi-Domain Operations.

First, if the concept is to be truly joint and multi-service, we need clarity and alignment in how we talk. The Air Force talks of Multi-Domain Operations and Multi-Domain Command and Control, while we talk of Multi-Domain Battle – often covering similar, if not the same, ideas and capabilities. To this point, none of the many people I have talked to, including my predecessor, are wedded to the use of 'battle' – it was what fit best in time, place, and circumstances. What they are committed to are the ideas of converging capabilities across the joint force with continuous integration across multiple domains. Second, we cannot do this alone. The armed services can win battles and campaigns, but winning wars takes the whole of government. It helps the entire effort if our interagency partners are comfortable with and conversant in our warfighting concepts and doctrine. As highlighted to me by a former ambassador at a recent forum, talking in terms of operations instead of battles brings together those who want to get things done – whether they are civilians or the military.

And third, it is never just about the fight. When it comes to combat, there is no one better than the combined weight of the US military and our allies and partners. However, the operating environment is evolving and nation-state-level competition has re-emerged, as evidenced by recent actions by both Russia and China. Our National Defense Strategy highlights the importance of winning the 'competition' that precedes and follows conflict. However, our use of 'Multi-Domain Battle' seemed to indicate our concept was only for the conflict phase. While there are battles within competition, winning them is pointless if they are in isolation to the larger context of deliberate operations supporting national strategy.

Multi-Domain Battle served its purpose – it sparked thinking and debate and it created a foundation. But what we need now is Multi-Domain Operations, and the next revision of the concept to be released this fall will reflect this change.

Language is important. It conveys meaning. This change is not cosmetic – it is about growing an idea to its greatest potential in order to change the way we fight today and ensure overmatch against our adversaries of tomorrow. To do this we need clarity and alignment across the joint force, whole-of-government inclusion, and perspective that reinforces our need to compete effectively outside periods of armed conflict. Changing the name does not do this by itself, but it communicates a clear vision of what we need to accomplish and where we are headed.

General Stephen Townsend is the Commanding General of US Army Training and Doctrine Command. He previously served as commander of 18th Airborne Corps and Combined Joint Task Force Operation Inherent Resolve. His combat and operational experience includes deployments in support of Operation Urgent Fury, Operation Just Cause, Operation Uphold Democracy, Operation Enduring Freedom, and Operation Iraqi Freedom.



The Complexity of Multi-Domain Operations

By General (ret.) 'Hawk' Carlisle

Courtesy of National Defense, NDIA's Business & Technology Magazine

or the US military to maintain its status as the greatest fighting force in the world, it must continue to learn and understand the Multi-Domain battlespace and significantly improve its operations across the entire range of military activity.

It is widely believed that the US military is exceptional and by far the best in the world, but adversaries are catching up. The key to maintaining its advantage and deterring or defeating its enemies rests in its ability to simultaneously operate through and across all domains. It must present foes with multiple dilemmas for which they have no answer and no way to predict what will happen next.

Potential adversaries are making significant improvements in cyber warfare in order to minimize traditional US dominance in all the other domains. The United States must become the best in cyber just as it has mastered all the other domains.

This will require significant advancements by the US defense industrial base and the US military in new technologies like artificial intelligence, machine learning, autonomous and semi-autonomous systems,

quantum computing and big data, to name a few. Also, just as it understands and works to gain and maintain space, air, land and naval superiority, it must also understand and work to gain and maintain superiority across the entire electromagnetic spectrum.

The US military has been nothing short of spectacular and its command and control of its forces has continually improved. The beginnings of Multi-Domain Operations can be seen on today's battlefields. For example, air operations centres have made significant advancements to fuse space, air and some nascent cyber effects to support the joint fight.

There is similar progress at space, land and maritime operations centres. But they are all somewhat stovepiped. There is ongoing work to integrate the operations centres, but it often becomes a matter of de-confliction. There are still struggles to find the best way to incorporate the cyber command and control into all the operations centres as well as the intelligence community and interagency.

Much like John Boyd's OODA loop – observe, orient, decide and act – the military can approach this problem through the three layers of the execution of operations.

First is the sensing layer – intelligence, surveillance, reconnaissance and analysis – to understand the enemy, the environment and the military's place in the joint Multi-Domain fight. Second is the command-and-control layer. And finally, the effects layer, which includes kinetic, non-kinetic and information operations.

To truly get to Multi-Domain Operations, one has to look at all the domains as they relate to the three layers. The first challenge that has to be worked through is visualization. One must see how domains relate to each other. Can a common operating picture of all the domains be created – along with the necessary networks – to provide the joint force with all the needed information to stay inside the adversary's OODA loop?

The second challenge is time. Each domain works on different timelines. Dismounted special operators move at a few miles per hour. Aircraft carriers sail at 30 knots. Jet fighters break the sound barrier and cyber operations move at the speed of light. All this must be coordinated so the right effect is delivered at the right time.

The third challenge is cyber and spectrum superiority. The US military must operate across the entire electromagnetic spectrum to maintain networks and create effects in the targeted domains – all while the enemy is attempting to do the same.

Here is a tactical scenario that illustrates where improvement is needed. It involves a group of heavily defended mobile targets in the littoral area of a hostile country.

First, a sensing layer is needed to find, fix and track the targets, which the stealthy F-22 can provide. Given the number of targets and the long-range necessary to reach them, a large magazine is required with long-range weapons. A submarine carrying Tomahawk land attack missiles is available. These are stealth platforms that can penetrate enemy defences long enough to accomplish the mission.

A network is also required to take the F-22 sensor data and send it to the Tomahawks. A command-and-control network creates a common operating picture of the environment that allows the joint force commander to understand what it takes to get both the submarine and the F-22s to the right place at the right time to execute the mission. Accomplishing the mission becomes more complicated as other domain requirements are added. For example, a cyber weapon may be needed to disrupt the enemy's integrated air defence systems to allow the F-22s to stay on station long enough to provide sensor information.

A Special Forces operational detachment alpha team may be on the ground taking action to disrupt the enemy's command-and-control network. Communication and GPS satellites may have to be adjusted to operate in a heavy electromagnetic jamming environment.

All of these capabilities operate on different timelines. There is the time it takes to deploy a submarine into a launch area, or to adjust satellites. There is the time needed to insert a special ops team.

And all of this could happen as cyber effects are transmitted at the speed of light.

The US military needs the ability to understand and visualize all the domains and their timelines so it can create a common operating picture. It needs networks that connect all the domains to pass and receive the data necessary for its missions. And it needs to control the electromagnetic spectrum to accomplish all this in environments where the enemy will do everything in its power to disrupt US communications and networks.

Bringing the military, industry and academia together in open collaborative settings will facilitate the true integration of sensors, command and control and effects across all domains. **General (ret.) Herbert J. 'Hawk' Carlisle (USAF)** is the president of the National Defense Industrial Association. Gen. Carlisle came to NDIA after a 39-year career in the Air Force, from which he retired as a four-star general in March 2017. His last assignment was as commander, Air Combat Command at Langley Air Force Base in Virginia.



Is Fluidity the Key to Effective Multi-Domain Operations?

By Wing Commander Jeremy Parkinson, GBR, Air Force Joint Air Power Competence Centre

Introduction

any will have heard the phrase 'Flexibility is the Key to Air Power'. Some will have heard the corollary that 'flexibility' is too rigid a concept and that it is actually 'fluidity' that is required; this is my starting point – Fluidity is the key to Multi-Domain Operations.

Domains

Those reading this will likely be familiar with the concept of domains (e. g. Maritime, Land and Air). Over the years we have developed our thinking on the concept of domains to include activity that takes place sub-surface and in Space and more recently, the Alliance has decided to consider Cyber-space as a domain. The first question that occurs is: In developing our thinking about the domains, have we also adequately developed our thinking about how we might operate within them? Or indeed: How might these domains be contested and by whom? The word 'contested' is used to suggest that there will be both aggressors and defenders and in the course of

any contest, roles may reverse (i. e. the attacker is repulsed and subsequently becomes the defender). Understanding a domain is only a part of the challenge. Further, given the complexity of modern warfare, is it sufficient to understand only a single domain?

Beyond the Physical

To complicate the situation further, the physical domains of Land, Air, Maritime, and Space are generally well understood, to the extent that Joint Doctrine does not apparently see the need to define the domain. However, the non-physical areas of Cyberspace, the Information Environment, and the Electromagnetic Spectrum (EMS) are perhaps more difficult to both conceptualise and bound; below are offered definitions:

a. Cyberspace. Cyberspace is defined as a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. According to this definition, cyberspace is a very real, physical domain that is comprised of electronics and networked systems that use electromagnetic energy. Cyberspace exists across the other domains of air, land, sea, and space and connects these physical domains with the cognitive processes that use the data that is stored, modified, or exchanged. Cyberspace is therefore distinct from the information that may be resident in or transferred through the domain (US National Military Strategy for Cyberspace Operations).

b. Information Environment. An environment comprised of the information itself; the individuals, organisations and systems that receive, process and convey the information; and the cognitive, virtual and physical space in which this occurs (AJP-3.10, Allied Joint Doctrine for Information Operations).

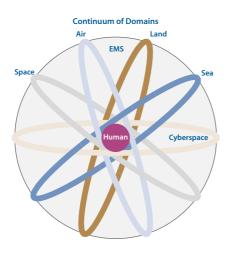
c. The Electromagnetic Spectrum. The Electromagnetic Spectrum (EMS) is the range of frequencies of electromagnetic radiation and their respective wavelengths and photon energies (Encyclopaedia Britannica).

Threat Considerations

During the Yom Kippur War, Israel lost a large numbers of aircraft to Egyptian Air Defences during the first few days of the conflict. These loses were due to Israel being caught by surprise and as a result, not being able to mount Suppression of Enemy Air Defences (SEAD) missions against Egyptian SA-6 surface-to-air missile systems. The problem was compounded as Israeli Air Force (IAF) radar warning receivers were not initially programed to detect the SA-6 radar. Were it not for the IAF's size, resilience and ability to rapidly adapt, this event could have had game-changing results. The IAF learned the important lesson that Electronic Warfare had come of age; this was in 1973. Fast forward to the present and the era of multiple simultaneous and complex threats (360° threats), and many actors, state and non-state have access to complex technologies. As a result, the Operational Environment of today is very different to that of 1973.

Operational Environment

The Operational Environment¹ of today will consists of factors and conditions that must be understood to successfully apply military capabilities, protect the force and complete any task. It extends beyond the physical boundaries of a defined area. The operational environment includes the sea, land, air and space, the enemy, neutral, friendly and other actors, facilities, weather, terrain, the EMS, CBRN² threats and hazards, and the information environment (extracted from AJP-3.2, Allied Joint Doctrine for Land Operations). Most if not all of the factors that combine to create the Operational Environment, affect all of the domains and therefore, all of the military



components; this is particularly true for the EMS as the Figure shown highlights:

At the centre of the diagram³ (left) sits the human and therefore human activity, to include warfare. If there is a relationship between all of the domains and all domains encroach into the EMS, is this not then the way that we should conceptualise modern warfare?

Current Doctrine – Current Thinking?

Having explored domains and the operational environment, we can turn to the components. How do the components currently view their primary role? Offered below are current definitions:

a. Maritime Power. Maritime power is derived from the ability of a state or non-state actor to use the freedom of movement provided by the sea to exert diplomatic, economic, and military influence at a time and place of choice. Maritime power has traditionally been employed globally to maintain the freedom of navigation essential to the general economic welfare or survival of states. Conversely, it has been regularly used to disrupt an opponent's sea lines of communication (SLOC) as part of a wider Allied, joint, or combined operation (AJP-3.1, Allied Joint Doctrine for Maritime Operations).

b. Land Power. No such definition exists in NATO Doctrine (AJP-3.2, Allied Joint Doctrine for Land Operations). However, the following is offered for considera-

tion: The use of the term 'land power' reflects the dynamism of the strategic environment over the past 15 years. Land power encompasses the employment of an array of land capability – from Army and across government – to achieve specified objectives. The Army must always view itself not in terms of simply'winning the land battle', but as a force capable of exerting land power for strategic effect across the modern spectrum of peace, crisis and war. The term land power also raises Army's concept of itself above this tactical 'win the land battle' and accepts that the generation of effects on the land also has strategic impact. It is multidimensional: land power may involve the employment of capabilities from all the operational environments (land, sea, air, space and cyberspace) to achieve results on land (extracted from Australian Land Doctrine).

c. Air Power. The ability to use air capabilities to influence the behaviour of actors and the course of events (AJP-3.3, Allied Joint Doctrine for Air and Space Operations).

It can be seen that only within a national definition of Land Power do we see the mention of other domains to include domains that are beyond the physical. Alliance forces are competent in the physical domains but, without simultaneous supporting activity in the non-physical domains or activity that is ill-defined, ineffectual, or non-existent, we risk opening serious if not critical vulnerabilities to our adversaries.

Relationship between Domains, Components and Threats

It is here that we encounter what was once not a question, or at least, not one that required serious consideration. Which Component operates in which Domain and against what threat? One may offer a simple answer. The Land Component operates in the Land Domain against a land-based threat etc. Today, however, given the 'continuum of domains' it is offered that even the most basic military activity takes place in several domains simultaneously. Therefore, to win in the Air, requires supporting activity in all the other domains to include secured access to Space and the EMS. This requires new thinking and new ways of operating.

Development of Thinking

If Alliance Air and Space Power is to be able to deliver effects from the Air at a time and place of our choosing (our asymmetric advantage and what our adversaries most fear), then we need both protection and support across all domains, physical and non-physical, if we are to be effective and resource efficient. That is to say, whilst projecting effects from the Air, we need to be simultaneously be protected and supported in each and every other domain and the threats that exist within that domain. Of course, a similar argument should be advanced for each of the other components. Freedom of Action within the Information Domain and within Cyberspace is now as important as Freedom of Manoeuvre in the physical domains; to achieve this requires mastery of the EMS. The EMS is required by all war-fighters, from basic radio operators to electronic warfare assets to satellite sensors. The sheer number of electronic devices in the battlespace, that function across a poorly controlled and coordinated EMS, are leading to routine blue-on-blue incidents of Electromagnetic Interference up to and including fratricide events. This will only be compounded if our adversaries deliberately attempt to deny friendly forces access to the EMS. Therefore: Is current thinking at the component level fit for the current operating environment? Going forward, understanding how to fight and win in each domain (or indeed pan-domain) is what the Alliance actually requires.

So What?

It is offered that we are now in an age where it is impossible to conceive of activity in any domain without considering what support or supporting

activity is necessary in each of the other domains concurrently – a Complex All Domain Environment (CADE). Furthermore, the components will need to become increasingly agile across all domains in order to seamlessly transition from the supported to the supporting role. This is the synthesis of Multi-Domain Operations.

Summary

It is no longer sufficient for air forces to be masters of the Air. Yes this is the domain in which they project power but, in order to do so there needs to be mastery, both intellectual and physical, of all of the other domains. If deterrence is to be effective, or failing that, if we are to fight and win, robust analysis is required that seeks to answer the question: How does the Alliance achieve Domain Superiority? A further subtly is to explore: Is Domain Superiority required or, just a favourable situation for a specified time in order to achieve an objective and/or effect? Clearly, superiority, or a favourable situation, may be required in multiple domains concurrently or consecutively so, moving forward, Joint Campaign Synchronisation needs to evolve to become Multi-Domain Synchronisation; fluidity will be the key.

Wing Commander Jez Parkinson is a RAF Regiment Officer with 32-years' Service; over half in the Multinational environment. He is the Author of NATO FP Policy, FP Doctrine for Air Operations and the current Custodian for Joint FP Doctrine.

Endnotes

- The operational environment is defined as: A composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander (NATO Term).
- 2. Chemical, Biological, Radiological and Nuclear.
- 3. Diagram from OTH article 'The Multi-Domain Operational Strategist' by Dr Jeffrey Reilly 8 Nov. 2018.



\mathbf{V}

Multi-Domain Operations and Challenges to Air Power

By Lieutenant Colonel Juan Canovas, ESP, Air Force Joint Air Power Competence Centre

Introduction

ew concepts of operation, fuelled by technological advances, have facilitated interconnectivity across different domains of warfare. Consequently, this cross-domain interconnectivity now provides an opportunity to access objectives through non-linear (nonsegregated) approaches. Indeed, the Alliance has a burgeoning opportunity to change how it reaches strategic objectives in a future conflict. More to the point, success in the future will very likely be through the realisation and implementation of Multi-Domain Operations (MDO).

What is Multi-Domain?

Over the last few decades, Air Power has performed a central role in assuring successful joint operations. The inherent jointness of Air Power could be a major reason for such success. Indeed, the air component (not always wielded solely within an Air Force) routinely influences the domains of air, land, maritime and space. In most spheres of thought, these physical domains are routinely complemented by at least two other domains, the cyberspace domain (accepted as a domain at the NATO-Warsaw Summit) and the cognitive or human domain. Also, though currently not widely accepted, some authors also define the Electromagnetic Spectrum (EMS) as a domain. Furthermore, domains are typically grouped within three larger categories: physical (air, space, land, maritime); digital (cyber, EMS, information, new technologies); and cognitive (disinformation, psychological, strategic communications). While intuitive to most operational practitioners, it is important to state that domains are interrelated. For example, the cyber and space domains must be defended to exert control in other domains.

So, with that as a background, one definition of Multi-Domain is 'an evolution of joint operations' that results from the necessity to overwhelm an adversary by simultaneously creating multiple problems across multiple domains. An alternative definition of Multi-Domain Operations is 'simultaneous, cross-domain operations that take into consideration the interdependence of different domains to exploit limited windows of opportunity.'

How are Multi-Domain Operations Challenging Air Power in the Future?

To take advantage of the full capabilities of MDO, the Alliance needs to carefully consider some of MDO's key enablers. Specifically, Command and Control, connectivity, interoperability and technology and training must be deliberately addressed.

Command and Control

Today's Allied joint operations are conducted at a de-conflicted or coordinated level, as per the command and control (C2) maturity model.¹ Currently, the Alliance does not have adequate capabilities to plan and control joint operations at a Collaborative C2 level nor execute truly simultaneous operations in multiple domains. Instead, the battlespace is routinely de-conflicted and segregated, and thus, most events are in fact mono-domain operations. Exacerbating this, reach-back capabilities of the future will likely be contested. Not only that, but the EMS will be heavily contested, and both terrestrial and space-based communications will most probably be disrupted.

Therefore, to fully operate in a highly dynamic environment, especially to gain an advantage in decision cycles, the future design of the C2 structure should be combat-centric instead of command-centric. In this construct, decisions should be delegated to the lowest operationallycompetent level and forward commanders will have to be regularly trained to execute mission-type, Multi-Domain orders. However, Multi-Domain commanders must understand the constraints and restraints in all domains and account for impacts across operational seams to effectively plan force packages. Also, while the overall commander's intent must be preserved, delegation of control to distributed command and control nodes should enable these local mission commanders to exert adequate control over their Multi-Domain forces. Consequently, Air Power's foundational principle of centralized control/decentralized execution will be forced to shift to a distributed-control approach which adapts to operational changes by having pre-planned bandwidth allocations and a vision for manoeuvring between gateways.

In this context, Multi-Domain Command and Control (MDC2) may be defined as 'the coordinated execution of authority and direction to gain, fuse, and exploit information from any source to integrate planning and synchronize execution of Multi-Domain Operations in time, space and purpose to meet the commander's objectives.²

Connectivity

Once you have critical, useful MDC2-level information, connectivity will be the key to disseminating it. While much has been said about a potential 'combat cloud', it worth noting that such a database could conceptually allow high-speed sharing of information to different entities that, at the same time, generate more data with their own sensors and update the cloud. As a result, this information sharing process could increase targeting speed and reduce the time from sensor to effector.

As an important note, in order to effectively enable MDC2 Allies will have to agree to robustly share real-time intelligence, as limited windows of opportunity will close in the quickly evolving battlespace. Also, despite disruptions in the EW and EMS domains, there will still be a requirement to communicate securely to all force packages, to provide clear guidance and to direct them effectively. Accordingly, the Alliance needs to develop better data sharing mechanisms (i.e. technical connectivity) and these mechanisms will need robust crypto technology and accompanying procedural authorities to share. Indeed, many might say that technical connectivity is not really a significant limitation; it is the political will to share data that often prevents true interoperability.

Interoperability and Technology

In respect to interoperability, NATO Allies must establish MDO concepts and define a roadmap to reach a Multi-Domain strategy. All parties need to be part of the process, including the political decision makers. To implement a change in the culture of operations to conduct MDO, a new legal framework will be needed in most Europeans nations. Additionally, preconflict political decisions will be necessary to share all of the intelligence necessary for each operation. The 'Need to Know' concept is viewed as a risk control measure but not sharing information often creates additional risk to mission and security. Sharing data is the heart and soul of interoperability, so security processes need to be revised to avoid excessive protection of data and to find an equilibrium between data availability in a certain place and time and security and integrity. The solution for the 'Need to Share' principle should be built into the common data architecture, without limiting rights properties and available to different applications that may use that data. For example, the information used to construct a Common Operating Picture, (COP), should be developed by a mechanism that integrates data from different classification levels and sources to provide the user with an appropriately filtered, but useful, picture.

On a practical level, NATO should utilize joint exercises that specifically experiment with interoperability and data sharing as vehicles to minimize or eliminate technical and procedural hurdles to MDO. As such, it is urgent to improve the cohesiveness of both Alliance members' software and hardware and continue to address international and inter-service confidence building. In conjunction with these exercises, the Allies should leverage breakthroughs in Al, machine learning and automation to research, reach and maintain a MDC2 advantage. For this reason there should be deliberate engagement with industry to gain an advantage of emerging technologies and to reduce acquisition cycles. These technological advances will eventually permit delegation of authority to the lowest echelons, further enabling MDC2. Even in limited operations, it will be still desirable to conduct distributed control and decentralised execution to avoid a long chain of C2.

As a recurring theme, technology will be key to the future of MDC2. Emerging threats and opportunities will have to be identified and the status of forces, plus their enabling and supporting elements, updated in real time. Consequently, dynamic targeting will be ruled by machine to machine communication. Al will be used to calculate such things as GO – NO GO criteria, collateral damage, caveats, best weapon available, and to assign assets to the correct targets. Additionally, it will be necessary to be able to discern decision-quality information in operationally-relevant context and integrate open source and publicly available information.

Some examples of emerging technology in the cognitive domain are the techniques used to read the human brain and to apply readings in a hybrid form of bionic machine that can execute integrated algorithms coming out of, or through, the helmet of a pilot. In this way a single human can control a group of machines through his or her mind. In this way, virtual reality and AI supporting cognitive activity can integrate air assets in Multi-Domain Operations.

Training

When discussing the implementation of MDO, one of the most important facets is the human strand. A bottom-up cultural change is needed in the education process. Structures and processes related to personnel need to be addressed by the Joint Forces to begin training with, and to define new requirements for, MDO personnel. Airmen must become attuned to various forms of cross-domain manoeuvre until they develop an appreciation and understanding of true Multi-Domain Operations.

In the long term, a formal cadre of dedicated MDC2 experts is critical for the success of MDO. Allies should focus on developing a specific career branch that has the purpose of understanding how to employ Joint capabilities across a Multi-Domain environment. These professionals should be dedicated to operational level activities from the early stages of their career and will form the cornerstone of future operational, Multi-Domain planning and execution. In addition to dedicated personnel, another requirement might be to create Multi-Domain Operational Training Infrastructures to experiment, implement and improve MDC2 at all levels. These infrastructures would be separate, but complimentary to joint exercise enablers previously described. An integrated training system, taking advantage of the Live, Virtual and Constructive, (LVC) training paradigm, should be the first step in developing MDO training. LVC provides integration of virtual, (machine driven), man in the simulator and real entities in a common scenario to replicate all types of threats and Multi-Domain entities. This type system can provide improvements in MDO decision making through complex and personalised training environments and by simulating rare space and cyber entities.

In addition to specifically trained personnel and a robust LVC environment, future MDO training iterations, especially those tailored for highly contested environments, requires an integrated opposition force (OPFOR) with standardised doctrine, capable support and dissimilar assets, including so-called hybrid capabilities, all in a cost-effective solution. When developed, OPFOR will execute enemy hybrid/MDO operations in which Red, (the forces replicating OPFOR), cyber and space actions affect Blue, (the training audiences), training in realistic ways.

Conclusion

The different domains; physical, digital and human are interconnected. Actions in a single domain will increasingly influence the others, creating windows of opportunity to achieve favourable results, even in contested domains.

Multi-Domain Operations are not just an evolution of joint operations. MDO requires mission commanders to simultaneously conduct parallel actions in multiple domains of the battlespace according to dynamic situations. Given that, an effective MDC2 structure will be required to recognise windows of opportunity, through real-time situational awareness in all domains, and execute faster decision cycles. Additionally, in a contested and degraded environment it will be extremely important to conduct operations using a decentralised execution model. Consequently, redundant connectivity and data sharing will be required to enable commanders to effectively provide guidance and receive feedback on the status of their forces.

Next, Nations need to be engaged with industry to gain an advantage from emerging technologies and to reduce acquisition cycles, especially in the fields of artificial intelligence and cyber defence.

Lastly, a training effort is needed to adapt operational level staff to MDO and to create a cadre of MDC2 experts. These professionals will be expert in combining all domains in operational level planning, and execution, from the earliest stages of their career.

Lieutenant Colonel Juan Canovas (ESP AF) is a Subject Matter Expert at the Joint Air Power Competence Centre. He is an experienced F-5 instructor and F-18 pilot. He has participated in NATO operations as a Forward Air Controller and at the JFACC level.

Endnotes

- Air Warfare Communication in a Networked Environment. Conclusions reviewed from Joint US DoD Command and Control Research Program and the NATO System Analysis Studies (SAS-065) about Alberts et al, C2 Maturity model. JAPCC, Jul. 2017.
- 2. Doolittle Series 18: Multidomain Operations. Air University Press, Maxwell Air Force Base, Alabama. Feb 2019.

Casper 1774 Studio/shufterstock URSGA72/shufterstock Berezka_Klo/shutterstock

Training Joint Forces for Multi-Domain Operations

'I have instructed my staff to put large-scale, high intensity, all domains warfare against a near-peer adversary at the very heart of all our training from now on, and I am prepared to assume some risk in other areas to achieve this.'

> SACEUR's Annual Guidance on Education, Training, Exercises and Evaluation 2019

By Lieutenant Colonel Ed Wijninga, NLD, Air Force Joint Air Power Competence Centre

Introduction

n 2013, JAPCC provided extensive support to the Joint Warfare Centre (JWC) in Stavanger for the first time with an OPFOR Air team. The supported exercise was Steadfast Jazz 13 and, for the first time, based on a complex and comprehensive Article 5 scenario. In the years leading up to Steadfast Jazz 13, NATO had focused many of its exercises on out-of-area operations and counter-insurgency scenarios. This meant that there was only limited 'air play' as these exercises featured virtually no opposition air forces. An interesting aspect of Steadfast Jazz 13 was that the scenario introduced the use of proxy forces and hybrid operations.

The JAPCC team in 2013 also encompassed one Space Subject Matter Expert (SME) who supported the scenario and scripted several Space injects that were executed during the exercise. This took the Training Audience (TA) more or less by surprise, who were not well prepared to deal with Space-induced incidents and were not adequately staffed to deal with challenges like the effects of Space weather or GPS jamming. As of 2015, the JAPCC team has also provided a Cyber SME to the JWC-led exercises, which again for the first time, challenged the TA. Last but not least, the JAPCC proposed introducing the Training Audience to the challenge of Advanced-Layered Defence Systems, better known as Anti-Access Area Denial (A2AD).

The three areas of Cyber, Space and A2AD have been further developed and included in subsequent exercise scenarios. Their positive impact on the Training Audiences resulted in a request from JWC for JAPCC to lead development, not only for OPFOR Air scenarios for Exercise Trident Juncture 18, but also for the Space and Cyber scenarios. Russia's illegal annexation of Crimea has provided further momentum for NATO to exercise and develop scenarios with all aspects of modern warfare in mind. These exercise scenarios now provide the Training Audience with comprehensive Multi-Domain challenges.

The Changed Landscape

After decades of counter-insurgency operations against opponents who possessed limited means and certainly no credible standing forces, in 2014 the world was taken by surprise when it was confronted with hybrid operations on the Crimea. At first, these operations were rather covert but later were openly supported by Russian forces, who occupied and illegally annexed this southern Ukrainian peninsula. A few months later then the story repeated itself in the Donbass region in Eastern Ukraine when hybrid

forces started operations, again covertly supported by Russia. This hybrid activity culminated with a SA-17 missile launch that resulted in the crash of Flight MH-17. The Joint Investigation Team (JIT) later found clear evidence that although proxy forces operated the SA-17 system, Russia had provided it. The JIT was even able to provide evidence specifying from which Russian Air Defence Brigade the system originated.

At the same time, the World was increasingly confronted with villainous Cyber activity, in many cases originating from Russia, China or North Korea. In keeping with the classification of this article, one can safely assume that the world will continue to face Cyber challenges on a daily basis. Some hackers try to disrupt processes, disturbing public services such as transport, some try to obtain military information, and some try to gain access to economic information to strengthen their economic position.

Space has also become a factor at play in adversarial tactics with the proliferation of anti-satellite weapons, anti-satellite jammers, Directed Energy Weapons, dazzlers and espionage satellites. Employment of these could disrupt or destroy NATO's capability to gather information, apply Command & Control and conduct operations.

Current Status

Scenario development for Trident Juncture 18 (TRJE18) encompassed a comprehensive set of forces to include a robust OPFOR Space Order of Battle (ORBAT) and Cyber capabilities. As a result, the TRJE18 scenario could be seen as a Multi-Domain scenario providing exercise play that not only included A2AD in its most comprehensive form, but also challenged the TA with realistic in-Space and Cyber incidents. The TA was prepared for this and had invested in manning, knowledge and capabilities to deal with the challenges presented to them. Despite this, the TA still struggled with

the vast scale of the scenario across all acknowledged domains and Space at the same time. One of the greatest challenges for the Joint Commands and their staffs was building a comprehensive and shared Multi-Domain picture using outdated C2 systems, and accounting for activities and effects originating outside as well as inside the Joint Operations Area (JOA). These complex scenarios require a completely new approach to conducting operations and creating the desired effects in the locations where these effects are most successful.

In past exercises, no TA was able to successfully deal with A2AD challenges. The added complication of Space and Cyber operations has presented them with even greater challenges. There is still an ongoing school of thought that A2AD is an Air Component's (ACC) problem to be solved primarily by the ACC. In reality, the A2AD puzzle can only be solved by synchronised, coordinated joint (and most probably Multi-Domain) approach. The Joint Force Commander and his staff play a key role here. Gone are the days when one can only think in terms of supported/supporting relationships, gone are the days of me first, you later. The best approach is to think in effects on how to address the problem and where and when to create these effects. All the components, including Space and Cyber, have a role to play in this approach and, most probably, all at the same time.

The Air Component can degrade the opponent's Integrated Air Defence System, protect air/sea ports of em- and debarkation, can protect its air bases against long-range strike and can provide force protection. Space can try to degrade the opponent's precision navigation and timing and intelligence, surveillance and reconnaissance (ISR) systems and can force the opponent to use other systems over which they have no direct control. special operations forces (SOF) can contribute by conducting deep reconnaissance missions and counter- hybrid operations. The land component can provide joint fires, (counter-)mobility operations and ensure freedom of movement of main supply routes. Cyber can contribute with offensive cyber operations to degrade opponent's command & control and other systems and the maritime component can contribute with anti-submarine warfare, anti-surface warfare, mine-clearing operations and joint fires as well. Strategic communications can be utilised to gain support for NATO operations while at the same time trying to influence the opponent's population. All at the same time and fully coordinated and synchronised. I would like to call that simultaneous Multi-Domain (SMD) operations.

The SMD approach is moving away from operations which are synchronised as well but more so in a sequential order. This simultaneous approach requires a different mindset. It also requires that NATO obtain better access than it currently has to Space and Cyber capabilities. Both Space and Cyber assets are only provided by individual NATO nations upon request. Offensive Cyber is even more sensitive in the sense that very few NATO nations now have offensive Cyber capabilities that they are willing to provide for NATO operations. If NATO were able to use offensive Cyber and Space capabilities, there would also be legal aspects to consider; a topic which is addressed elsewhere in this read ahead by Lieutenant Colonel MacKenzie. NATO, therefore, has to rely heavily on capabilities that it does not own, which can be a limiting factor in the planning and conduct of Multi-Domain Operations. Whichever capabilities are used to address the problems in Multi-Domain Operations, a simultaneous approach might be worth considering and this is a marked difference from the sequential order of operations with which NATO is most familiar.

Future

The Supreme Allied Commander Europe (SACEUR) has made it clear in his Annual Guidance for Training and Exercises for 2019 (SAGE19) that highintensity, near peer-to-peer, Multi-Domain scenarios as should be the main training and exercise objectives for the coming years. He even goes as far as making them a priority by accepting some risk for other areas. This means that future exercise should focus on highly complex and comprehensive Multi-Domain scenarios, thus demanding more of the Training Audiences. The combination of SACEUR's Guidance and SMD should lead to a rethink by Joint- and Component staffs on how they might need to interact with each other. At the same time, NATO might also need to look at whether their current construct of exercises provides the necessary training in terms of planning and staff processes to address Multi-Domain Operations. The conduct of exercises in recent years have focused on sequential operations and would suggest that the current training does not address the problems identified.

One other consideration that is not frequently exercised is the civilian domain. This could be a whole domain by itself. The reader might argue that this aspect is fully covered in NATO's current comprehensive approach to operations but several facets are not covered in this perspective on warfare. A comparison with the Cold War can be made for the deployment of NATO's forces; individual nations would use their resources, state-owned companies, requisitioned transport means and NATO would have planned the synchronisation and coordination of movements. This was particularly important as several Corps-size army formations moved through Europe at the same time crossing each other's paths to deploy to field locations. When NATO troops need to deploy to a Joint Operations Area in an Article 5 scenario in current times, the requirements for transport and sustainment might be even greater. However, NATO nations, to a large extent, do not own these capabilities anymore. State-owned railways, transport resources, telecommunications providers, and sustainment facilities have been privatised, and governments need to negotiate their availability for military operations without disrupting the economy too much. This is an entirely new aspect of warfare that is rarely exercised but might be a completely new domain to be considered. The dependency on external resources, in particular, might prove to be an enormous vulnerability for the deployment of forces and the conduct of operations.

Exercises traditionally consist of several phases in which the TA is preparing and executing the scenario. One of the most critical phases is the battle staff training (BST) where the Joint Staff conducts force integration training at the staff level and prepares for the execution phase. One option might be to directly connect the BST to the execution in a sense that during the BST plans are developed and subsequently executed before the execution phase in a simulated environment so that the results are available at Startex. This would provide valuable feedback to the Training Audience about the validity and feasibility of their original plan. Another option would be to organise specific table-top exercises for General Officers in which they are subjected to a Multi-Domain scenario. A final suggestion would be to re-introduce Command Post exercises like those conducted during the Cold War which involved Operational Joint staffs, Strategic Commands and National Headquarters, including politicians. Scholars of the time know these as the WINTEX/CIMEX exercises. These scenarios could be used to address the full complex environment of Multi-Domain Operations and could start the thinking processes required to deal with the kind of threats and challenges we are confronted with today.

Lieutenant Colonel Ed Wijninga (RNLAF) is currently serving in the Education, Training, Exercises and Lessons Learned Section. He has supported the Steadfast and Trident NATO CPX exercises as Chief OPFOR Air for the past six years.



Doolittle Series 18 Multi-Domain Operations



Courtesy of Air University Press, Web Edition, 9 January 2019, Lemay Center for Doctrine Development and Education

Note: Except for the Assessment done by the JAPCC, below is a summary of the article from 'Doolittle Series 18: Multi-Domain Operations.'

A Table Top Exercise to Explore Multi-Domain Warfighter Concepts

he Doolittle Series (DS18) was chartered by the Chief of Staff of the United States Air Force to explore Multi-Domain warfighting concepts to improve command and control of air, space, and cyberspace forces in support of dynamic and operationally agile operations. The event held 6–8 November 2018 at the LeMay Center Wargaming Institute, Air University, was the first in this series.

Three teams were assembled with individuals having backgrounds in cyberspace, electromagnetic spectrum, space, air, ISR, nuclear operations, legal, and Air Force special operations. There were also participants from the Royal Air Force and the Royal Australian Air Force. Each team was presented with the same scene-setting scenario of fighting a peer competitor in the 2030 timeframe while having to constrain simultaneously another peer competitor.

Team #1 was to maintain the 'Status Quo' of organization and policy, but was allowed to slightly modify the current C2 architecture.

Team #2, 'Status Quo Redesigned,' was encouraged to modify 'within the box' the current C2 architecture and use likely technology.

Team #3, 'Clean Sheet Unconstrained' was encouraged to look at technology within the realm of the possible and create an 'outside the box' MDC2 architecture.

Doolittle Series 18 Concepts and Objectives

DS18 specifically examined Multi-Domain Command and Control (MDC2) with the hypothesis that, 'The USAF must modernize rules, responsibilities, relationships, and authorities and tactics, techniques, and procedures (TTP) to effectively command and control (C2) Multi-Domain Operations to converge air, space, and cyber capabilities to meet the challenges of these contested domains.' To test the hypothesis, the following objectives guided DS18's development and execution:

1. Examine the opportunities and limitations regarding commanders' authorities, command relationships, and their collective abilities to exercise command and control at the operational level.

2. Examine the C2 mechanisms and processes the respective commanders use to exercise authority and direction to facilitate integrated planning and synchronized execution of operations to achieve integrated effects across the Air, Space, and Cyber domains.

3. Examine Air, Space, and Cyber effect timelines and tasking order processes (to include classification restrictions) to achieve integrated effects across the Air, Space, and Cyber domains.

Cross-Cutting Observations

Analysis of the interviews conducted with game participants and comments made during the game and by senior facilitators found three cross-cutting observations.

OBSERVATION 1: Invest in a shared data 'cloud' backed by resilient/reliable/secure communication network.

Discussion: The two teams with freedom to manoeuvre from the Status Quo both cited the need for a shared data network, even Team #1 team emphasized the need for reliable communication networks and nodes to secure and enhance current C2 operations. The backbone of any system discussed during this exercise was access to and manipulation of large amounts of information. Terms used to describe these data networks were 'robust' and 'self-healing', a network back by multiple nodes with multiple machine-to-machine access points. Team members stressed the need for 'cloud' based data storage, machine learning, algorithmic targeting solutions effects pairing with tasks, an application-based interface, and a common data standard. The use of Artificial Intelligence (AI) was emphasized to automate many, if not most, AOC processes, and a robust global communication network would need to be in place for this to be possible.

OBSERVATION 2: There is a need for highly trained and operationally experienced personnel in Command and Control.

Discussion: It is important to understand current C2 structure in order to build future C2 structures, and a first and key enabler to exercise MDO is training. Observations across the teams during this exercise showed an apparent lack of knowledge of the overall C2 structure and, specifically, an overall lack of familiarity and experience with C2 processes in domains players are not familiar with. For example, a cyber-player did not understand Space C2. A senior leader commented that many players had a lack of understanding of the processes in an AOC and resulting products. Much of the discussions on the first day focused on gaining a shared understanding of the current C2 structure. As the exercise progressed, players consistently commented on the need for larger exercises to integrate Multi-Domain Operations. The integration of Multi-Domain operators in large exercises should foster support for and training on MDO while providing participants needed experience. In addition to large exercises, a global communications system could provide training in a real-time environment. Teams suggested that training should consist of less white cards and more realism.

OBSERVATION 3: The capability to integrate Coalition partners needs to be built into new MDC2 hardware and software from the beginning.

Discussion: Coalition access to data and the network was identified as key. The teams thought that this would require addressing classification, access to the network and the 'cloud' from coalition locations, and a mechanism to allow easy, yet selective, access to information of varying levels of classification. The teams thought that coalition capabilities/effects need to be 'baked in' when planning operations rather than 'tacked

on.' To accomplish this may require significant policy changes where a standing Alliance is formed rather than ad-hoc coalition to deal with an unplanned crisis. However, there are things the US military can do to improve coalition integration into MDC2. For example, when Team #3 group proposed new command relationships, the terminology and definitions were modified to use terms and concepts understood by the RAF and the RAAF. In addition, the post-DS18 surveys pointed out that there may be a situation where the US is not the lead in an operation, and how the US would integrate its MDC2 into that coalition's command and control.

OBSERVATION 4: Push capabilities and authorities to the lowest level possible.

Discussion: All teams stressed the need for a fast and agile C2 structure to quickly respond and counter threats from a peer competitor. In order to increase the speed of their C2 structure, teams recommended pushing capabilities and authorities to the lowest level possible. Pushing authorities down to trained personnel who understand the employment risks allows those personnel to perform C2 faster. Currently there are a lot of unknown risks in the MDO environment and those risks need to be quantified, with the potential for holding some risks at a higher level. This could lead to a structure built on conditions-based authorities and allow quick reaction to known scenarios.

In order to push authorities to the lowest level capable of integrating MDO, those authorities and supported/supporting relationships need to be defined. All teams said that supported/supporting relationships are not well-understood. In a global fight, with multiple problems, the relationships between combatant and functional commanders is very important.

OBSERVATION 5: Each team included a Multi-Domain Operations Center (MDOC).

Discussion: Each team saw a need to incorporate various forms of a Multi-Domain Ops Center into their command structure. Team #1 placed an MDOC directly under the Joint Forces Air Component Commander. The MDOC would operate as a planning cell in direct support of the JFACC to integrate effects. This MDOC would include liaison officers from the functional combatant commands. Team #2 designed a virtual MDOC using cloud-based technology and limited use of Artificial Intelligence. This virtual MDOC would combine inputs from all planning levels to build an integrated battle plan. Users could make inputs and adjustments regardless of location as well as have a common picture of the battlespace. Team #2's focus was on unity of effort rather than unity of command. Team #3 incorporated an MDOC at the Global Command level with MDOC functions replicated at lower echelons. Various functions of this future MDOC would be fully automated and led by advanced Artificial Intelligence, with a human in control of critical decisions. This Al-led MDOC would continuously calculate COAs based on current conditions and support various Mission Task Groups.

Assessment of the outcome of the Table Top Exercise to explore Multi-Domain warfighter concept.

The availability of information and the processing of large amounts of information is key to a successful MDO. Therefore not only full availability of the communication network is a must but due to the vast amount of information, the required knowledge of all possible domains (AIR, LAND, SEA, SPACE, CYBER), all possible effects and employment risks, makes the use of AI inevitable to support highly trained MDC2 teams in large scale exercises. Furthermore, a paradigm shift from Need to Know to Need to

Share over all domains and all participating allies, including the AI, is imperative. Where to put MDC2 in our organizations remains a question. Whether it will be centralised or decentralised or even replicated by AI over all levels, with only a man in the loop for critical decisions, should be a major vector in the development of new concepts within NATO.

Endnotes

1. Source: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/LP_0003_Multi_Domain_Operations.pdf

Multi-Domain Operations and Counter-Space

We need to train a Space Mission Force. We need our space operators focused on what to do in case of a threat and to operate through the threat environment.

General John Hyten, April 2016

By Major Richard W. Gibson Courtesy of Small Wars Journal

here is still much work needed for US forces to not be hamstrung by the capabilities of peer and near-peer competitors. China over the last decade has become a peer adversary. Much of this change in status is due to its investment in emerging technologies, specifically huge strides in space launch and spacecraft capabilities. Of concern is emerging counter-space capabilities.

China has developed a counter-space strategy that involves creating a denied, degraded and disrupted space operations environment (D3SOE) against the US government and military in future conflicts. China plans to employ its counter-space strategy through an Anti-Access/Area Denial environment (A2/AD) and the use of anti-satellite weapons (ASAT).

One US development that may help mitigate A2/AD capabilities is the creation of the Multi-Domain Operations (MDO) concept and the Multi-Domain Task Force (MDTF).

Crux of the Problem

The Multi-Domain Operations concept began as a joint US Army and Marine Corps white paper in October 2016. It specifies that the crux of the problem statement is ground combat forces, operating as part of joint, inter-organizational and multinational teams, are not sufficiently trained, organized, equipped or postured to deter or defeat highly capable peer enemies to win in future war.¹

The white paper states, '[a]dversaries will counter US strengths such as air and maritime superiority, and degrade key capabilities by limiting access to space, cyberspace, and the [electromagnetic spectrum]. Adversaries will also exploit perceived US weaknesses such as time and distance for force deployment, logistics nodes, and vulnerable command and control networks.'²

Major General William K. Gayler, commander of the US Army Aviation Center of Excellence and Fort Rucker, said Multi-Domain Operations will be helpful given that potential enemies have observed the US military's strengths. Using their own technologies and tactics, those nations are seeking to overcome US advantages in the five domains: space, air, land, sea and cyberspace.³

For example, the Chinese People's Liberation Army has 'emphasize[d] the necessity of 'destroying, damaging, and interfering with the enemy's reconnaissance ... and communications satellites,' suggesting that such systems, as well as navigation and early warning satellites,

could be among the targets of attacks designed to 'blind and deafen the enemy.'⁴

Multiple Options

Incorporating long-range precision strike, integrated air defence, electronic warfare and cyberspace capabilities, MDO creates multiple difficulties for adversaries and multiple options for national leaders and Joint Force commanders.⁵ Army and Marine Corps forces can project persistent, land-based power into other domains for fully integrated joint manoeuvre and joint operations.

The MDO concept was formulated when the US military was transitioning from counter-insurgency conflicts in the Middle East to the prospect of dealing with a peer adversary on the modern battlefield. A significant aspect of this concept is development of the Multi-Domain Task Force.

General Mark A. Milley, the 39th Army Chief of Staff, stated that the task force is 'a relatively small organization ... 1,500 or so troops. That organization will be capable of space, cyber, maritime, air and ground warfare. So smaller dispersed, very agile, very nimble organizations–that are networked into other lethal systems that are delivered by either air or maritime forces–will be essential to rip apart the A2/AD networks.⁷⁶

Milley understood that the counterinsurgency fights in the Middle East have left the US military challenged by peer adversaries in Eastern Europe and East Asia. He stated, '[I]and-based forces now are going to have to penetrate denied areas for the rest of the joint force while having the capacity to operate in all domains simultaneously.'⁷ A major player in MDTF experimentation is US Army Pacific Command, currently commanded by General Robert B. Brown. Under Brown's supervision, the command employed the concept in a series of major exercises in fiscal years 2017 and 2018 to test its validity against a peer competitor in a wargame environment. These tests have been ongoing now for about a year with the MDTF Pilot Program.

In a recent example, at the multinational 2018 RIMPAC exercise, US Navy P-3 and P-8 antisubmarine aircraft flew alongside Army Gray Eagle unmanned aircraft systems and AH-64E attack helicopters.

Brown stresses that cross-domain effects are not entirely new, citing the example of Multi-Domain effects created by the introduction of airplanes and submarines during World War I. He states that to achieve success with this new approach, there has to be a change in mindset and culture. Brown describes the three essential elements of the Multi-Domain concept as joint integration, technology and people.⁸

Dealing with a Peer

The Chinese have researched and adapted to the perceived US advantages in technology, specifically in the space domain. They have adopted strategies to counter those advantages through the development and acquisition of a direct-ascent ASAT; missiles designed to strike mobile platforms at sea; a robust cyber force; and space-based assets. China's overall strategy is an overarching plan of increased defence spending and technological advances that have catapulted China to the status of a peer adversary for the United States.

Testing of the ASAT in 2007 and 2014 is one A2/AD capability where China has demonstrated proficiency. The tests highlighted China's

capability to launch a weapon to both lower earth and geostationary orbits, which threatens all US space-based assets. Many military experts have argued that China will use this type of weapon early on in a conflict with the United States to degrade capabilities, such as GPS, that are dependent on space-based assets.

Another tool of the A2/AD fight that China has invested in is electronic warfare/jamming assets designed to degrade adversaries'GPS and satellite communications satellites and ground-based facilities. Chinese electronic warfare capabilities, specifically jamming, are focused on denying an adversary the use of space-based capabilities, thereby removing a position of advantage.

One key recognition in the MDO concept is that US forces currently are not sufficiently trained, organized, equipped or postured to deal with a peer adversary. The concept also addresses the lack of awareness by senior leaders in regard to fighting in a degraded space environment.

The MDO white paper states that headquarters and subordinate units must be capable of operating in a degraded operational environment. The paper further states that the US Army must reduce vulnerabilities through more redundant and survivable systems in such areas as Positioning, Navigation and Timing.

Recognize and Train

The first order of business is to recognize biases that military leaders have and how they are anchored in their beliefs. One of the biggest unrecognized biases is the anchoring effect. Psychologist Daniel Kahneman states that the anchoring effect happens when people consider a value for an unknown quantity before estimating the quality.⁹

Therefore, leaders must first realize the characteristics of the space domain before they make an assessment on its value. The method to approach this is through institutional, home station and Combat Training Center (CTC) education and training.

The Army Space Training Strategy is gaining momentum with the Army's manoeuvre force as training teams deliver instruction at unit homestations and at Combat Training Centers. A continued emphasis from strategic down to tactical-level leaders is a practical solution to developing situational understanding across the force about degraded space operations. More realistic and demanding training on all facets of space-based capabilities ensures the United States achieves success in any conflict.

A major training objective during CTC rotations is to degrade and deny GPS reception through electromagnetic interference techniques for a fixed period. One of the common observations during this training was that most units did not recognize the importance of using mitigation techniques, such as encryption of GPS devices, prior to training. Also, units did not realize they were in a degraded environment and sometimes operated poorly in the situation.

Mobile training teams have noted that many of the CTC observer/controllers were able to provide immediate feedback to units regarding the degraded space environment. They also observed that many units were incorporating D3SOE into their operations orders and into their overall mission success criteria.¹⁰ This specific awareness by soldiers and leaders across the US Army is essential for future conflicts.

The key observation made during these rotations was that units which operated effectively in the degraded space environment were those that had conducted D3SOE home-station training prior to their CTC rotation. Leaders of these organizations placed emphasis on this training objective so the unit would be prepared to fight in a degraded GPS and space environment.¹¹

Such training is vital to preparing US forces to operate effectively in a degraded space environment. The Department of Defense must ensure that there is continued emphasis placed on both home-station training and CTC rotational unit training in order for units to know how to fight in a disrupted space environment.

In a similar fashion, a critical component of the Multi-Domain Task Force's purpose is to ensure that leaders have a better understanding and appreciation for the correct space capabilities matched with the appropriate Army space professionals. Integration of both offensive and defensive space capabilities coordinated with the employment of cross-domain fires will enable the US Army and joint force to achieve desired effects. If space-based capabilities are integrated into the task force, the A2/AD and anti-space effects that an adversary like China will employ should be neutralized or at least degraded.¹²

The correct composition of people with the proper skill sets within the task force is critical for forward stationing in order to provide coordinated effects on the battlefield. Space professionals are a critical component, but other specialties bring critical effects to the fight. Members of the cyberspace and electronic warfare communities are critical to synchronizing non-lethal fires for exploitation to create the greatest advantage possible against adversaries.

One key issue that the MDFT will address is the authorities aspect to ensure that these effects are conducted in time and space with synchronization of the other domains. These task force members will play a critical role in the US military being able to extend its operational reach by countering the adversaries' attempts to degrade the space and other domains.¹³

Steps in the Right Direction

The MDTF concept is a step in the right direction in addressing the military problem of effectively fighting in a degraded space environment. The exercises in the US Pacific Command region over the next few years will provide the necessary feedback to assess the concept's feasibility in dealing with the D3DOE threat.¹⁴ US Army Pacific Command and the Army Training and Doctrine Command are collecting all relevant data to assess the concept in fiscal years 2018 and 2019 for future integration into doctrine and other exercises.

The last integral piece for the task force to deal with is the appropriate equipment disposition. The task force should employ appropriate available defensive and offensive space capabilities and capacities. Achieving that goal will take appropriations at the policy and strategic levels to procure the requisite amount of equipment. Doing so cannot be done overnight but can be planned and appropriated before 2030.

The MDO concept and the creation of the MDTF are much-needed changes in an emergent operational environment. These Multi-Domain approaches will ensure that the US Army and joint force will be properly trained, equipped and postured to deal with the conflicts presented by Chinese strategy.

Multi-Domain Operations and the Multi-Domain Task Force will ensure that the US Army creates opportunities for the land component to exploit against peer adversaries, and that these forces can effectively operate in an Anti-Access/Area Denial environment. The mandated Army Space Strategy and the Army Space Training Strategy will educate and train Army forces to operate in a degraded space environment.

The ultimate question is: Can the US Army effectively operate in a degraded space environment?

Both the Army Space Training Strategy and the MDTF pilot program are steps in the right direction, but it still might not be enough in a current conflict. It does highlight that the issues of a degraded space environment and Anti-Access/Area Denial capabilities of peer adversaries have been evaluated and are being addressed appropriately.

The current state of Army readiness for a degraded space environment is still in need of improvement. Much more education at the institutional level and training at the tactical and operational levels needs to occur. The MDO concept is currently under evaluation during various exercises with the MDTF Pilot Program, and the MDTF creation will facilitate changes in mindset and organizations for the future fight.

Only time will tell if the US Army and other military services can effectively fight in a degraded space environment, but current efforts and trends lead to an encouraging forecast shifting upward.

Major Richard W. Gibson, a space operations officer, is a future operations planner with the US Army's I Corps at Joint Base Lewis-Mc-Chord, Washington. This article is excerpted from his monograph for the School of Advanced Military Studies, US Army Command and General Staff College.

Endnotes

- Michael Redman, 'Multi-Domain Battle: Combined Arms for the 21st Century' (white paper, US Army Training and Doctrine Command, Army Capabilities Integration Center, 2016), p. 7.
- 2. Ibid., p. 5.
- David Vergun, 'Multi-Domain Operations to Exploit Enemy Vulnerabilities, Say Army Leaders,' Army News Service, 10 Sept. 2018, https://www.army.mil/article/210929/multi_domain_operations_to_exploit_enemy_vulnerabilities_say_army_leaders.
- Anthony H. Cordseman and Steven Colley, Chinese Strategy and Military Modernization in 2015 (Washington: Center for Strategic and International Studies, 2015), p. 37.
- 5. 'US Army Pacific Contributions to Multi-Domain Battle,' brochure, US Army Pacific, 15 Mar. 2017.
- Sydney Freedberg Jr., 'New Army Unit to Test Tactics: Meet the Multi-Domain Task Force,' Breaking Defense, 21 Mar. 2017, http:// breakingdefense.com/2017/03/new-army-unit-to-test-tactics-meet-the-multi-domain-task-force.
- Nathan A. Jennings, 'Realign the Army for Multi-Domain Battle' (Arlington, Va.: Association of the United States Army, 11 Apr. 2017), https://www.ausa.org/articles/realign-army-multi-domain-battle.
- 8. Robert B. Brown, 'The Indo-Asia Pacific and the Multi-Domain Battle Concept,' Military Review (Sep.-Oct. 2017), p. 15.
- 9. Daniel Kahneman, Thinking, Fast and Slow (New York: Farrar, Straus and Giroux, 2011), p. 87.
- 10. Joan Rouseau, 'G37 HST and CTC Rotation Observations,'USASMDC/ARSTRAT Observations, Jun. 2017, p. 4.
- 11. Ibid, p. 5.
- 12. Todd South, '4-Star: Multi-Domain Battle Will Fundamentally Change How the Army, Other Services Fight,' Army Times, 8 Oct. 2017, https://www.armytimes.com/news/your-army/2017/10/08/4-star-multi-domain-battle-will-fundamentallychange-how-the-army-other-services-fight.
- 13. Ibid.
- 14. Redman, p. 5.



Cyberspace and Multi-Domain Operations

X1

By Lieutenant Colonel Paul MacKenzie, CAN, Air Force Joint Air Power Competence Centre

t has been two years since NATO recognized Cyberspace as a Domain of Operations¹ (8 July 2016) and progress is being made along many lines of effort toward implementation, most of which are outlined in the Roadmap to Implement Cyberspace as a Domain of Operations.² With respect to some other key efforts underway in parallel, the North Atlantic Council (NAC) approved the Military Vision and Strategy on Cyberspace as a Domain of Operations on 12 June 2018³ and the final draft of Allied Joint Publication (AJP) 3.20 Doctrine of Cyberspace Operations was submitted to the NATO Forum for harmonization early this year and should be ratified before the end of 2019.⁴ While the progress to date on these key elements is promising, having agreement on the message in these documents is only the beginning on the way ahead to realizing the full potential of Cyberspace as a Domain of Operations. Gaining competence in the integration of Cyberspace operations with operations in other domains for conducting Multi-Domain Operations will be a significant advancement in the ongoing military operationalization of the Cyberspace Domain.

Since the introduction of personal computers and web-based services in the early 1990s, militaries have experienced a rapid evolution in their use

of Cyberspace capabilities. Information Technology (IT) and Communications and Information Systems (CIS) transformed how operations are planned and conducted. From improving the speed and efficiency of communications, data processing and general administration, the explosive developments (in keeping with the predictions of Moore's Law⁵) have seen IT/CIS transform from being a force multiplier, to an enabler of operations in other Domains, to the declaration of a Cyberspace Domain of operations. Despite this declaration, planners struggle to adopt these new capabilities into mainstream military operational planning in parallel with capabilities in the traditional physical domains. Air Power history enthusiasts are aware of the early stages of air capabilities when they were portrayed as merely support to land operations, such as for conducting reconnaissance. General Keith Alexander (former head of US Cyber Command and the National Security Agency) is on record for noting the challenge to integrate Cyberspace as a war-fighting domain is 'strikingly similar to what our military faced during the Interwar years from 1919 to 1938' in understanding air-power.⁶ The development of Air Power in the last century has been astronomical, such that our Joint Doctrine stipulates that we must have air superiority in the area of operations lest we risk significant losses or even mission failure. The development of capabilities in Cyberspace is proceeding exponentially faster than those of the Air Domain for a number of reasons but largely because it is orders of magnitude cheaper to develop capabilities in Cyberspace.

Maritime, Land and Air services are more mature than those operating in the Cyberspace Domain, with entrenched doctrine, and having exercised and executed Joint Operations for decades they are now exploring what it means to conduct Multi-Domain Operations. While military operations in the Cyberspace Domain are in their early phases of formation, they are developing rapidly. Still, it is not unusual, in fact quite common, to hear Commanders refer to Cyberspace as simply an enabler for operations in other domains. Until all levels of command recognize the potential

benefits of operating in Cyberspace, NATO will be disadvantaged compared to those actors who have grasped this potential and adapted their operational strategies accordingly. As stated in the NATO Vision, 'To fully establish cyberspace as an operational domain, clear cultural shifts ... are a prerequisite.⁷ In fact, operational effects may very well be achievable by the Joint Force Commander (JFC) through capabilities delivered primarily through Cyberspace capabilities alone. For example, if the mission is to achieve cognitive change and influence public opinion, this might be achieved via actions through Cyberspace. Attacks on government services and on critical infrastructure coupled with an Information Warfare campaign utilizing Cyberspace capabilities may influence the opinions of the general public such that they adjust their behaviour in the manner reguired for the mission. The key is understanding the desired impact – what the operations are intended to influence. The decisive conditions in an operational campaign may be achievable by variety of capabilities, not all of which operate in the traditional Domains. Therefore, it is necessary to transition from the view that Cyberspace is simply an enabler for operations in other domains to a paradigm in which all services from all Domains enable each other; being mutually enabling and interdependent. For example, as the Navy enables the Marines in amphibious operations, and the Air Force enables the Army in Land operations, Cyberspace can be an enabler for operations in other domains and can be enabled in return. The JFC must be able to integrate Cyberspace operations into joint and Multi-Domain Operations, as a co-equal participant. Mission success increasingly depends on freedom of manoeuvre in Cyberspace, and opportunities to project power in and through Cyberspace are evolving.8 'Commanders cannot continue to run the risk of inappropriately delegating key decisions because they and their staffs lack an understanding of the domain.'9 For NATO, the Cyberspace Operations Centre (CyOC), which stood up in August of 2018 as part of the adapted Command structure, will establish the equivalent of the Cyber Component staff for the theatre commander. The CyOC staff participated in its first exercise (Trident Juncture) in November 2018, and is anticipated to be fully operational with a staff of 70 persons, by 2023.¹⁰ Some may argue how NATO can consider Cyberspace a Domain when NATO will not develop offensive capabilities in Cyberspace. To partially mitigate this shortfall, several nations have voluntarily offered to provide sovereign Cyberspace capabilities in support of NATO operations, though the mechanics for this process have not yet been determined.¹¹

[Note: Whether and/or how Cyberspace, Electronic Warfare and Space will evolve, transform, or evenly potentially merge, is a subject a number of experts in each of these fields think are topics worth exploring in the near future.]

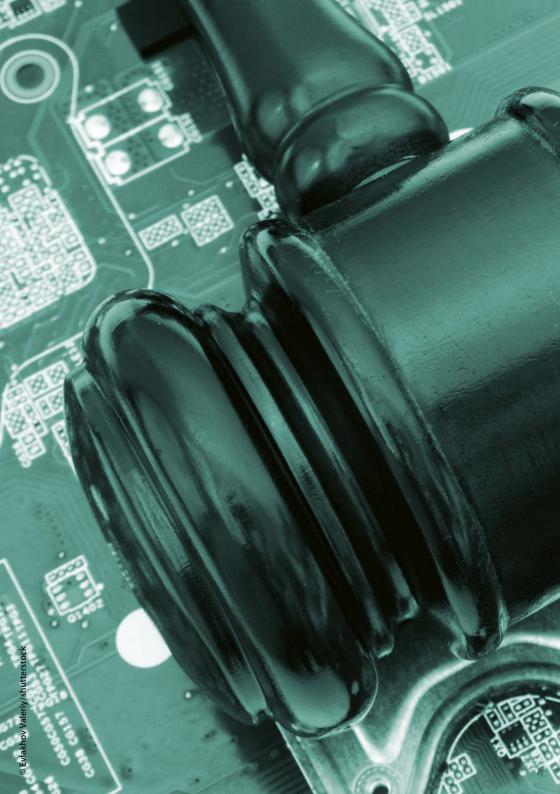
As stated in the recently published Allied Joint Doctrine for the Planning of Operations,¹² 'although all operations are unique, they can be approached in the same manner'.¹³ The objective in applying the operational art is to 'determine how to employ the joint force with best effectiveness.'¹⁴ Understanding the Cyberspace Domain and how capabilities operate in and through Cyberspace, particularly when synchronized with Joint functions in a Multi-Domain operation, is fundamental to the planning to meet the Commander's Intent and critical to support the ways and means for reaching the Decisive Conditions needed to achieve the desired end state in the operational design. Multi-Domain Operations are not dissimilar to Joint operations as they concern 'fields of activities which are not separated, but are in fact mutually combined and balanced for the desired outcome.'¹⁵

Planning for Multi-Domain Operations will be disastrously incomplete without the integration of operations in and through the Cyberspace Domain. Each of the military operational Domains are mutually-enabling, therefore mission success in Multi-Domain Operations in the future will be in doubt unless military planners apply to the Cyberspace Domain the operational planning processes that have been so successfully conducted for operations within the traditional Maritime, Land and Air Domains. Achieving the necessary cultural shift to accept this new reality and generating the cadre of professionals to implement the steps necessary to entrench the Cyberspace Domain in military operations are themselves decisive conditions toward the end state of fully integrating Cyberspace operations into Multi-Domain Operations.

Lieutenant Colonel Paul J. MacKenzie (RCAF), JAPCC Cyberspace SME, examines the many facets of Cyber as it relates to NATO Joint Air Power and from a defensive perspective through to the potential in exploiting offensive effects.

Endnotes

- 1. NATO, Warsaw Summit Communiqué, https://www.nato.int/cps/en/natohq/official_texts_133169.htm, accessed 29 Apr. 2019.
- 2. Approval of the Roadmap to Impliment Cyberspace as a Domain of Operations PO(2017) 0072 (INV) 10 Feb. 2017 (NR).
- 3. NATO, MC 0665 Military Vision and Strategy on Cyberspace as a Domain of Operations, 12 Jun. 2018.
- 4. E-mail, Clare Lane CCDCOE (AJP 3.20 Custodian).
- 5. Moore's law simply put means processing power of computers will double every 2 years.
- 6. K. B. Alexander, 'Warfighting in cyberspace,' Joint Forces Quarterly, vol. 3rd Quarter, 2007, p. 61.
- 7. Ibid. 3., p. 4.
- Williams, Brett T. The Joint Force Commander's Guide To Cyberspace Operations, Joint Force Quarterly 73, 2nd Quarter 2014, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73_jfq-73_12-19_Williams.pdf, accessed 29 Apr. 2019, p. 12.
- 9. Ibid., p. 13.
- Underwood, Kelly, NATO's Answer to Cyber Warfare, The Cyber Edge, SIGNAL Magazine, 1 Apr. 2019, https://www.afcea.org/ content/natos-answer-cyber-warfare, accessed 29 Apr. 2019.
- Freedberg, Sydney J., NATO To'Integrate' Offensive Cyber By Members, Breaking Defense, 16 Nov. 2018, https://breakingdefense. com/2018/11/nato-will-integrate-offensive-cyber-by-member-states/, accessed 29 Apr. 2019.
- 12. NATO AJP 5.0 Allied Joint Publication for the Planning of Operations, Feb. 2019.
- 13. Ibid., p. 15.
- 14. lbid., p. 17.
- 15. lbid., p. 83.



Tracing Opinio Juris in National Cyber Security Strategy Documents¹

X11

By Ann Väljataga, Law Researcher, NATO Cooperative Cyber Defence Centre of Excellence. The article below is a summary of Ann Väljataga, 'Tracing Opinio Juris in National Cyber Security Strategy Documents', NATO CCD COE, Tallinn, 2018.

n this study, Ann Väljataga, a law researcher at the NATO Cooperative Cyber Defence Centre of Excellence, reviews the national cyber strategies of the United States, United Kingdom, Netherlands, China, France, Russia and Australia. She examines the cyber strategies in the context of sovereignty, foreign interference, thresholds to be considered an attack, the sufficient grounds for assigning responsibility/attribution and, lastly, how states might respond. The following paragraphs are a summary of the salient points of Väljataga's study.

With cyber law still in the early stage of formation, opinio juris could at least, ideally, compensate for underdeveloped and/or incoherent legal practice, since strong positions regarding national postures in cyber-space as of now are still more often expressed or communicated than practiced. Ms Väljataga writes that, since international law is ultimately made by states and states alone, national declarations expressed in National Security Strategies, though not containing legally binding norms, reflect the nation's overarching belief in existing or desired norms.

Consequently, and while they tend to be, intentionally, overly generic and cautious, they contain aims that states deem realistic, desirable and achievable and reveal prevalent legal opinion.

Sovereignty

Having no formally recognized obligations with respect to sovereignty in cyberspace allows states to conduct cyber operations on other nations without contravening international law. At the same time, this void weakens any protection international laws would offer against cyberattacks. National positions vary on cyber sovereignty, ranging from its perception as an infringement-immune environment (as in the cases of the US and UK where the concept is as abstract as the principle of sovereignty itself²) to where infringements are advocated as binding in nature, as in the case with the bi-national accord between Russia and China.³ Sovereignty implies obligations and, therefore, due diligence, meaning an expectation of exerting a reasonable amount of control over national cyberspace infrastructure. For some this opens up an avenue to permit more aggressive states to operate with a degree of impunity, but is intended to mean the duty to pursue controls over infrastructure just as nations foster support to countering international terrorism. In the end, any obligations from due diligence depends on context.

Based on the review of the national cyberspace strategies the following conclusions can be reached:

- Sovereignty applies in cyberspace.
- Sovereignty can be threatened and needs to be protected.
- Due diligence follows from cyber sovereignty (and is sometimes interpreted to involve a level of capacity building to assist those nations unable to contribute to the global effort).

• There is no agreement in whether or how cyber due diligence can be the basis of state responsibility.

Foreign Interference

Regarding foreign interference, the author references Australia's international cyber strategy and foreign policy documents both announcing its intention to exercise strict sovereign control to protect the integrity and cohesion of its borders and infrastructure from coercive power. Unwanted foreign influence includes hybrid and information operations, and though perhaps not technically unlawful in themselves, constitute breaches of sovereignty according to Australia.⁴ This differs from the US and the UK who argue that a breach of cyber sovereignty is not a wrongful act since sovereignty is an underlying principle and not a binding rule, and that something more grave, a clearly prohibited intervention in domestic affairs, would mark the threshold for a wrongful act. US strateay avoids cyber sovereignty terminology throughout the document.⁵ UK strategy notes cyberspace as just a sphere in which national interests must be defended to contribute to broad national security, just as actions in the physical sphere. This leads to the question whether something that cannot be violated should be defended. Ultimately, no state commits to recognizing foreign intervention (such as election meddling) as prohibited and justifying proportionate countermeasures, nor whether cyber espionage is anything more than a legally-controversial but necessary evil.

Threshold as Use of Force/Armed Attack

There is no agreed upon threshold to trigger a nation to respond. If the UK position on cyber sovereignty is obscure, the criteria for the threshold for necessitating a response in self-defence is not much clearer. An

attack on the banking system causing severe financial damage to the state and economic security for the people would constitute a use of force.⁶ A cyber-attack on the scale of one against nuclear reactors or Air Traffic Control resulting in large scale loss of life is considered grave, an attack on the scale of which reaches the threshold to trigger the UK to take action in self-defence. Cyberattacks leading to serious disruptions with long-term consequences, such as on the financial systems or government preventing the execution of essential services is the threshold for the Netherlands to qualify as an armed attack and to assert its right to defend itself. Australia caveats some of the parameters to assess threshold such as the intent, whether the effects are direct or indirect and whether the cyber activity could have reasonably been expected to cause extensive damage, destruction or loss of life. However, they also express concern about the cumulative effect on international peace and security of continual low-scale, malicious activity, that they can be treated as reaching the threshold of armed attacks if/when their cumulative effects achieve the same scale. Many of the strategies merely hypothesize of the possibility of cyberattacks reaching the scale of an armed attack but few offer specific examples. Ms Väljataga concludes that there is no factual consensus on what consequences meet the criteria of either the use of force or an armed attack and remarks that grave kinetic consequences are not always viewed as the absolute litmus test.

Attribution

Ms Väljataga indicates there was a breakthrough in 2014 with respect to attribution with the attack on Sony being publicly attributed to North Korea, and again with the US indictment in 2017 of two Russians for hacking, espionage and other criminal activity conspiracy. Germany was the target for a number of attacks from 2015–2016 on its parliament and parties and attributed these and the world-wide NotPetya virus (of 2017)

to actors with ties to Russia. The author cites the most clear-cut attribution to date being a 14 Oct 2018 news release from the UK whereby the Foreign Office candidly, and with high confidence, accused Russian foreign intelligence services of conducting four major cyberattacks that constituted a flagrant violation of international law. Overall, however, the predominant tendency is for states to concede that attribution is difficult to achieve and advancement is required through sharing intelligence and enhancing digital forensics. The French believe attribution is a state level function, part of state duty for practicing due diligence discussed earlier, while the Netherlands support a three-part formula, requiring technical (detection) and political attribution as prerequisites to legal attribution. Most incidents for which there has been public attribution have not progressed beyond the technical and political levels, perhaps because closer discrimination would bring into question what counts as effective control over infrastructure. Consequently, attribution is looked upon more as a naming and shaming method for deterrence. The US refrains from legal terminology altogether indicating its intentions to attribute and deter through swift, costly and transparent consequences. Overall, the national strategies have very little reference to legal attribution at this time.

Response

The Netherlands indicates in its 2018 cyber strategy that it is open to the integration of offensive cyber actions as well as contributing same to NATO operations.⁷ Also, for instance the Czech strategy has direct examples of their capacity and intention of developing capabilities to respond (defensive and offensive)⁸ and the UK has expressed intentions to become the world leader in offensive cyber capabilities. The Australian strategy includes an array of responses including, but not limited to, offensive cyber capabilities, followed by the explanation that they will

only be deployed in accordance with the principle of proportionality. The French would include measures to characterize and neutralize the attack to include influencing systems at the origin, including the possibility of pre-emptive as well as anticipatory defence measures.⁹ The UK aims to have the capability to respond to cyberattacks as it does to any other attack and by whatever means is the most appropriate, including cyberattacks to cause damage, disruption or destruction.¹⁰ The author points out that collective countermeasures are currently prohibited under positive international law, which raises the guestion how NATO can legally employ sovereign offensive cyber capabilities provided voluntarily by Allies for operations. However, all of the strategies examined acknowledge that the majority of cyber operations at the moment take place below the threshold of armed attack and, correspondingly, emphasis has shifted from self-defence to countermeasures. Consequently, national strategies are trending toward prevailing over the ban on collective countermeasures in cyberspace whether in near or farther future.

Summary

The author concludes that cyber opinio juris is in a formative stage, almost always extremely vague and discreet. However, national cyber security strategies can contain legally binding norms states intend to convey to the international community. Sovereignty is recognized predominantly as a parameter that can be violated and for which states have obligations and responsibilities. All nations condemn foreign interference via cyber, but there are no agreed-upon criteria for categorizing the use of force or an armed attack. It is generally accepted that countermeasures (including collective and anticipatory) not self-defence alone, are the key to combatting cyberattacks, and some strategies introduce legal aspects on attribution for consideration.

Questions to Stimulate Discussion:

Considering Command and Control (C2) of Multi-Domain Operations (MDO), does having the decision for both thresholds for attack and attribution at the political level inhibit operational commanders from responding in a timely fashion with appropriate countermeasures and through any domain?

Can mechanisms be put in place to expedite C2 and liaison between political and operational levels if decisions with respect to threshold and attribution remain at higher levels. Can this be expedited to something similar to the executive decision scenario between the Commander-in-Chief and the Commander of a Ground-Based Air Defence Unit on whether to engage a hijacked Aircraft?

Is it feasible to create Rules of Engagement (ROEs) to the potential of decision-making hindering the Commander's OODA loop?

Endnotes

- 1. Väljataga, Ann, Tracing opinio juris in National Cyber Security Strategy Documents, https://ccdcoe.org/library/publications/ tracing-opinio-juris-in-national-cyber-security-strategy-documents/, accessed 1 Mar. 2019.
- 2. Schmitt, M., 'In Defense of Sovereignty in Cyberspace', Just Security, https://www.justsecurity.org/55876/defense-sovereigntycyberspace/; Corn, Gary P., and Robert Taylor.
- 3. China, Joint statement between the presidents of China and Russia, Jun. 2016, Article 1.
- Australia, 2017 Foreign Policy White Paper, Chapter V: Open, Free and Secure Syberspace, available at: https://www.fpwhitepaper.gov.au/foreign-policy-white-paper/chapter-five-keeping-australia-and-australians-safe-secure-and-free/open.
- National Cyber Strategy of the United States of America, Sep. 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.
- United Kingdom Ministry of Defence, Cyber Primer 2nd Edition, 2016, available at: https://assets.publishing.service.gov.uk/ government/uploads/system/uploads/attachment_data/file/549291/20160 720-Cyber_Primer_ed_2_secured.pdf.
- 7. Australia, Cyber Engagement Strategy, supra note 27, p. 36.
- 8. Czech Republic, National Cyber Security Strategy, p. 18.
- François Delerue, Aude Géry, France's Cyberdefense Strategic Review and International Law, Lawfare, 23 Mar. 2018, https:// www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law.
- 10. UK, National Cyber Security Strategy 2016–2021, p. 51.



The Executive Director's Closing Remarks

Lieutenant General Klaus Habersetzer, DEU, Air Force Executive Director, JAPCC

hope that you've found the series of essays provided in our Conference Read Ahead informative and enlightening. Our desire is that these essays will provoke thought and stimulate discussion about the role of Joint Air Power in a multi-domain operation in preparation for our upcoming conference. I wanted to take this opportunity to offer my perspective as the Executive Director of the Joint Air Power Competence Centre, highlighting some of the topics presented by our authors.

The first two articles will help to explore a working definition of what a Multi-Domain Operations actually is and should be taken as a starting point for the discussions in our first panel. This is especially important as there is no commonly agreed definition of MDO in NATO or its Nations right now, although it has become a buzzword in recent years and new domains such as cyber and space have emerged.

We may argue that multi-domain is merely a more modern way of describing jointness, whereas jointness encompassed the traditional domains of air, land and sea. Simply adding the new cyber and space domains to the list and label it MDO is however not sufficient. The seamless integration of five domains is likely to add a lot more complexity to Command and Control procedures, which have to ensure the coordinated and synchronized execution of actions and delivery of effects from all the different domains. This is also highlighted by the next two articles and I want to quote from General S. Townsend's article that 'this change is not cosmetic – it is about growing an idea to its greatest potential in order to change the way we fight today ...'

The integration of cyber and space-based effects opens a completely new 'toolbox' for the Joint Force Commander to pick suitable military actions from, ranging from pre-emptive to reactive and from non-lethal to lethal. In this regard, we may also argue if NATO's Joint Force Command structure is still suitable for an MDO.

Fully integrating five domains into our existing 'three-domain' architecture likely requires significant improvements and upgrades of NATO's current C2 infrastructure and will be a major enterprise comparable to the integration of our 5th Generation jets into NATO's fleet of legacy aircraft. This 'next generation' C2 infrastructure will be even more reliant on the electromagnetic spectrum, space and cyberspace as information gathering, sharing and communications will be essential for Multi-Domain Operations.

Therefore, the initial phase of a potential future conflict against a peer adversary will probably be shaped by the fight for superiority in the electromagnetic spectrum, space and cyberspace. Air Power will have to contribute to each of these objectives while at the same time operating in and dealing with a heavily defended and contested airspace.

I am really looking forward to discuss the role of Air Power in an MDO and the challenges it will present to us with you and our distinguished speakers and panellists.

In closing, I hope you have enjoyed reading the articles and that they have piqued your interest in this year's topic of Shaping NATO for Multi-Domain

Operations of the Future. I firmly believe that your expertise will be required to successfully navigate the coming years and I invite you to be a part of providing ideas and solutions for the continued success of the Alliance.

I sincerely hope to see you this fall in Essen.

Klaus Habersetzer Lieutenant General, DEU AF Executive Director, JAPCC

Conference Itinerary

8 October 2019

Icebreaker and Industry Showcase

9 October 2019

Inaugural Session with JAPCC Director's Opening Address

Keynote Speech

Panel 1: What is a Multi-Domain Operation?

Director's Luncheon and Lunch Buffet

Panel 2:

What Requirements Go Along with a Multi-Domain Operation?

Director and VIP Tour of Industry Showcases

Networking Dinner and Industry Showcase

10 October 2019

Keynote Speech

Panel 3:

Which Challenges does NATO Face in Order to Meet the Requirements?

Lunch Buffet

Panel 4: What are the Future Enablers to Cope with the Challenges?

Wrap-up and Director's Closing Remarks

1001¹⁰¹ 10:11 0, 1100 10110 ₁, 1, 01 00 10110 1, 100 10110 1 0, 11 00 1, 100 1, 110 00 1, 100 1, 100 001 0, 1110011001(م, 01, 100 001 0, 110011001110, 100 01 0, 100 1, 10011001100110, 100 1, 000 1.011 11 00 1 00 110011 1 1 00 11 01 01₁₁ 001110011(



Joint Air Power Competence Centre

von-Seydlitz-Kaserne | Römerstraße 140 | 47546 Kalkar (Germany)

Visit us in the web:



