iesd
Institut d'études de stratégie et de défense
Faculté de droit
Université Jean Moulin - Lyon III

DECEMBER 2019

The Evolution of Command and Control (C2) in Multi-Domain Operations

John Gerlach

RESEARCH PAPER

Operational Concepts

About IESD

The **Institute of Strategic and Defense Studies (IESD)** is an academic research centre created in 2018 and specializing in strategic studies. The IESD is supported by the Université de Lyon (UdL) and belongs to the **Law School of Université Jean Moulin – Lyon III**. The institute consists of a multi-disciplinary team of researchers (Law, Political Science, Management, Economy) and unites a network of experts, researchers, PhD students and master students specialised in strategic studies.

The IESD is currently a candidate for selection as one of the Defense Ministry's (DGRIS)"National Centre of Defense Excellence" focusing on: "*Interconnection of high strategic functions (air power, space, nuclear deterrence, missile defense): political and operational implications of high intensity capability interactions in homogeneous spaces and contested commons*."

Director of IESD: **Olivier Zajec**

Site web : https://iesd.univ-lyon3.fr/
Contact : iesd.contact@gmail.com

IESD – Faculté de droit
Université Jean Moulin – Lyon III
1C avenue des Frères Lumière – CS 78242
69372 LYON CEDEX 08

RESEARCH PAPER

Operational Concepts

John Gerlach, « The Evolution of Command and Control (C2) in Multi-Domain Operations », *Note de recherche IESD*, coll. « Operational Concepts », n°1, December 2019.

Abstract

Throughout the past two decades, adversarial nations have capitalized on advancements in technology and are now capable of contesting operations in all domains. In order to counter this threat, the United States and its allies have adopted a Multi-Domain Operations doctrine. The complexity of this new strategy requires advancements in communications technologies, the adaptation of artificial intelligence, and a redesign of current command structures and processes. This research paper seeks to quantify the effects of Multi-Domain Operations on command and control. A comparative analysis is made between the current C2 challenges and capabilities. This analysis provides the context for the proposed recommendations of implementing force-wide information sharing technology, adapting artificial intelligence software, and accomplishing necessary structural reforms. The status quo is incapable of effectively responding to contested operations in a Multi-Domain environment. Command and Control must evolve.

Résumé

Au cours des deux dernières décennies, plusieurs Etats en compétition avec les Etats-Unis ont capitalisé sur les progrès de la technologie et sont désormais capables de contester la domination opérationnelle américaine dans tous les domaines. Afin de contrer cette menace, les Etats-Unis et leurs alliés ont adopté une doctrine d'« opérations multidomaines ». La complexité de cette nouvelle stratégie exige un progrès dans les technologies de communication, une évolution et une adaptation de l'intelligence artificielle, ainsi qu'une refonte des structures et processus de commandements actuels. Cette note de recherche a pour objectif de mesurer les effets des opérations multidomaines sur le commandement et le contrôle (C2), à travers la comparaison entre les capacités actuelles des C2 et leurs tâches futures. Cette analyse nous permettra de proposer plusieurs recommandations, comme la mise en place d'un système de partage d'information interarmées, l'adaptation des logiciels d'intelligence artificielle et la nécessaire mise en œuvre de réformes structurelles. Le statu quo n'est aujourd'hui plus en mesure de répondre efficacement à la contestation opérationnelle adverse dans un environnement multidomaine : le commandement et le contrôle doivent évoluer.

About the author

John Gerlach is an associate researcher in international security and defense at the University of Lyon III, Jean Moulin School of Law, Lyon France. He graduated Syracuse University (2006), with a Bachelor of Science in Aerospace Engineering and a Master of Social Sciences (2014). After graduating university, he was commissioned in the United States Air Force and received his pilot wings in 2008. He has completed multiple deployments in support contingency operations overseas piloting the C-17 Globemaster III aircraft. Prior to moving to France as part of the Olmsted Scholar program, he was an instructor at the United States Air Force Weapons School. Recently, John received his Master Degree in International Security and Defense (2019) from the University of Lyon III, Jean Moulin School of Law.

Table of Contents

The Evolution of Command and Control in Multi-Domain Operations

The objective of this Note is to understand the why and how behind the need for current command and control structures to evolve in order to provide an appropriate response to adversaries in a Multi-Domain environment. The history leading to the development of Multi-Domain Operations doctrine is discussed to provide an understanding of the current command and control system. This research will also often reference the tactics employed by Russia and China. This is due in part to their emergence on the world scene as the principal competitors to the US and its allies. It also serves to highlight the actions countries can now take as a result of easily acquired advanced technology. These tactics along with the background context of current command and control structures serves as the framework for analysis. This analysis is used to provide recommendations for the current system to meet the challenges posed by Multi-Domain Operations. Finally, considering the strategic aims of Russia and China and the effect they will have on a global scale, this paper analyzes the challenges posed to the coalition level and proposes areas where collaboration at improving interoperability can work.

Multi-Domain Operations is a topic of interest among many defense circles. The principal difference behind Multi-Domain Operations and its predecessors are the additional levels of complexity resulting from advancements in technology, which open up multiple domains in which the enemy can contest operations. Up until approximately the early 21st Century, the primary domains of war consisted of the air, land, and sea. The primary military strategy was a phase-based approach in which superiority of the air domain was typically the first step, which would then allow forces the freedom of maneuver among the remaining two.

However, adversaries can now exploit the cyber, space, and public information domains to achieve their political aims. This poses several problems to current militaries. First, adversaries can execute operations just below the threshold of armed conflict. This renders a conventional military response less than effective. Secondly, the cyber, space, and information domains offer adversaries unprecedented access. Their presence is now a permanent fixture in the public domain where they seek to achieve their objectives, in part, through a barrage of influence campaigns taking the form of disinformation campaigns or by exploiting societal tensions. They are also able to conduct operations that can shape the battlefield in less than 24 hours and can conduct these operations across multiple borders from anywhere in the world. The scope and speed at which adversaries can operate is too great for existing military structures. To make matters worse, western countries have spent the better part of two decades focusing on counter-insurgency operations, thus missing out on the opportunity to stay of ahead of the technology curve.

In order to meet these challenges, current C2 systems must evolve. Current information systems are ineffective and decision-making processes are too slow for a Multi-Domain environment. Soldiers, regardless of their service or the unit to which they are assigned, need to have access to an information data base from anywhere in the world. Additionally, every sensor onboard every asset should have the capability to share data to this centralized database. This amount of data will also surpass the capabilities of normal human processing. Therefore, operations in a Multi-Domain environment require augmentation from artificial intelligence software to assist in data processing and interpretation. Finally, these measures are not suitable if only taken unilaterally. Allies must find common ground in terms of increasing their interoperability with one another. The nature of Multi-Domain Operations centers around near-peer adversaries, which will require a global response.

Multi-domain Operations as a response to New Generation Warfare

In order to understand the effects of Multi-Domain Operations on the evolution of Command and Control (C2), it is first necessary to comprehend the origins of the preceding doctrine; AirLand Battle. The threats the western world faced during this time not only influenced AirLand Battle doctrine, but also helped to shape the C2 structure

that is still in place today. Similarly, we are currently experiencing an evolution of adversarial tactics that is driving a change in doctrine. Multi-Domain Operations doctrine is in direct response to tactics employed by Russia and China. Through understanding our adversary's strategy and how they intend to utilize advancements in technology in addition to how the US military intends to operate in a Multi-Domain environment, we can better understand how our C2 system must change.

AirLand Battle

The concept of AirLand Battle focused on a lethal mixture of maneuver and the use of both conventional and unconventional weapons. At the heart of the doctrine was a close coordination between United States (US) Army and US Air Force assets. The overall objective of AirLand Battle was to secure a lodgment of territory in a contested environment from which to conduct forward operations. The corps, the principal fighting unit, would continue to maneuver and strike opportunistically while the US Air Force conducted interdiction missions targeting the enemy's second echelon forces.[1] There would be no ceding of offensive capability for better defensive positions as had been the case in the preceding doctrine leading up to AirLand Battle.

The concept of AirLand Battle was developed following a large amount of suspicion surrounding the North Atlantic Treaty Organization (NATO) strategy of Active Defense that centered on NATO forces moving between a network of defensive posts throughout Europe. The purpose behind Active defense was to maximize the attrition of Warsaw Pact forces while minimizing those of NATO. This strategy, like Vietnam, deprioritized the offensive nature to which the US army was accustomed. Additionally, military strategists observed the lethality of technologically modern arms during the Yom Kippur War.[2] The potential of these weapons combined with an offensive based strategy could produce the western forces' desired effects against the Soviet Union, thus giving birth to the doctrine of AirLand Battle.

The focus of AirLand Battle doctrine was primarily on the land and air domains. It sought to interrupt the enemy's Observe-Orient-Decide-Action (OODA) loop through offensive ground maneuvers supported by air assets conducting interdiction on targets beyond the opposing force's leading edge. The minimal number of domains allowed for a structured phase-based approach to operations, which was supported by an efficient, all be it, rigid C2 architecture. This C2 architecture, which is still in use today, consists of Geographic Combatant Commands (COCOMs) responsible for specific areas around the world. The fact that both the C2 structure and AirLand Battle doctrine were solely dependent on the land and air domains was suitable enough for the adversarial threat they were designed to combat; the Soviet Union.

New Generation Warfare (NGW)

During the peak of the Cold War, strategists were eager to develop a doctrine that would counter a Soviet advance across Germany. This desire to achieve a decisive victory over the USSR became the catalyst behind developing Airland Battle doctrine. Today, Russia has once again catalyzed the evolution of doctrine. Multi-Domain Operations is in direct response to Russia's Hybrid War strategy. This new Russian concept came to light particularly during the 2014 annexation of the Crimean peninsula. Russia brought to bear an effective mixture of conventional and irregular

[1] Romjue John L. "From Active Defense to Airland Battle : The Development of Army Doctrine 1973-1982"; Historical Office United States Army Training and Doctrine Command, Fort Monroe, Virginia, June 1984, 63.

[2] Farley, R. (2018, août 1). AirLand Battle: The Army's Cold War Plan to Crush Russia (That Ended Up Crushing Iraq) [Post de blog]. Consulté le 25 novembre 2019, à l'adresse https://nationalinterest.org/blog/buzz/airland-battle-armys-cold-war-plan-crush-russia-ended-crushing-iraq-27477

forces along with a very robust economic coercion and disinformation campaign.[3] This massing of force across multiple domains showcases the evolution of Russian tactics and their exploitation of advanced technology. These evolved tactics directly support Russia's current geopolitical strategy.

The Russian strategy revolves around three principal ideas originating from its history. Russia throughout the 19th and 20th centuries has been marked by attacks from continental Europe. For example, the French invasion of 1812 and more recently, the confrontations with Germany during both World Wars. As a result of these past conflicts, Russia desires to maintain influence along its western border with Europe in order to prohibit a potential future invasion across its western flank. Compounding its desire to provide self-protection, Russia also hopes to increase its influence on former nations of the Warsaw Pact. In doing so, Russia can give support to its current political mantra, which is the return of Russia as a principal global power.[4] Finally, Russia seeks to support population centers with ethnic Russian ties. This level of support can be seen across the Baltic states, Georgia, and Ukraine.

In order to support these three strategic objectives, Russia uses the aforementioned hybrid warfare in order to exercise all available options short of open conflict with its principal antagonist, NATO. Russia regularly conducts large scale force employment exercises along the western European border to highlight its ability to quickly mass forces. In combination with these large-scale exercises, Russia uses its cyber operations capabilities to conduct disinformation campaigns and to economically coerce other nations. The cyber operations campaign is meant to sow doubt and divide NATO members.[5] The ultimate goal would be a non-committal to Article 5 among the members of the transatlantic alliance.

These tactics were on full display during the annexation of Crimea in 2014. Russia began its annexation by conducting a large-scale exercise along the Russo-Ukrainian border. This was followed by disguising Russian troops as civilians and dispersing them among a variety of pro-Russian Ukrainian armed militia groups. Finally, Russia concluded its three-pronged approach by launching a network attack against the Ukrainian defense network along with a multitude of civilian targets. This created confusion as to what was actually happening and resulted in a muted response from Western forces. Russia's ability to create effects across all domains and achieve success in Ukraine shows how effective a multi-domain approach can be. It also increases the pressure in developing an appropriate counterstrategy.

The Multi-Domain Response

Much like the development of its predecessor, the doctrine of Multi-Domain Operations is in response to the evolving tactics of near-peer adversaries such as Russia and China. Both of these nations have acquisitioned technology and put it to use in order to contest all domains. Through the combination of advanced technology and the exploitation of the air, land, sea, space, and cyber domain, Russia and China are able operate just below the threshold of conventional war. This increases the challenges of deterring these efforts. Non near-peer nations can also acquire this technology and begin to compete against nations with more comparatively advanced militaries. Additionally, the rate at which the world is

[3] Wither, James K. "Making Sense of Hybrid Warfare." *Connections*, vol. 15, no. 2, 2016, pp. 73–87. *JSTOR*, www.jstor.org/stable/26326441

[4] A November 2016 poll by the independent Russian Levada Center reported that 64 percent of Russians responded affirmatively to the following question: "Do you think that Russia today is a great power?" In 2011, three years before the Ukraine intervention, only 47 percent responded positively to that question. Levada Center (2017, Janvier 9), "Russia as a Great Power," Consulté le 25 novembre 2019 à l'adresse http://www.levada.ru/en/2017/01/09/russia-as-a-great-power/

[4] Kühn, U. (2018). *PREVENTING ESCALATION in the BALTICS A NATO PLAYBOOK*. Washington D.C. : Carnegie Endowment for International Peace, 13.

[5] *Ibid*.

urbanizing is increasing, which increases the chances that conflict will occur in a densely populated urban zone.6

The focus on anti-access and area denial (A2/AD) strategies by both Russia and China or in Russia's case a combination of A2/AD and NGW have highlighted the deficiencies of western based forces. This deficiency is a direct result in the over focus of western forces on counterinsurgency operations for the better part of almost two decades. Current assessments describe western forces as not being properly equipped to manage a multi-domain conflict. According to the US army, 2028 is the expected date the army will become capable of managing a multi-domain conflict; however, some technologies and tactics will not be ready until approximately 2035.7. These assessments combined with the timeline estimates have raised the priority to develop and implement Multi-Domain Operations within the US military and larger coalition community.

According to the US Army's TRADOC pamphlet, Multi-Domain Operations is broken down into five problem sets. These problem sets highlight the strategy the US joint force will take concerning combat throughout all domains. Understanding what actions will be employed within each problem set will also give a better perspective as to how this will affect the evolution of C2. The problems sets are as follows:

1. How does the Joint Force **compete** to defeat an adversary's operations to destabilize the region, deter the escalation of violence, and, should violence escalate, enable a rapid transition to armed conflict?
2. How does the Joint Force **penetrate** enemy anti-access and area denial systems throughout the depth of the operational framework to enable strategic and operational maneuver?
3. How does the Joint Force **dis-integrate** enemy anti-access and area denial systems in the Deep Areas to enable operational and tactical maneuver?
4. How does the Joint Force **exploit** freedom of maneuver to achieve strategic and operational objectives through the defeat of the enemy in the Close and Deep Maneuver areas?
5. How does the Joint Force **re-compete** to consolidate gains and produce sustainable outcomes, set conditions for long-term deterrence, and adapt to the new security environment?[8]

In order to resolve these problem sets, the US joint force will not only be at a constant state of readiness but will constantly engage the enemy through the combination of forward based multi-domain capable forces ready to engage the enemy throughout the spectrum of domains. Conventional forces and tactics will be used to demonstrate to the adversary the US joint force's ability to respond in hopes of deterring aggression. Concurrently, unconventional tactics such as deception along with the use National Level assets (intelligence, cyber, space, and some limited strike capabilities) will work together throughout the domains to engage the adversary before the conflict crosses the threshold of conventional war.

If this deterrence were to fail, the US joint force strategy will again synergize its forces across the domains in order to dis-integrate or decouple the adversary's A2/AD systems and exploit moments of opportunity to return the level of effort below the threshold of open conflict. The adversary will be posed with multiple problem sets that span the domains, which are designed to disorient and reduce the effectiveness of their response. The ideal situation is where the enemy remains stuck in between the Observe and Orient phases of Boyd's OODA loop. Figure 1 below depicts an overlay of the

[6] TRADOC. (2018). *The U.S. Army in Multi-Domain Operations 2028*. Fort Eustis, Virginia : US Army TRADOC.

[7] *Ibid*.

[8] *Ibid*, viii-ix.

five problem sets put forward by the US army onto the A2/AD strategy Russia and China have adopted.

The Multi-Domain Operations strategy described above highlights a force that is not only at a constant level of readiness, but a force that is constantly engaged at some level against an adversary. The thought of a long-term constant engagement is something that is no longer foreign to us (reference two decades of COIN operations). The difference lies in the tactics used, level of required personnel expertise, material expended, and an evolved C2 structure. We are no longer assured of maintaining long-term domain dominance. Instead, cross-domain capabilities will be synergized together to provide windows of opportunity. The next section will discuss the concepts behind perpetual conflict in order to frame the problems with the current C2 construct.

Challenges as a result of perpetual conflict

Multi-Domain Operations rests on the principal that the joint force will be constantly engaged at some level throughout the spectrum of conflict. Whether just short of conventional war or open hostilities, the joint force will be engaged across all domains. This level of perpetual contestation poses several challenges to existing civil and military structures. A thorough understanding of these challenges will help to understand why the current C2 structure must evolve.

Contesting the electromagnetic spectrum

One of the primary challenges put forth by Multi-Domain operations is the contestation of the Electromagnetic Spectrum (EMS). Adversaries such as Russia and China have already fielded technology aimed to disrupt operations across the EMS. For example, it was uncovered in 2005 that

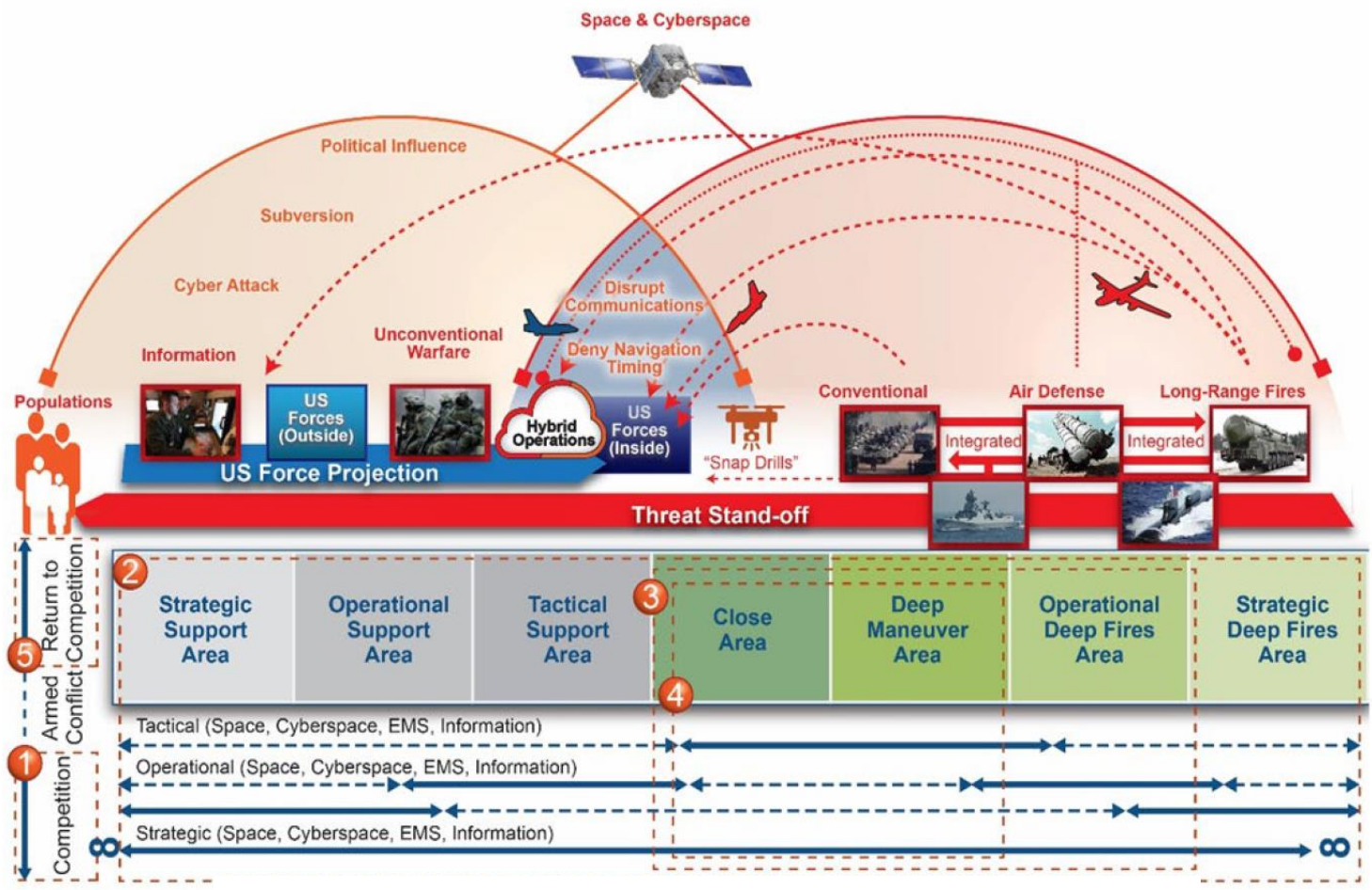


Figure 1. Overlay of Multi-Domain Objectives on A2/AD strategy: Photo credit: US army TRADOC MDO pamphlet 525-3-1

China had acquired the capability to detonate a low-yield nuclear device at an altitude several hundreds of miles above the earth's surface. This low altitude detonation would minimize the kinetic effects of a nuclear explosion while maximizing the effect of the Electromagnetic Pulse (EMP). For reference, an atomic bomb detonated at an altitude of 300 miles above ground level would produce an EMP covering most of the North American continent.[9] This EMP would cause destruction on critical energy grids, telecommunications networks, computers etc. This could have secondary and tertiary effects on all sectors within a country ranging from disruptions to transportation systems to the financial sector. This would also be in addition to the negative effects it would have on the joint force's ability to plan, execute, and manage contingency operations due to the reliance on land and space-based communication devices.

China and Russia have also invested in other non-nuclear technologies that could cause the same disruptive effects to the EMS domain. These technologies consist of ballistic missiles and submarines, which could cause a more localized effect. There also exists handheld devices that if operated near airports or other critical information nodes could cause disruptions to the freedom of movement and free flow of information. The potential daily disruption to communication networks would greatly impact C2's ability to perform their primary mission.

Constant presence in the public information domain

In addition to disruptions of the EMS domain, adversary nations are currently and will continue to contest the public information domain through widespread use of disinformation campaigns. Examples of these tactics include the insertion of falsified textbooks in classrooms, targeting specific population groups with falsified advertisements via social media, falsifying news segments or posing as legitimate news sources. The intent of these disinformation campaigns is to exploit societal divisions within countries. This increases tension and weakens a country from within. In some cases, Russia has employed disinformation campaigns targeting a nation's commitment to the North Atlantic Treaty Organization (NATO) alliance. For example, in France during the "Gilets Jaunes" demonstrations, 340 pro-Russian accounts disseminated or retransmitted falsified information 20,000 times via social media.[10] This falsified messaging targeted the French president's ability to govern while simultaneously amplifying anti-immigrant and anti-NATO sentiment. These types of tactics will cause national governments to focus on domestic issues reducing their ability to not only counter disinformation, but also reducing their ability to promote sanctions or military action against the offending nation.[11] Nations like Russia and China will continue to utilize disinformation to undermine the effectiveness of democracy itself. Disinformation campaigns are relatively cheap with average costs ranging from thousands to hundreds of thousands of dollars and can have a large impact. For this reason, it is logical to presume their presence will continue. The Joint Force will have to remain constantly engaged in order to counter these effects. This will require a constant presence within the public information domain, which increases personnel and technology requirements.

Complicated management

An additional problem originating from multi-domain operations relates to the management of joint forces. The increased number of domains where the joint force can engage the enemy combined with an increased frequency of

[9] Cohen, A. (2019, avril 5). Trump Moves To Protect America From Electromagnetic Pulse Attack. Consulté le 25 novembre 2019, à l'adresse https://www.forbes.com/sites/arielcohen/2019/04/05/whitehouse-prepares-to-face-emp-threat/#576caaeee7e2

[10] Gricius, G. (2019, mai 11). How Russia's Disinformation Campaigns are Succeeding in Europe. Consulté le 25 novembre 2019, à l'adresse https://globalsecurityreview.com/russia-disinformation-campaigns-succeeding-europe/

[11] *Ibid*.

engagement due to the perpetual nature of Multi-Domain Operations results in a more complex management problem. This problem set includes the deconfliction of joint assets, the appropriate lowering of command authority, and the establishment of areas of responsibility.

Deconflicting assets is a necessity in any operational plan and as more and more domains are involved it only increases in complexity. The most obvious reason why there needs to be tedious management of deconflicting assets is to avoid losses due to fratricide. Aircraft collisions and friendly fire accidents are the most common occurrences of a poor management of forces. These accidents can result from overly complex plans, inadequate flow of information, and a loss of situational awareness. These are all areas where a robust and capable C2 system can assist.

In addition to the loss of physical assets, the joint force must also properly deconflict operations that rely on the EMS. Radio frequencies must be deconflicted to avoid over saturation. For example, once a unit is assigned a certain frequency for conducting its operations, no other unit can utilize that same frequency.

Deconfliction of the EMS also goes beyond simple frequency allocation. Desired effects emanating from certain systems must be deconflicted. If a unit were to request certain cyber effects it could create a situation where those same effects are no longer available to subsequent requests.

C2 must also be aware that some requested effects require a high level of approval authority. This complicates their management since hardened communication channels will be required to ensure communication of their approval is effectively received. This necessitates the existence of a reliable and constant connection between “front line units” and their C2. This problem is exacerbated when confronting an adversary who is employing A2/AD tactics designed primarily at severing communication lines or targeting communication nodes. C2 systems and processes must be resilient and “self-healing” in a multi-domain environment.

Compounding the problem, C2 must concern itself with deconflicting areas of responsibility around a specific target. Given the complex nature of multi-domain operations, it is not unlikely to think that C2 could receive multiple requests from different domains to strike the same target. Failing at this would result in an over expenditure of assets and can increase the likelihood of a friendly fire accident.

The technology bill

The primary causal factor for the birth of Multi-Domain Operations is directly related to the proliferation of advanced technology among adversarial nations such as Russia and China. Not only has advancements in technology opened up the possibility for contested operations throughout multiple domains, but it also poses a problem related to the perpetual nature of Multi-Domain Operations. Due to the constant presence of forces throughout the domains in addition to an increased number of sensors collecting information, the amount of received data will be exponentially greater than previously experienced. Therefore, the joint force must acquire a robust and efficient communication systems and the technological means necessary to process the large quantity of received data.

In terms of a robust and efficient communication systems, the joint force requires a communications network that is redundant, self-healing, able to transmit data and communications without delay, and be capable of operating throughout western based forces. Redundancy is required due to the adversary’s capability at disrupting communications lines and nodes. Following a disruption, the communication system must possess a level of self-healing. This characteristic refers to the ability of a system to bring itself online as quickly as possible with little human intervention. Self-healing also refers to a system’s ability to reroute communication data via an alternate system of networks and nodes if an adversary’s presence is sensed in the primary network. Finally, communication systems must be interoperable. Every sensor, regardless of the platform, must be capable of collecting and disseminating data on all

available coalition-based platforms. In turn, those receiving the data must be able to interpret it.

A current example of where US assets fall short in this category is the current data link architecture employed by the F-22 Raptor 5th generation aircraft. The Intra-Flight Data Link (IFDL) was developed to help reduce an adversary's capability to locate the F-22 by minimizing conventional radio calls while simultaneously transmitting situational awareness data across a secure network. However, IFDL only permits access to this data with other users who possess the same equipment. Currently, only F-22s possess this capability; therefore, are only able to communicate with each other. This is in stark contrast to the F-35, which utilizes the Multifunction Advanced Data Link (MADL). MADL supports the F-35's low observable stealth fighter role at the same time allowing it to share data over a conventional Link-16 network that is common among numerous US and NATO military units.[12] The ability to communicate across a common communications architecture is an absolute necessity for succeeding in a multi-domain environment.

The large quantity of data being collected from across all domains that requires processing and interpretation also presents a problem to C2. Currently, the amount of data being collected already exceeds the amount that can be processed by existing analysis processes.[13] In order to address this problem, C2 structures must enlist the help of Artificial Intelligence (AI) technologies. However, despite the allure of Hollywood films showcasing AI as an unstoppable force that will replace human existence, current AI technologies require large amounts of human involvement. These types of AI technologies are referred to as "Specialized AI", which can manage specific tasks using data sets that were previously analyzed. Additionally, "Specialized AI" systems must be trained and programmed in order to accomplish their assigned tasks.[14] Even though current AI technologies might not able to complete cognitive decision-making cycles as well as the human brain, they are still required to assist human operators in processing the large amounts of received data. The joint force must continue to prioritize the development of AI technology and C2 must adopt it immediately.

Complex problem sets emanating from advancements in technology and an increased number of domains in which to engage the enemy highlight the challenges C2 must overcome to be successful. Addressing these challenges requires highly skilled personnel, means of freely processing and disseminating data, and a flexible command structure that can adapt quickly to dynamic situations that span all contested domains.

Problems with existing C2 structures

The current US C2 structure, much like AirLand Battle doctrine, was created to counter a conventional threat tied to the physical domains of the air, land, and sea. This command structure relies heavily on well-defined boundaries demarcating areas of responsibility, a structured operational approval process, and a clear understanding of the role of functional supporting commands. Multi-Domain Operations calls into question this entire framework relating to C2. Adversaries can exploit weaknesses in this current system by operating just below the threshold of conventional war and by executing cross-domain operations at a pace faster than the current decision-making process and subsequent targeting

[12] Everstine, B. (2018, mars 1). The F-22 and the F-35 Are Struggling to Talk to Each Other ... And to the Rest of USAF. Consulté le 25 novembre 2019, à l'adresse http://www.airforcemag.com/MagazineArchive/Pages/2018/March%202018/The-F-22-and-the-F-35-Are-Struggling-to-Talk-to-Each-Other---And-to-the-Rest-of-USAF.aspx

[13] F Feickert, A., Kapp, L., Elsea, J. Harris, L. 2018. *U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress*. Washington, DC: Congressional Research Service, November 1st. https://crsreports.congress.gov/product/pdf/R/R45392,9

[14] *Ibid*.

cycle. The problems with existing C2 structures presented in this section highlight the evolutionary changes C2 must take to remain effective in a Multi-Domain environment.

Geographic constraints

Currently, there are 11 total Combatant Commands (COCOMs) with six being associated to a specific geographical region of the world. The remaining five are considered Functional COCOMs whose capabilities serve to support the geographical commands in terms of space, cyber, special forces, nuclear, and strategic airlift. Each of these geographically based COCOMs retains combatant command, operational, and tactical control authority over its assigned forces in order to support regional objectives. The problem that arises due to Multi-Domain Operations is how do commands manage a crisis that extends across multiple areas of responsibility (AOR)?

COCOMs are not necessarily unfamiliar with this situation where a conflict can span across different zones of responsibility as was the case for Operation Iraqi Freedom (OIF) in 2002. During OIF, members from both United States European Command (USEUCOM) and United States Central Command (USCENTCOM) met to establish the proper transfer of command authority over assets transitioning through both AORs. An agreement was reached where USEUCOM would maintain tactical control over the movement of forces, intelligence surveillance and reconnaissance (ISR) and logistical support assets up to the border of Turkey. Once these assets were ready to commence offensive operations, all levels of authority (command, operational, and tactical) were then transitioned to USCENTCOM.[15] This agreed upon transition of command authority resulted in clearly defined "supported" (USCENTCOM) and "supporting" (USEUCOM) relationships. The establishment of supporting relationships was codified by the Secretary of Defense and would serve as the framework for future campaign plans.

Whereas the example of OIF highlights a success story in terms of a clear delineation of supporting versus supported relationships, it must be emphasized that this operation involved the coordination between only two neighboring COCOMs. Additionally, OIF benefited from 12 years of intense regional focus beginning after the Persian Gulf War of the early 1990s. This regional focus resulted in two operational plans (OPLANs), 1003 and 1003-98, both of which involved a military response against Iraq specifically.[16] OIF was further aided by the intelligence garnered from Operations Northern and Southern Response.

This context concerning OIF is important because crisis response in a Multi-Domain environment will not be afforded the luxury of meticulously developed OPLANs or well delineated supporting relationships. For example, a cyber-attack against a country's electrical grid can come at a moment's notice with zero warning. An adversary nation can begin a disinformation campaign, which can remain undetected for long periods of time.[17] Contested operations in a Multi-Domain environment can happen at anytime and anywhere.

The speed at which operations will move in a Multi-Domain environment also highlights the problems associated with the establishment of geographic AORs linked to COCOMs. An important questionto ask of the current C2 structure would be what if an adversary launches a cyber-attack within

[15] United States Department of Defense. (2017). *Joint Operations 3-0* (17 January 2017 Incorporating Change 1 22 October 2018). Washington D.C. : US JCS, III-4.

[16] Perry, Walter L., et al., editors. "Planning the War and the Transition to Peace." *Operation IRAQI FREEDOM: Decisive War, Elusive Peace*, RAND Corporation, 2015, pp. 31–56, www.jstor.org/stable/10.7249/j.ctt19w72gs.11

[17] European Parliamentary Research Service. (2019). *Automated tackling of disinformation* (1). Consulté à l'adresse https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf

the European AOR against targets located on the North American Continent? Who would maintain command authority if China were to employ the aforementioned low-yield nuclear device since the EMP has the potential to traverse multiple COCOM AORs? Similarly, cyber and informational attacks can span multiple AORs complicating supporting relationships.

Additionally, Geographic COCOMs do not necessarily contain the necessary forces needed to respond to contested operations in a Multi-Domain environment. This raises yet another problem in terms of the relationship between the two types of COCOMs. The two most obvious Functional COCOMs regarding this problem are US Cyber Command (USCYBERCOM) and US Strategic Command (USSTRATCOM). Currently, the commanders of both these Functional COCOMs retain directive command authority concerning the use of their respective assets. This centralized control of cyber and space capabilities exists despite joint doctrine necessitating the integration of cyber and space experts throughout a Geographic COCOM's staff and planning process. The requirement to receive approval authority concerning the use of cyber or space effects adds to the delay in responding to a threat. Additionally, since it is assumed that the adversary has the capability to influence the EMS, there is a strong possibility of experiencing disrupted communications between the Functional and Geographic COCOM. The dis-integrated nature of the current system has, in some fashion, aided the adversary in its denial efforts.

The use of the cyber and information domains also poses a problem to the current C2 construct. The entire concept of a COCOM was to face down a conventional adversarial threat. Commanders and military planners alike are still becoming more and more comfortable with conducting operations against unconventional targets that exist in these domains. However, much progress is left to be made. An example of the lack of capability within the cyber and information domains is the fact that western forces have still yet to solidify an appropriate response to Russian cyber-attacks in the Baltic states or even a response to Russian disinformation campaigns in both the US and Europe. The bottom line is COCOMs, in their current construct, are not yet capable of countering unconventional threats that span multiple AORs.

Delegated command authority constraints

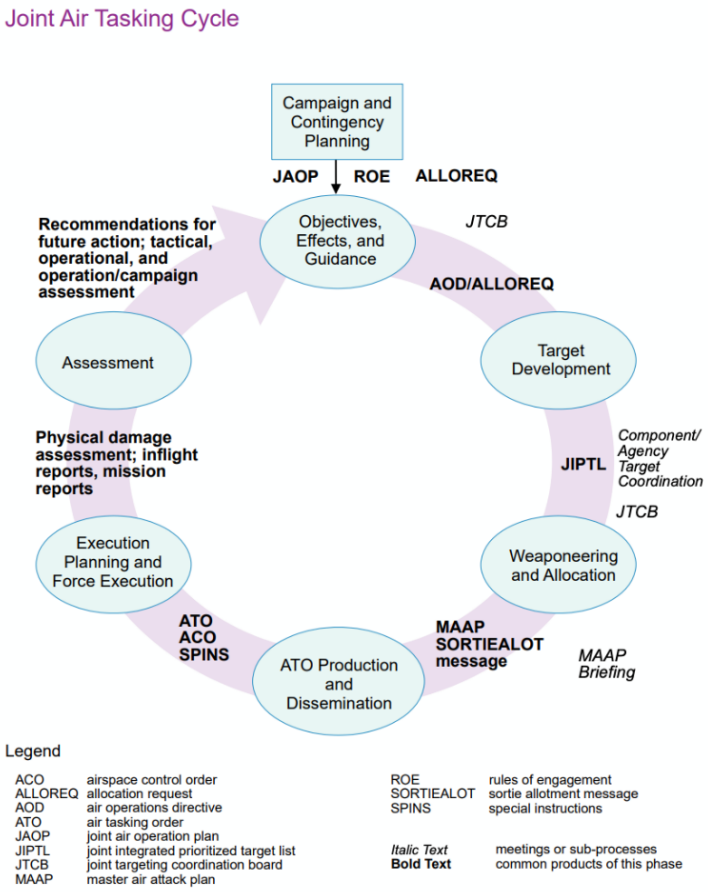
Multi-Domain Operations also complicate the joint decision-making process and calls into question the delegation of command authority. Currently, C2 structures operate off of a fixed target planning period. An example of this battle rhythm is found in the Joint Air Tasking Cycle, which produces the Air Tasking Order (ATO). The ATO consists of a list of prioritized targets that are a function of the Joint Force Commander's (JFC) objectives and coordinated support from the Joint Force Air Component Commander (JFACC). There are six phases in producing an ATO with each ATO period lasting 24 hours. The entire joint ATO process spans a 72-hour period, which incorporates the active ATO in execution, tomorrow's ATO in production, and the following day's ATO in planning.[18] Figure 2 provides a visual depiction of the ATO process.

Once again, the existing process for target identification, selection, and assessment was based off of a conventional war model in which the joint force would have at least a 72-hour window to interpret and process intelligence. Realizing the ATO cycle in a Multi-Domain environment will be a complicated endeavor as the adversary is able to quickly move throughout domains since their assets are not necessarily tied to the physical domains of air, land, and sea. In a Multi-Domain environment, following the execution of the active ATO, the battle space may be completely different for the proceeding day's plan. A Multi-Domain

[18] United States Department of Defense. (2017). *Joint Operations 3-56.1* (14 November 1994). Washington D.C. : US JCS.

capable force must be able to interpret, plan, and execute with less than 24 hours of notice.

Figure 2. Joint ATO Cycle
Photo Credit: JP 3-30



One step above the Joint Targeting Cycle is the seven-step Joint Planning Process (JPP). The JPP is a logical step by step process that begins by defining the problem, then developing and comparing different Course of Action (COAs), followed by selecting the appropriate COA, and ends with producing a plan or order.[19] The process begins from direction of the President of the United States, Secretary of Defense, or Chairman of the Joint Chiefs of Staff. Combatant Commanders (CCDR) then derive their commander's intent or overall objective based upon received guidance such as the National Security Strategy. The process ends with CCDR approval, which can then initiate the Joint Targeting Cycle defined above. The JPP highlights the current and very structured military decision making process. It also demonstrates at what level approval authority resides.

The rigidity of the JPP presents a major obstacle to effective C2 since the speed at which operations in a Multi-Domain environment can occur will cause severe degradation of the current planning process. The time required for the JPP and subsequent Joint Air Tasking Cycle to be completed is currently estimated at greater than 96 hours, which gives more than enough time for an adversary to complete its own OODA loop subsequently rendering the joint force ineffective. By the time the CCDR arrives at the approval step, the battlespace may have changed two or even three times based on a 24-hour adversarial battle rhythm. The joint force will continue to find itself in a reactionary and defensive posture.

The level of command approval will also cause degradations in effectiveness. There is approximately five levels of command between the tactical operator and the CCDR. Each level of command becomes more and more bureaucratic with an increasing number of staff officers and processes. Depending on the level of delegated command authority, authority to engage a random target could necessitate CCDR or higher approval. This is especially the case, if the requested engagement involves cyber or space assets, whose authority still resides at the national level. Multi-Domain Operations are dynamic, which requires a rapid enough planning and decision-making process to furnish a tactical operator the ability to conduct engagements inside the adversary's OODA cycle.

[19] United States Department of Defense. (2017). *Joint Operations 5-0* (16 June 2017). Washington D.C. : US JCS, V-I.

The theme coursing through each of these challenges facing C2 is speed. Each adaptation to existing C2 structures must take into account its ability to increase the speed at which information is collected, processed, interpreted, and acted upon. Similarly, to past operations, those with the faster OODA loop will succeed. Multi-Domain operations does not change this concept, but it does add layers of complexity. As was the case with the creation of the Unified Command Plan following the end of the Second World War establishing the basis for today's COCOM structure, the joint force must once again evolve.

Recommendations for the evolution of C2 architecture

The preceding sections discussed why Multi-Domain Operations doctrine came into existence, the challenges associated with this type of environment, and the current problems facing C2 structures and processes. The intent behind that discussion was to outline some of the necessary adaptations C2 must take to remain effective in this new atmosphere. The following section will provide analysis on several proposed changes, which include the transfer of information to a cloud-based network, inclusion of AI and machine learning technologies, as well as proposed structural changes to C2 hierarchies. All of the subsequent recommendations are intended to be adopted together in consortium.

Information in the cloud

The first major evolution of C2 is the transfer of military networks from traditional information sharing means to a cloud-based system. Current networks hinder the rapid dissemination and processing of data because access to these networks is restricted to members within that agency. For example, an army intelligence officer primarily can only access intelligence information on the army's network. This problem also occurs within services. Most intra-service units operate off of independent network servers where access to data is limited to only members of that unit. Additionally, this data is accessible when physically connected to the network. This means a deployed soldier does not have access to data that is regularly available when they are at their home station.

Cloud based computing provides the solution to the impediments to the flow of data described above. A cloud-based network is necessary for Multi-Domain Operations because it provides on-demand network access, which enables servicemembers the ability to access data at anytime from anywhere. Cloud-based networks also eliminate inter-service network roadblocks. Officers, regardless of their service, would be able to access data contained within a common pool of information. This would help to increase the speed of information dissemination and interpretation. In a perfect solution, cloud-based computing would allow access to data fused together from every available sensor. As former director of the Defense Information Systems Agency Army Lt. Gen. Alan R. Lynn stated "You build a lake of information that you can pull from…If we need logistics to go here, and an amount of ammunition to go there, we're now able to correlate all those different pieces at one time, which is very powerful for the warfighter."[20]

There are additional benefits to adopting a cloud-based informational architecture. First, it will help to reduce dependency on physical access to networks. This eliminates maintenance and installation requirements concerning network access. It also reduces costs as these tasks can be consolidated into a central facility as opposed to having trained personnel available at every physical node. Secondly, cloud-based computing also allows for a more rapid implementation of software and hardware updates. This would improve network security because system-wide security

[20] U.S. DEPARTMENT OF DEFENSE. (2017, décembre 21). Defense Department to Move to Cloud Computing. Consulté le 25 novembre 2019, à l'adresse https://www.defense.gov/Explore/News/Article/Article/1402556/defense-department-to-move-to-cloud-computing/

enhancements are more rapidly installed. Additionally, reducing a networks dependency on physical nodes also enhances its security. Furthermore, approved military applications would also be more quickly implemented resulting in the warfighter having the latest means of processing data.

Although cloud-based computing is a necessary requirement for enabling success in Multi-Domain Operations, there are potential drawbacks the joint force must take into account. Cloud-based systems increases the potential for Distributed Denial of Service (DDoS) attacks. The goal behind these attacks is to overwhelm the target's network in hopes of degrading connectivity or rendering it completely unusable.[21] DDoS attacks accomplish their goal by creating a network of "zombie" or infected computers. Each of these infected computers then targets a specific network, CPU, web server, or storage facility in order to deplete the target's available bandwidth.[22] This would cause severe degradation in a Multi-Domain environment since a DDoS attack on a cloud informational architecture could potentially limit functionality to all cloud-dependent users. This necessitates the need for a hardened, constantly monitored, and self-healing network.

Providing access to the cloud is another hurdle that must be crossed for it to be effective in a Multi-Domain environment. A soldier in the middle of Afghanistan must have the same data accessibility and connection speed as an intelligence officer located at the Pentagon. Current data communication networks make this problem all the more apparent. However, with the implementation of 5G, world-wide connectivity is more of a possibility. 5G networks increase upload and download speeds as well as decrease latency time.[23] 5G connection speeds enable advanced technologies such as driverless cars and the possibility to conduct remote surgical operations. These types of technologies are analogous to those required by the military in a Multi-Domain environment. Near-instantaneous collection of data from sensors and subsequent interpretation by tactical operators would be possible with a 5G network. Table 1. shows a comparison of current 4G and future 5G characteristics.

Characteristic	4G	5G
Max speed	1.45 GB/Sec	10 GB/Sec
Connectivity	10K – 100K devices supported /Sq. M	1 million devices supported/Sq. M
Mobile Data Volume	1/100 Terabytes/Sec/Sq. KM	10 Terabytes/Sec/ Sq. Km
Latency	40-50 milliseconds	Less than 10 milliseconds

TABLE 1. Network comparison characteristics.[24]

It must be noted that the concept of the developing a cloud-based computing system for the US military is already underway. Former Secretary of Defense James Mattis, following a 2017 trip to silicon valley, outlined the necessity for the Department of Defense to begin drafting plans in order to renovate the military's informational systems.[25] This resulted in the creation of the Joint

[21] Deshmukh, R., & Devadkar, Kailas . (2015). *Understanding DDoS Attack & Its Effect In Cloud Environment*. Consulté à l'adresse http://iranarze.ir/wp-content/uploads/2017/04/6554-English-IranArze.pdf

[22] *Ibid*.

[23] Puranik, M. (2019, août 19). How the rise of 5G will disrupt cloud computing as we know it. Consulté le 28 novembre 2019, à l'adresse https://www.cloudcomputing-news.net/news/2019/aug/19/how-rise-5g-will-disrupt-cloud-computing-we-know-it/

[24] The 8 Attributes of 5g Network Performance. (s. d.). Consulté le 25 novembre 2019, à l'adresse https://www.verizonwireless.com/business/articles/business/5g-network-performance-attributes/

[25] Nickelsburg, M. (2019, octobre 28). What is JEDI? Explaining the $10B military cloud contract that Microsoft just won over Amazon. Consulté le 25 novembre 2019, à l'adresse

Enterprise Defense Infrastructure (JEDI), which is a $10 billion project aimed at providing an enterprise-level approach to developing a common information architecture across all services.[26] While the JEDI program is currently on hold because of legal complications regarding Microsoft being awarded the contract, military officials understand the importance of getting this program right and doing so quickly. China is also currently developing a similar cloud-based system, which is in addition to the Chinese state-owned Huawei communication company developing its own 5G network. Both the US and China's actions highlight the demand for a cloud-based data system.

In summary, cloud-based computing is still in the conceptual phase. Senior leaders are in the progress of determining the next step so as to ensure its success. A massive technological transformation of this magnitude is essentially a too big to fail decision. Despite the final decision, cloud-based computing is one of the many necessary evolutions C2 must take in order to gain the advantage in a multi-domain environment.

Inclusion of artificial intelligence

Cloud-based informational structures are only one piece of the necessary technological adoptions required for C2 to be successful in Multi-Domain Operations. The other piece being the inclusion of Artificial Intelligence (AI). In an ideal Multi-Domain environment, every sensor on every platform is interoperable and connected. This translates into an exponential increase in the amount of received data compared to that of today. The processing and interpretation of this data is simply too overwhelming for human operators to carry out. AI technologies are needed to help recognize, appropriately categorize, and disseminate received data. They are needed to enhance human capability and are a necessary evolution for C2's success in a Multi-Domain Operations.

The US Department of Defense, in 2018, launched its strategy concerning the implementation of AI. The US strategy focuses on four key areas:

1. Delivering AI-enabled capabilities that address key missions
2. Partnering with leading private sector technology companies, academia, and global allies and partners
3. Cultivating a leading AI workforce
4. Leading in military ethics and AI safety[27]

Focusing on the first focus area, the US Department of Defense wants to implement AI technologies to help collect and process raw data in order to provide decision makers an increased level of situational awareness.[28] Their hope is that AI will eventually help in better determining the right course of action taken towards a given scenario. This will have direct impact on the problem mentioned above concerning the current timing of the decision-making process and the joint targeting cycle. Planners will now be able to more quickly understand data and potential COAs. Again, the joint force must be able to reduce their planning cycle to less than 24 hours. AI technologies combined with cloud-based information systems will make this goal possible.

Along with the release of the national strategy concerning AI, the US also created the Joint Artificial Intelligence Center (JAIC). The JAIC is focusing on the following mission areas:

1. The acceleration of delivery and adoption of AI capabilities across the DOD

https://www.geekwire.com/2019/jedi-explaining-10b-military-cloud-contract-microsoft-just-won-amazon/

[26] *Ibid*.

[27] United States Department of Defense. (2018). *SUMMARY OF THE 2018 DEPARTMENT OF DEFENSE ARTIFICIAL INTELLIGENCE STRATEGY: Harnessing AI to Advance Our Security and Prosperity*. Washington D.C. : US DOD,11 - 16.

[28] *Ibid*, 11.

2. The establishment of a common foundation for scaling AI's impact
3. Synchronizing DOD AI activities to ensure alignment with the National Defense Strategy
4. Developing a team of AI experts[29]

US policy concerning AI along with the creation of the JAIC is a necessary step. Much like the JEDI project described above, there needs to be an enterprise-level response to the adoption of AI technologies. C2's success in Multi-Domain Operations rests on the ability for systems to be interoperable and one way of increasing interoperability is approaching these challenges as a joint team. This allows each service to accurately communicate their specific service-related needs. This also gives services and senior leaders a "34,000 foot" perspective on the implementation of AI, which will help reduce any potential glaring deficiencies.

While AI is necessary in the evolution of C2 for it to handle the challenges of Multi-Domain Operations, its limitations must be understood. There is a current fear that AI technologies will soon match or outperform human cognitive ability. However, current data suggests AI technology is a long way off from reaching this level of performance if it is even ever able to reach it. Current AI researchers vary widely on their predictions of when the AI singularity, the point at which AI surpasses the human brain, will occur. Answers vary from around the year 2045 to 2100, with some predicting it will never occur.[30] The fact of the matter is, this type of "Strong AI" is not necessarily needed for C2 to be successful in Multi-Domain Operations.

What is needed are AI technologies that augment human performance. These technologies are referred to as specialized AI and are currently in use. A commonly used AI technology in place today is known as machine learning. Machine learning uses a combination of mathematical modeling and sample data in order to make decisions.[31] This type of AI technology is useful for C2 systems because it would help provide confidence intervals to certain data sets. For example, if data existed concerning the time of year and geographic location of an adversary's cyber-attacks, by using statistical modeling, machine learning could provide levels of confidence concerning when and where the adversary will strike next. Most systems in nature, given a large data set, represent normal distributions. Given this fact, there are credible mathematical approaches at predicting a system's behavior.

This type of AI technology; however, requires a constant human presence to monitor the software's performance. Additionally, machine learning requires heavily treated data, which also requires human intervention. Without human involvement there can exist a possibility where the AI technology is providing incorrect estimates. Nevertheless, this level of AI capability does exist and is a mandatory evolution for C2 systems.

Structural evolution

The final recommendation for C2 to be successful in a Multi-Domain environment involves an evolution of the physical C2 hierarchies. Each one of these proposals is intended to increase the speed of decision making, reduce organizational friction caused by overlapping responsibilities, and

[29] U.S. DEPARTMENT OF DEFENSE. (2019, février 12). DOD Unveils Its Artificial Intelligence Strategy. Consulté le 25 novembre 2019, à l'adresse https://www.defense.gov/Explore/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/

[30] Azulay, D. (2019, mars 18). When Will We Reach the Singularity? – A Timeline Consensus from AI Researchers. Consulté le 28 novembre 2019, à l'adresse https://emerj.com/ai-future-outlook/when-will-we-reach-the-singularity-a-timeline-consensus-from-ai-researchers/

[31] Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*: Springer.

make it more possible to delegate command authority to the lowest level possible. It is also recognized that the level of change in the current C2 architecture is a function of money, manpower, and political will.

Historically, a crisis or failure was needed to satisfy all three variables. For example, the last major overhaul of the US military's C2 structure was due to the Goldwater-Nichols Act of 1986. This act was in direct response to the lack of inter-service coordination that resulted in poor performances during the Vietnam War and the failed Iranian Hostage Rescue mission of 1980.[32] These instances of failure served as the catalyst for a monumental change in C2 operations. Recognizing this fact, minus a crisis or failure, it will be very difficult to attain the necessary drivers of change. To this end, the proposed recommendations are organized under three different levels of change; minor, moderate, or major. These three levels correspond directly to varying levels of political will. They could also serve as subsequent steps to take in the evolution of C2 to meet Multi-Domain operational demands. These proposals are intended to simply articulate different possibilities of transformation. They by no means represent all of the possible C2 configurations.

The first level, or "minor" changes, assumes the existing Geographic and Functional COCOM structure remains in place. The proposed changes corresponding to this level are mainly focused on providing an increased emphasis on Multi-Domain Operations and the inclusion of a specifically tailored Multi-Domain task force located on the joint staff of each Geographic COCOM.

The increased emphasis on Multi-Domain Operations mainly focuses on specifying command relationships and delegating command authority to the lowest levels possible. As noted above, one of the identified problems from the current C2 structure is the question of which COCOM maintains operational responsibility given a conflict that spans multiple AORs. The decisional authority and processes already exist within the DOD; however, their understanding is less than ideal. In order to streamline communication, this paper recommends the decisional authority, for which COCOM maintains operational responsibility, rest with the Chairman of the Joint Chiefs of Staff (CJCS). Along with this decision, the CJCS would also determine the supporting roles of the remaining COCOMs. The speed at which the CJCS can accomplish these tasks is enabled by a cloud-based technology and AI software.

In addition to the CJCS maintaining decisional authority, a Multi-domain task force must be created for each Geographic COCOM and reside on their respective joint staffs. Each of these task forces would be comprised of specially trained Multi-Domain officers and liaison officers from each domain. The Multi-Domain specialists will possess the expertise at integrating assets and creating effects across domains. The liaison officers will help to address any questions surrounding operational control of assets belonging to Functional COCOMs. It must be noted that liaison officers already exist within the current structure. However, the principal difference in this proposed change is that these officers reside within the Multi-Domain task force and are solely responsible for attaining desired effects. Given these minor changes, the current C2 structure can reduce its deficiencies related to Multi-Domain operations. Figure 3 below provides a visual depiction of this concept.

"Moderate" changes to the C2 structure involve maintaining the current Geographic and Functional COCOM structure in place; however, they would be subordinate to two or more overarching Multi-Domain Commands.[33] The need for at least two Multi-Domain Commands is based on the US

[32] Cole, Ronald H. (1999). "Grenada, Panama, and Haiti: Joint Operational Reform" (PDF). *Joint Force Quarterly* (20 (Autumn/Winter 1998-99)): 57–74. Retrieved October 20, 2019.

National Military Strategy, which necessitates the US military being able to defeat a regional adversary while simultaneously denying objectives of another.[34] In the event of a crisis, each of these Multi-Domain COCOMs would have command authority and operational control over all domains. They would be responsible for assigning and integrating assets from across the various affected Geographic COCOMs. Additionally, the Multi-Domain Task Force, described above, would now be associated with these new commands.

The Geographic COCOMs' role under this proposal would be reduced. Their primary roles would consist of maintaining regional expertise and ensuring the administrative and logistical needs of assigned forces were met. Furthermore, there would be less of a need for maintaining a large staff of officers since the necessary staff functions for conducting combat operations would reside at the Multi-Domain Command level. Functional COCOMs would be dissolved and their capabilities dispersed equally among the overarching Multi-Domain Commands. Figure 4 demonstrates this concept.

The final and most drastic level of change to C2 structure calls for a complete overhaul of the current system. Geographic COCOMs would be completely dissolved in favor of trans-regional COCOMs. Each trans-regional COCOM would consist of nearly the same quantity and type of assets. This would allow each of them to be capable of providing cross-domain effects. They would also be completely interchangeable given their freedom from geographic constraints. The CJCS would still maintain overall authority and, in the event of a crisis, would direct which trans-regional command had authority.

Maintaining the same capabilities and not being constrained by geographic boundaries would aim to provide the maximum amount of flexibility in responding to a crisis. However, this flexibility is predicated upon a force that is completely interoperable. Therefore, the individual services in their mission of organizing, training, and equipping must ensure complete interoperability. When the services present forces to the trans-regional commanders, these forces must be able to seamlessly operate together regardless of their

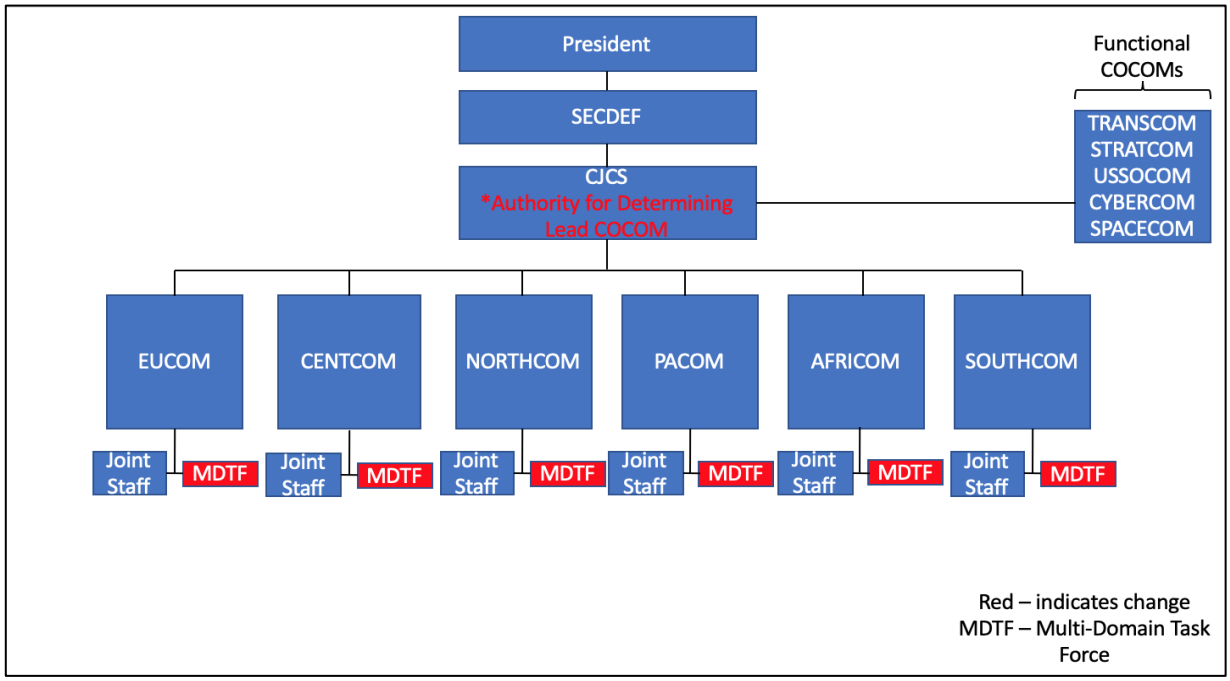


Figure 3. Minor Change to Existing C2 Structure

[34] US Department of Defense. (2018). *The National Military Strategy of the United States of America*. Washington D.C. : US DOD.

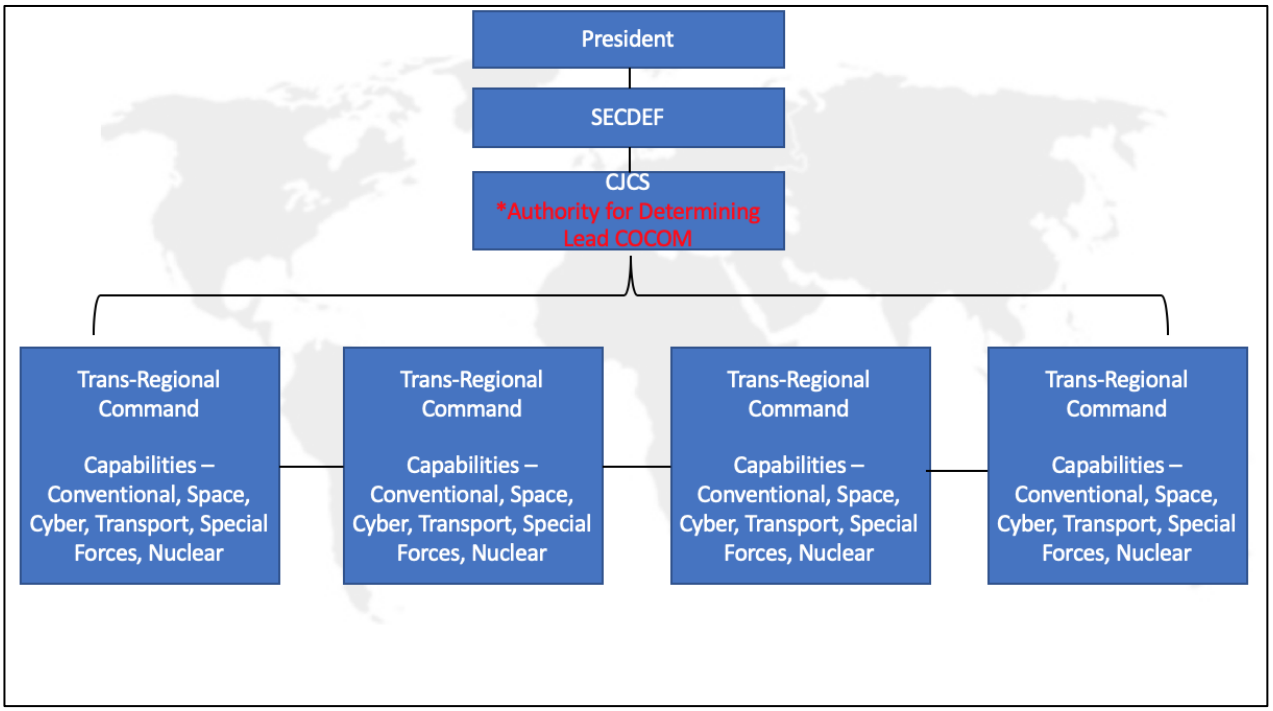


Figure 4. Moderate Change to Existing C2 Structure

location and mission set. This level of interoperability requires training in Multi-Domain Operations to begin at the start of an officer's career and have as much emphasis placed on it as their core profession. This would help induce a cultural shift within each service that would culminate with officers having a better understanding of their sister service capabilities, thus growing more effective joint capable leaders. A leader who has been raised in a Multi-Domain environment from the debut of their career will be able to process information more effectively leading to the potential of better decision-making capability. Figure 5 presents this final concept.

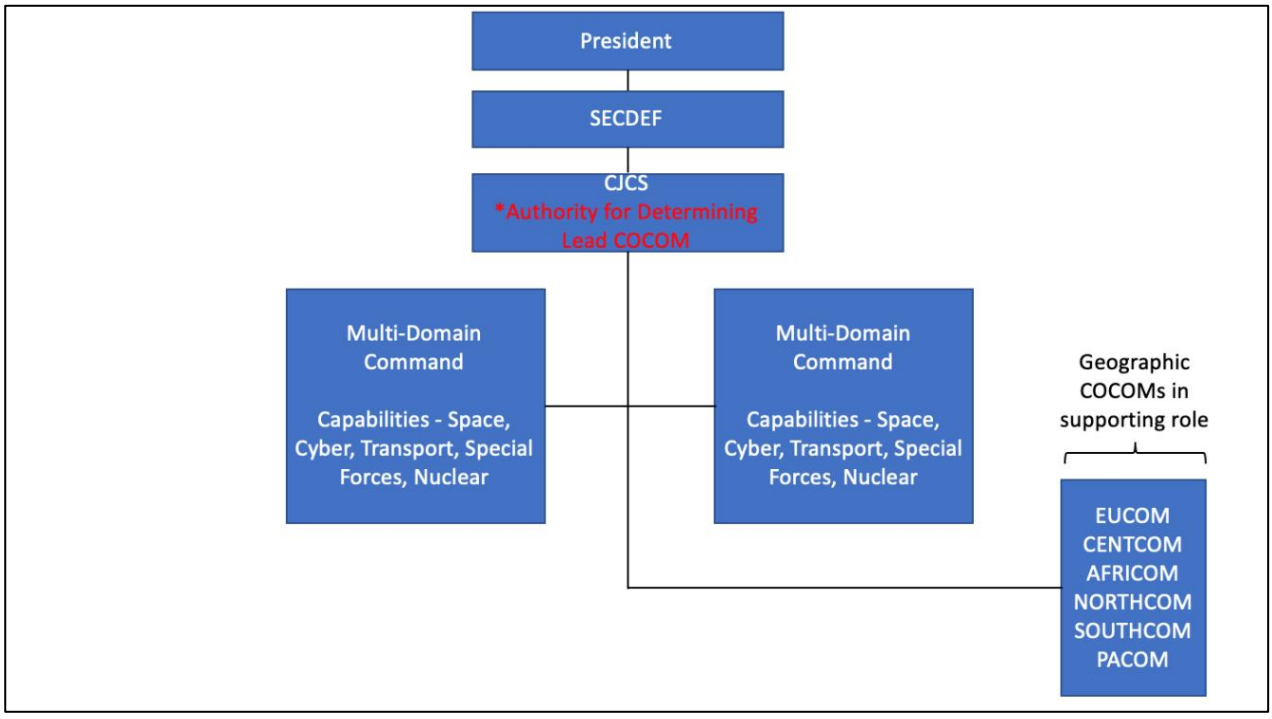


Figure 5. Major Change to Existing C2 Structure

Delegation of Command Authority

The final recommendation is concerned with the lowering of command authority in order to increase the speed of the decision-making cycle. This debate transcends the discussion on the evolution of C2 in a Multi-Domain environment. It has remained a topic of interest applicable to past, current, and future military concepts. However, due to its complexity many in the profession of arms lack an understanding on its application. While this topic alone is relevant to its own research paper, it is necessary to discuss this concept given Multi-Domain Operations' effect on C2.

Currently, due to technological advancements in the collection and dissemination of data, we have the capability to complete a kill-chain sequence in a matter of seconds. In a Multi-Domain environment, a tactical operator has the ability to remain connected with assets that correspond to each step of the kill-chain; find, fix, target, track, engage, and assess. This level of connectivity poses the question to which level should authority be delegated?

The lowering of delegated decision authority is directly related to speed of the decision-making process. The lower the level the faster decisions can be made and actions taken in a given scenario. Since the speed of completing an OODA cycle is a vital component to success in a Multi-Domain environment it would make sense the joint force should strive to lower command authority as much as possible. Furthermore, given the level of connectivity tactical operators currently possess, it is also logical to assume these operators have the best localized situational awareness.

However, tactical operators are missing a vital component of information concerning the third and fourth order effects resulting from any one decision made. These effects are related to the political, diplomatic, and economic repercussions. Effects of tactical decisions can potentially reverberate throughout the operational and strategic levels. Regardless of current technological capabilities, consideration of these higher-level repercussions is outside a tactical operator's purview of responsibility.

The understanding of political, diplomatic, and economic effects is directly related to western values of a free and democratic society. Great care is taken in target selection to ensure military actions are lawful and just. Collateral damage is thoroughly analyzed in order to avoid unintended effects regardless of kinetic or non-kinetic weapon usage. Adversaries will capitalize on mistakes and turn them into propaganda supporting their cause. Adversaries will also not afford the same level of respect towards innocent victims. This fact continues to remain true and will always cause an asymmetric disadvantage for western forces.

Values relating to respect for the rule of law and human rights is why the delegation of command authority is so complicated. Multi-Domain Operations only complicates this matter further since adversarial actions can happen at an increased frequency and speed. One way in which to strike a balance between speed and maintaining western societal values is for commanders to clearly articulate their intent and established rules of engagement must be clearly understood throughout all levels of command. These concepts are not revolutionary but become even more difficult to uphold given the increased complexity of Multi-Domain Operations.

Therefore, decision making authority that is delegated to lower echelons of command should be appropriate to the level of impact that decision will have on the political and military spectrum. The reality of Multi-Domain Operations dictates that commanders and their staffs must remain constantly engaged with subordinate levels to provide solutions to ever increasing complex problems. Tactical operators should still be given freedom to make some decisions in the absence of direct communication with higher leadership; however, in order to avoid harmful third and fourth order effects, these decisions must be made within bounds defined by clear and concise commanders intent in addition to specific rules of engagement. In summary, Multi-Domain Operations necessitates good leadership now more than ever.

Coalition based Multi-Domain Operations, an impossibility?

History has shown that seldomly a country will engage in worldwide combat operations unilaterally. Therefore, seamless interoperability is required at both an intra and inter-force level. It is likely that near-peer adversaries such as Russia and China, given the location of their current focus areas, will challenge the NATO alliance. Therefore, the US and its allies must be able to respond collectively. However, interoperability within a specific country's armed forces is no easy task. The difficulty increases drastically as more nations are required to work together. This next section seeks to outline current problems relating to coalition interoperability, examples of where progress has been made, and provide further recommendations.

Impediments to coalition interoperability

NATO currently serves as the best example at measuring coalition interoperability because it is history's longest lasting alliance and it has sought to improve its interoperability in recent decades. Following the end of the Cold War, NATO has undergone three attempts at reform; the Defense Capabilities Initiative (DCI), the Prague Capabilities Initiative (PCI), and the Smart Defense Initiative (SDI). All three reform attempts dealt with decreasing burden sharing, reducing the technology gap between the US and Europe, and increasing interoperability. Unfortunately, all three initiatives experienced very similar problems when attempting to address the topic of interoperability.

Problems associated with the DCI resulted from both a lack of interest in changing the status quo as well as a lack of political will. Following the collapse of the Soviet Union, many European nations were comfortable with the US maintaining its role as principal supplier of security, which in turn allowed Europe to focus on building its monetary Union. Smaller European countries argued, due to the size of their economies, that changes in defense spending would take years for an impact to be felt throughout the NATO alliance. To make things worse, the US proposed the acquisition of "off the shelf" ready military equipment. While this would increase interoperability there was little political incentive to take this course of action because the lack of benefit to European based defense companies. For these reasons, the DCI failed as a reform initiative.

The next reform attempt, the PCI, similarly tried to tackle the problem of interoperability between Europe and the US. The PCI, enacted in 2002, occurred during a time when NATO's focus was on combatting terrorism following the terrorist attacks of September 11th. The global fight against terrorism was able to motivate countries to work together; however, was not sufficient enough to drastically improve a country's willingness to improve on their interoperability. This was also the case because of a reduced possibility of a near-peer adversarial fight. The PCI, like the DCI, also failed to meet is intended objectives.

Finally, the SDI of 2012, hoped to succeed where the previous two attempts fell short. The overall objective of the SDI was to alleviate burden sharing, decrease the technology gap, and improve interoperability. The different approach taken by the SDI focused on creating niche competencies for each alliance member to achieve. No longer would each alliance member be required to attain the same level of military capacity. Despite the narrowed focus, the SDI still encountered a lack of political will as a result of the 2008 global recession and subsequent limitations numerous countries imposed on defense spending. Nonetheless, the SDI is still ongoing at the time of this report.

Examples of established collaborative projects

Notwithstanding the aforementioned setbacks of the DCI, PCI, and SDI, NATO has made progress with regard to increasing interoperability. This progress is seen through the establishment of multi-state collaborative centers, notably focusing in the cyber domain as well as the conducting of coalition wide training exercises. The following paragraphs will highlight the areas where coalition interoperability has improved.

A prime example of progress being made towards coalition interoperability is NATO's establishment of Centers of Excellence (COE). NATO defines a COE as:

"A COE is a nationally or multi-nationally sponsored entity, which offers recognized expertise and experience to the benefit of the Alliance, especially in support of transformation. It provides opportunities to enhance education and training, to improve interoperability and capabilities, to assist in doctrine development and/or to test and validate concepts through experimentation…"[35]

There are currently 25 COE providing expertise ranging from air operations to security force assistance.[36] Each COE is charged with creating innovative solutions to not only address challenges among alliance members but to also provide assistance to nations outside the of the transatlantic alliance.

One of NATO's COE that directly contributes to improving interoperability towards Multi-Domain Operations is the NATO Cooperative Cyber Defense Center of Excellence (NATO CCDCOE). This center is charged with supporting member nations and NATO by providing unique interdisciplinary expertise in cyber defense.[37] It also conducts research on the analysis of autonomous features of cyber operations, digital forensics, protection of critical infrastructure, Cyber C2, cyber deterrence, and cyber effects in battlefield and attribution.[38] The CCDCOE also can help plan, train, execute, and evaluate a NATO member's response to a simulated cyber threat.[39] This center helps to enhance interoperability by evaluating C2 structures in addition to certifying NATO member's ability to assume positions in the NATO Response Force.

The NATO COE focusing on C2 excellence also plays a role in improving interoperability. NATO's C2COE is the center of expertise concerning the employment of C2 structures at the operational level.[40] This organization also participates in numerous exercises throughout the year focusing on the enhancement of information, decision, and execution superiority. This focus area is directly applicable to one of the principal challenges of Multi-domain Operations; increasing the speed of the decision-making cycle.

The Baltic Defense College is another example where coalition partners are making improvements towards interoperability. This college was established by the Baltic states of Estonia, Latvia, and Lithuania. It serves as the center of strategic and operational research and also conducts professional military education to mid and senior level officers from around the EU.[41] This institution teaches primarily in English and integrates NATO principles and procedures to increase operational effectiveness and interoperability with its allies.

In addition to institutions aimed at improving interoperability, NATO also conducts coalition wide exercises such as Coalition Warrior Interoperability Exercise (CWIX) and Trident Juncture. CWIX's primary mission is to improve coalition interoperability. It accomplishes its mission by allowing nations to test current, near-term, future, and experimental capabilities alongside each other.[42] Added emphasis is placed on the evaluation of the interoperability among the various communication systems and C2 structures. The goal behind CWIX is to uncover deficiencies and provide remedies before a nation is certified as ready to participate in the NATO Response Force.

Trident Juncture also tests interoperability of NATO members, but at a much larger scale. The

[35] NATO Document MCM-236-03 "MC Concept for COE" dated 04 Dec 2003, 4.
[36] Ibid.
[37] CCDCOE. "About us". Retrieved August 3, 2019, from https://ccdcoe.org/about-us/
[38] https://www.act.nato.int/images/stories/structure/coe_catalogue_20190118.pdf
[39] CCDCOE. "About us". Retrieved August 3, 2019, from https://ccdcoe.org/about-us/
[40] NATO Document MCM-236-03 "MC Concept for COE" dated 04 Dec 2003, 4.
[41] "Agreement between the Government of the Republic of Estonia, the Government of the Republic of Latvia and the Government of the Republic of Lithuania Concerning the Baltic Defence College". (Estonia: Baltic Defense College, 2007).
[42] NATO. (s. d.). Coalition Warrior Interoperability eXercise : NATO's ACT. Consulté le 25 novembre 2019, à l'adresse https://www.act.nato.int/cwix

2018 Trident Juncture exercise involved 50,000 participants, 250 aircraft, 65 vessels, and 10,000 vehicles.[43] The alliance's ability to rapidly deploy and execute a large-scale force under arctic conditions was on full display. Whereas other exercises focus on a few areas, Trident Juncture evaluated the coalition force's capabilities in each domain. The exercise's secondary objective was to also reassure member nations of NATO's commitment to their protection against Russian aggression. The date of the 2018 Trident Juncture Exercise came shortly after Russia's largest military exercise that consisted of approximately 300,000 Russian soldiers accompanied by several thousand Chinese.[44]

Recommended areas for continued progress

Comparing the challenges exhibited by NATO's reform initiatives with the areas of successful integration such as COE and coalition wide exercises outlines a logical path to take for continued improvement of interoperability. This path includes a narrowed focus on acquiring common technologies relevant to C2. The minimum requirement for coalition success in a Multi-Domain Environment is to possess an interoperable informational architecture. This includes physical communication technologies in addition to common processes.

Focusing on interoperable communications systems is a logical path due to two important characteristics concerning European defense companies. First, it is challenging for European nations to find common ground with respect to joint military development programs. Secondly, they are subject to an intense European bureaucracy. An example of difficulty in finding common ground is the multi-variant Tiger helicopter in which each participating country has a different version. This is also highlighted by the numerous variants of the MF90. In terms of bureaucracy, European countries tend to favor military solutions posed by national industries. However, it is difficult for these industries to thrive given the varying size of European defense budgets and American dominance in the sector. However, finding common ground and cross-border agreements between European defense industries is more common in the narrowed field of electronics. This is favorable news given the necessity of interoperable communication systems.

The future path towards a more interoperable coalition force is focusing on C2 systems and processes. NATO has already established COE to address this very subject in addition to conducting numerous exercises with C2 as a focus area. Increased support must also be given to European defense companies in finding joint solutions concerning communications technologies. These recommendations will help the US and its allies in max performing their decision cycle in a Multi-Domain environment.

Conclusion

Multi-Domain Operations have drastically changed the complexity of war. Adversaries to the US and its allies understand their asymmetric disadvantage in terms of conventional military equipment and tactics. Having come to this realization, they intend to undermine conventional warfare through a combination of A2/AD strategies and operations just below the threshold of open conflict. The current C2 structure is not adequate to overcome this fundamental change in adversarial behavior. This paper analyzes the challenges Multi-Domain Operations present in order to provide recommendations for the necessary evolution of existing C2 structures.

[43] NATO. (2018, octobre 25). Trident Juncture '18. Consulté le 28 novembre 2019, à l'adresse https://www.nato.int/cps/en/natohq/news_158620.htm

[44] Masters, J. (2018, octobre 23). NATO's Trident Juncture Exercises: What to Know. Consulté le 25 novembre 2019, à l'adresse https://www.cfr.org/in-brief/natos-trident-juncture-exercises-what-know

The overall theme behind the proposed recommendations is the concept of speed. Cloud-based technologies allow for a more expeditious collection and sharing of vital information. The inclusion of AI technologies helps to increase the rate of data processing. Evolved C2 structures streamline command authorities and support the potential for a more efficient carrying out of operations. Success is still predicated upon the speed and effectiveness of the decision-making process. Multi-Domain Operations does not present a revolutionary change to this fact. It does; however, create a multitude of complexities compared to previous strategies. A country possessing an efficient and capable decision-making process can overcome one who simply possesses massive military power.

The necessary changes to C2 structures and the advancements in technology is also not a substitute for the tried and true concept of effective leadership. Commanders, now more than ever, given the complexity of operations in a Multi-Domain environment, need to be capable of breaking down extremely complex problem sets into concepts their subordinate forces can understand. This is best accomplished through a clear articulation of commander's intent and clearly written rules of engagement. The number of domains in which forces will conduct operations increases the chances for ill-intended 2nd and 3rd order effects. Commander's intent and rules of engagement are the mechanisms that will define the left and right bounds of conduct for tactical operators. Having a clear understanding of these bounds will also help to counter an adversary's attempt at disrupting communication lines, which is likely the case in Multi-Domain Operations.

The current culture of the US and allied forces as it relates to Multi-Domain Operations, does not currently suffice. All military personnel now must realize being successful does not only include being an expert in one's specific career field but requires expertise on how their career field integrates with others. This culture change needs to occur throughout the tactical, operational, and strategic levels.

This culture shift also affects US allies. Russia and China expansionism aims to affect the current global order. This will require a multi-lateral approach. Alliances such as NATO need to continue to find areas of agreement as it relates to interoperability. Analyzing past reform initiatives suggests C2 technologies and processes would be the best option. This area of continued integration also works out well based on the fact success in Multi-Domain Operations is dependent on a capable transmittal of data. Advanced technology has connected the world unlike ever before giving adversaries unprecedented access. Global problems presented by Multi-Domain Operations require a global response.

Bibliography

Azulay, D. (2019, mars 18). When Will We Reach the Singularity? – A Timeline Consensus from AI Researchers. Consulté le 28 novembre 2019, à l'adresse https://emerj.com/ai-future-outlook/when-will-we-reach-the-singularity-a-timeline-consensus-from-ai-researchers/

Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*: Springer.

CCDCOE. "About us". Retrieved August 3, 2019, from https://ccdcoe.org/about-us/

Cohen, A. (2019, avril 5). Trump Moves To Protect America From Electromagnetic Pulse Attack. Consulté le 25 novembre 2019, à l'adresse https://www.forbes.com/sites/arielcohen/2019/04/05/whitehouse-prepares-to-face-emp-threat/#576caaeee7e2

Cole, Ronald H. (1999). "Grenada, Panama, and Haiti: Joint Operational Reform" (PDF). *Joint Force Quarterly* (20 (Autumn/Winter 1998-99)): 57–74. Retrieved October 20, 2019.

Deshmukh, R., & Devadkar, Kailas . (2015). *Understanding DDoS Attack & Its Effect In Cloud Environment*. Consulté à l'adresse http://iranarze.ir/wp-content/uploads/2017/04/6554-English-IranArze.pdf

European Parliamentary Research Service. (2019). *Automated tackling of disinformation* (1). Consulté à l'adresse https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf

Farley, R. (2018, août 1). AirLand Battle: The Army's Cold War Plan to Crush Russia (That Ended Up Crushing Iraq) [Post de blog]. Consulté le 25 novembre 2019, à l'adresse https://nationalinterest.org/blog/buzz/airland-battle-armys-cold-war-plan-crush-russia-ended-crushing-iraq-27477

Feickert, A., Kapp, L., Elsea, J. Harris, L. 2018. *U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress*. Washington, DC: Congressional Research Service, November 1st. https://crsreports.congress.gov/product/pdf/R/R45392

Gricius, G. (2019, mai 11). How Russia's Disinformation Campaigns are Succeeding in Europe. Consulté le 25 novembre 2019, à l'adresse https://globalsecurityreview.com/russia-disinformation-campaigns-succeeding-europe/

Kühn, U. (2018). *PREVENTING ESCALATION in the BALTICS A NATO PLAYBOOK*. Washington D.C.: Carnegie Endowment for International Peace.

Levada Center (2017, Janvier 9), "Russia as a Great Power," Consulté le 25 novembre 2019 à l'adresse

http://www.levada.ru/en/2017/01/09/russia-as-a-great-power/.

Masters, J. (2018, octobre 23). NATO's Trident Juncture Exercises: What to Know. Consulté le 25 novembre 2019, à l'adresse https://www.cfr.org/in-brief/natos-trident-juncture-exercises-what-know

NATO. (s. d.). Coalition Warrior Interoperability Exercise: NATO's ACT. Consulté le 25 novembre 2019, à l'adresse https://www.act.nato.int/cwix

NATO. (2018, octobre 25). Trident Juncture '18. Consulté le 28 novembre 2019, à l'adresse https://www.nato.int/cps/en/natohq/news_158620.htm

NATO Document MCM-236-03 "MC Concept for COE" dated 04 Dec 2003.

Nickelsburg, M. (2019, octobre 28). What is JEDI? Explaining the $10B military cloud contract that Microsoft just won over Amazon. Consulté le 25 novembre 2019, à l'adresse https://www.geekwire.com/2019/jedi-explaining-10b-military-cloud-contract-microsoft-just-won-amazon/

Perry, Walter L., et al., editors. "Planning the War and the Transition to Peace." *Operation IRAQI FREEDOM: Decisive War, Elusive Peace*, RAND Corporation, 2015, pp. 31–56, www.jstor.org/stable/10.7249/j.ctt19w72gs.11

Puranik, M. (2019, août 19). How the rise of 5G will disrupt cloud computing as we know it. Consulté le 28 novembre 2019, à l'adresse https://www.cloudcomputing-news.net/news/2019/aug/19/how-rise-5g-will-disrupt-cloud-computing-we-know-it/

Romjue John L. "From Active Defense to Airland Battle : The Development of Army Doctrine 1973-1982"; Historical Office United States Army Training and Doctrine Command, Fort Monroe, Virginia, June 1984.

TRADOC. (2018). *The U.S. Army in Multi-Domain Operations 2028*. Fort Eustis, Virginia : US Army TRADOC.

United States Department of Defense. (2017). *Joint Operations 3-0* (17 January 2017 Incorporating Change 1 22 October 2018). Washington D.C. : US JCS.

United States Department of Defense. (2017). *Joint Operations 3-56.1* (14 November 1994). Washington D.C. : US JCS.

United States Department of Defense. (2017). *Joint Operations 5-0* (16 June 2017). Washington D.C. : US JCS.

U.S. DEPARTMENT OF DEFENSE. (2017, décembre 21). Defense Department to Move to Cloud Computing. Consulté le 25 novembre 2019, à l'adresse https://www.defense.gov/Explore/News/Article/Article/1402556/defense-department-to-move-to-cloud-computing/

United States Department of Defense. (2017). *Joint Operations 3-0* (17 January 2017 Incorporating Change 1 22 October 2018). Washington D.C. : US JCS.

United States Department of Defense. (2018). *SUMMARY OF THE 2018 DEPARTMENT OF DEFENSE ARTIFICIAL INTELLIGENCE STRATEGY: Harnessing AI to Advance Our Security and Prosperity*. Washington D.C. : US DOD.

U.S. DEPARTMENT OF DEFENSE. (2019, février 12). DOD Unveils Its Artificial Intelligence Strategy. Consulté le 25 novembre 2019, à l'adresse https://www.defense.gov/Explore/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/

US Department of Defense. (2018). *The National Military Strategy of the United States of America*. Washington D.C. : US DOD.

Wither, James K. "Making Sense of Hybrid Warfare." *Connections*, vol. 15, no. 2, 2016, pp. 73–87. *JSTOR*, www.jstor.org/stable/26326441.

The 8 Attributes of 5g Network Performance. (s. d.). Consulté le 25 novembre 2019, à l'adresse https://www.verizonwireless.com/business/articles/business/5g-network-performance-attributes/

"Agreement between the Government of the Republic of Estonia, the Government of the Republic of Latvia and the Government of the Republic of Lithuania Concerning the Baltic Defence College". (Estonia: Baltic Defense College, 2007).

Contact : iesd.contact@gmail.com

Site : https://iesd.univ-lyon3.fr/

IESD – Faculté de droit
Université Jean Moulin – Lyon III
1C avenue des Frères Lumière – CS 78242
69372 LYON CEDEX 08