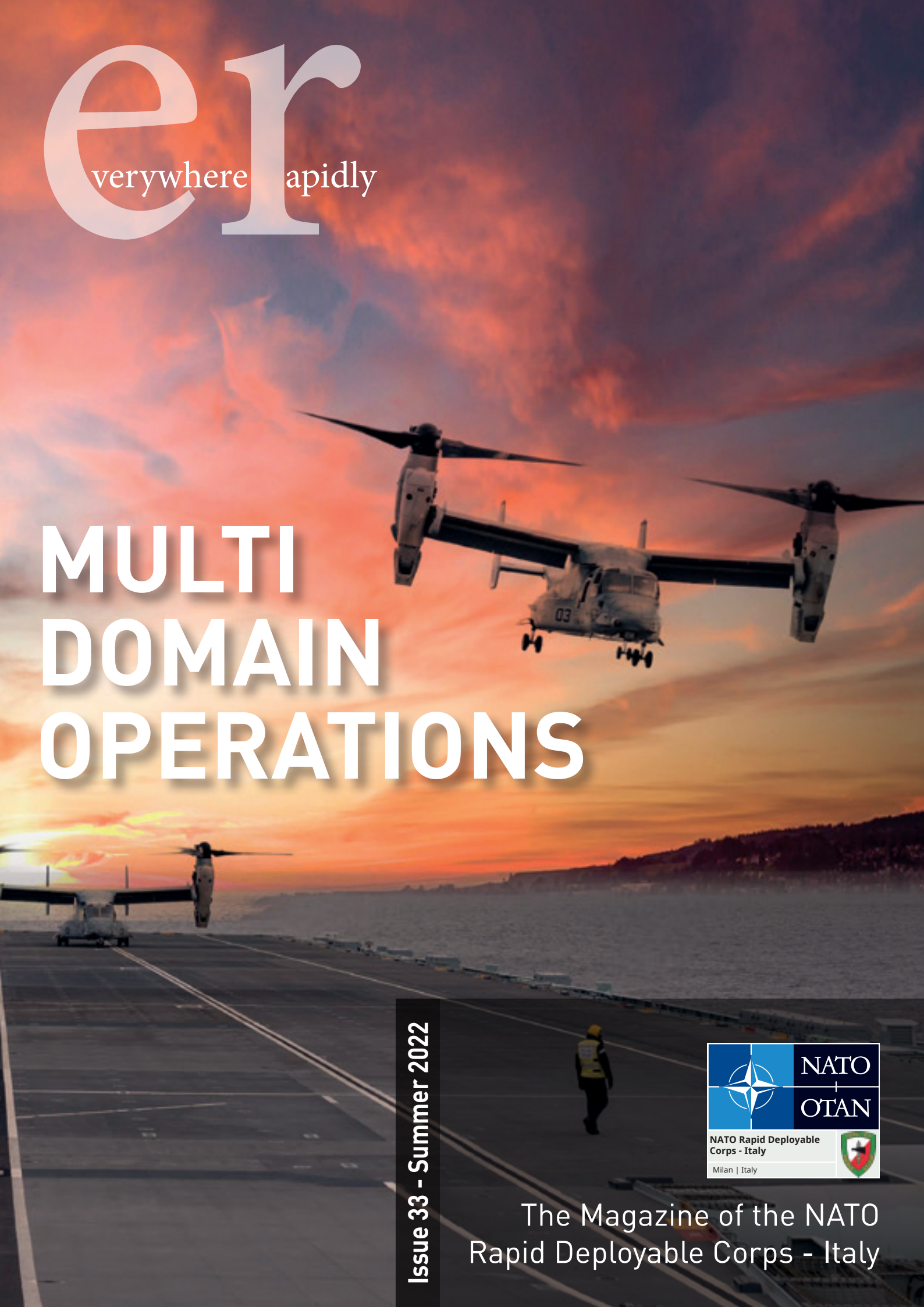
er

verywhere apidly

MULTI DOMAIN OPERATIONS



Issue 33 - Summer 2022

NATO OTAN

NATO Rapid Deployable Corps - Italy

Milan | Italy

The Magazine of the NATO Rapid Deployable Corps - Italy

NATO
Rapid Deployable Corps - Italy
Ubique Celere

/NRDCItaly

@NRDCITA

@nrdcita

NRDC-ITA

Everywhere Rapidly is the authorized official publication of the NATO Rapid Deployable Corps, Italy. All editorial content of Everywhere Rapidly is coordinated, for publication, by the Public Affairs Office.

Printed by:
Spinnaker s.r.l. - Olgiate Olona (VA)

CONTENTS

Commander NRDC-ITA

Lieutenant General **Lorenzo D'ADDARIO**

FOREWORD

Welcome to the latest edition of Everywhere Rapidly.

This edition of the Magazine is dedicated to the outcomes our recent Multi Domain Operations seminar. We hosted experts from NATO, Academia and Industry to share our perspectives and establish a common ground as we explore what MDOs mean to us, as a Corps HQ, particularly in view of our role of Joint Task Force HQ for Smaller Joint Operations (Land Heavy). Warfare is changing at a pace, and technology finds its place in the battlefield in ways that we might have not anticipated. The seminar was another step to sharpen our minds and avoid surprise. We must work to ensure that our procedures, battlerythm and products capture the opportunities that progress opens to us. As those who make of Command and Control our daily bread, we need to ensure that the unifying intent and mission, and the effects accomplishing it, are clearly laid and can be conducive of the orchestration that is required across the Domains. We must be pragmatic, concentrate on the problems that require a solution and remind ourselves that our behaviour matters: it is the first layer of co-operation, as it ensures that we all feel part of the solution. We are all precious to the Team.

On a personal note, I feel a lucky man, returning to NRDC – ITA more than twenty years after I joined the forming HQ in April 2001. I am humbled and honoured to be again part of this fantastic group, which so much has meant in my personal and professional development. It is also another great opportunity to continue to work in NATO, a lifelong learning process to improve as a Soldier for Italy and the Alliance. In addition, this is a wonderful region, full of opportunities for families.

NATO is where the allegiance to our Country springs us into a noble race to do our best. I have decided long ago that my motto, as a NATO Commander, is 'United in Commitment': we are together in our common endeavour to accomplish the Mission. In defending our values, freedom and peace, we are as one. To all members of the NRDC – ITA group, HQ and Support Brigade, our NSEs, to our families that so much put up with to support us, a very warm thank you. The events of the last few months are unequivocal as to what NATO stands for. Be proud of what you do, and let us all learn to do our best... it is worth!

I look forward to meeting you.

Multi-Domain Operations: The CIMIC perspective.

Colonel
ITA Army
Mattia ZUZZI
Multinational CIMIC Group
(MNCG) Commander

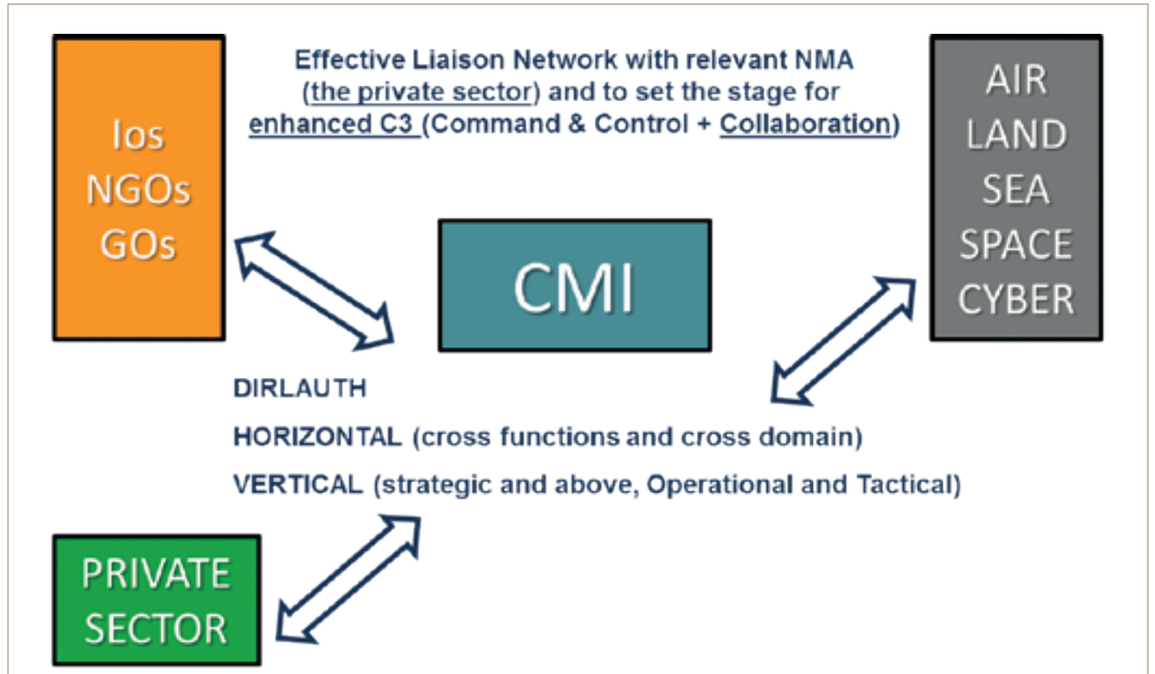
Tactical organizations should include assets that are able to perform those actions/activities related to Multi-Domain Operations (MDO). In this context, the Civil Military Cooperation (CIMIC) operational function could be considered as the interface between different stakeholders, bringing together capabilities and expertise and also allowing the flow of information from both the military and civilian domains.

The CIMIC function has a set of unique capabilities, including access to the vast and peculiar knowledge offered by subject matter experts. By thinking "out of the box", and devising innovative solutions, those could be leveraged to enhance MDOs.
Based on an interactional perspective widely used in NATO environment, we will examine the influence of CIMICer, providing an innovative approach and ideas that could contribute to the success of military operations.

Using a quasi-experimental approach, the results of this paper are contextualized and referenced, presenting the CIMIC function as an enabler, fostering both CMI and Collaboration with all the stakeholders. A Key Leader Engagement (KLE) will set the scene for CIMIC to demonstrate how civil-military interaction and collaboration can be enhanced, including the involvement of other military domain subject matter experts, and how working together can lead to the achievement of (common) effects.

Focusing on CIMIC contribution to MDO, in which MDO can be seen as NATO contribution to a comprehensive approach, it is relevant to showcase CIMIC's specific role in achieving desired effects. Particularly, in an increasingly complex, active, urbanised and connected battle-space, with no geographical boundaries, and where all domains (Air, Land, Sea, Space and Cyber) are contested, there is a paramount need to synchronize both military and non-military efforts. Thus to align and achieve effects in the virtual, physical and cognitive dimension.

In this context, the CIMIC role is specifically needed to synchronize Non Military activities to reach multi-dimensional (virtual, physical and cognitive) effects at the speed of relevance. The operative phrase is speed of relevance. For a CIMICer it means to understand the Civil Environment, assess impacts at the right time and place to support the Commander's Decision Making process so that dynamic options can be pursued in a timly, relevant manner.



Picture 1. Effective Liaison Network

Above all, the right mindset is paramount to achieve military objectives across '*all domains and environments*' Commanders should recognize that in addition to the Instruments of power[1] there are other private actors that collectively contribute to success. By orchestrating all actors' activities/contributions, the MDO Commander will achieve converging effect at the speed of relevance. Collaboration is an opportunity that is to be exploited by the Commander to maximize effects in a MDO.

In this perspective, CIMIC is a key enabler to enhance Civil Military Interaction (CMI) and collaboration. The key role of CIMIC is to connect relevant stakeholders in a synergic efforts approach. The mechanism to interact with the majority of IOs[2] , GOs[3] and NGOs[4] is in place and can be further enhanced with MoUs[5] which define roles, responsibilities and the missions of each of the parties. Alternatively, regarding the private sector, the challenge is to understand which actor is relevant in a MDO environment.

Of note, mainly neutral or friendly private actors will be considered to achieve effects. Building relationships at the highest level is essential, as it will facilitate further collaboration at lower levels. As it might be difficult for NATO military personnel representing the Alliance, to select the appropriate private sector representative, the decision is to be kept at the highest level. It is also key for the potential commander to seek Direct Liaison Authorized (DIRLAUTH) to access the relevant representatives as soon as possible.

At the earliest stage of a crisis, a potential commander should seek for DIRLAUTH[6] to access the relevant private sector representative as soon as possible.

[1] Instruments of power (IoP): Diplomatic, Information, Military, Economic, Financial, Intelligence, Law Enforcement- (DIMIFIL)
[2] International Organizations (IOs).
[3] Government Organizations (GOs).
[4] Non-Governmental Organizations (NGOs).
[5] Memorandum of Understandings (MoUs).
[6] Direct Liaison Authorized (DIRLAUTH).

Picture 2. CIMIC in MDO

In sum, we recommend the multiple SMEs, to support the tactical level Commander in:

- Identifying the CIMIC actions to support the delivery of effects as per mission assigned and in compliance with the overarching operational design;
- Identifying Non Military activities which can be performed and which he can orchestrate assuming DIRLAUTH.

REFERENCE LIST:

PO(2010)0143	*Comprehensive Approach Report;*
PO(2015)0216	*Guidelines for Engaging Local Actors*
MC 411/2	*NATO Military Policy on Civil-Military Co-operation and Civil Military Interction;*
AJP-3.19	*Allied Joint Doctrine for Civil-Military Cooperation;*
AJP-5	*Allied Joint Doctrine for the Planning of Operations;*
	UN-CMCoord, United Nations Humanitarian Civil-Military Coordination;

Protection of Civilians in Multi-Domain Operations

Dr. **Joanna SIEKIERA**

Faculty of Law
University of Bergen, Norway
Legal SME at NATO Stability Policing Centre of Excellence in Vicenza, Italy
& Finnish Defence Forces International Centre in Helsinki, Finland

When we look at the past seven decades of armed conflict since the end of World War 2, we may notice three major trends which drastically stand out. The first thing is a significant decline in the conflict between states – states being still the prime actors in the international arena, who create legally binding norms on themselves, their citizens, and other entities in international law. Secondly, there is an increase in conflicts within states, in the territory of particular states, while not anymore in the bordering area or territories of the two (or more) conflicting parties thus generating fronts. And lastly, what seems the most important from the protection of civilians (POC) standpoint, is a decline in casualty figures among combatants, but at the same time, significant harm to non-combatants occurs predominantly in urban areas.

Therefore, we can put forward a thesis that today it appears to be far more dangerous to be a civilian rather than to be a soldier in armed conflict. Civilians are being targeted not only by armed groups, so official military arms of states, but also by non-state actors (NSA) who become more and more powerful in both politics, economy, and security. Those groups deliberately attack civilians as it is one of their more effective, but also cheapest and fastest to accomplish, warfare strategies. Here not only killing is a tool. Other threats to POC which are enlisted in the latest (May 2022) Report of the United Nations Secretary-General "Protection of civilians in armed conflict": conflict-related sexual violence (CRSV), starvation, forced displacement, destruction of infrastructure, property, and livelihoods, mutilation, forced recruitment (also child recruitment), abduction, and slavery.

"Armed conflict continued to be characterized by high levels of civilian death, injury and psychological trauma, sexual violence, torture, family separation and disappearance. Conflict damaged and eroded critical infrastructure, disrupting vital water, sanitation, electricity and health services, and fuelling deprivation, hunger and displacement. The misuse of digital technologies facilitated the spread of misinformation, disinformation and hate speech, fuelling conflict and increasing the risks of civilian harm." reads the report. Knowledge about how civilians are affected by armed conflict, and what specific needs they truly need (medical, educational, legal) is indeed vital in order to effectively protect civilians from these threats.

Yet, the author's mission is to highlight the different mindsets represented by us – the Western world, the "West" and the perpetrator(s). Unfortunately, we keep losing when we expect that war criminal(s) would follow international humanitarian law principles or try their best to protect the vulnerable groups of children, women, and the disabled. No. We must assume that what is sacred for us might not, and most likely will never be, sacred for the enemy. One of the most fundamental principles in Public international law is the principle of goodwill. States do enter into international relations with such goodwill assuming that the second party will reciprocate and thus their affairs would go smoothly and in an expected manner. Nonetheless, the enemy is not only premeditated in breaching this international customary norm, but also misusing our deep faith in it.

The latest example, which caused unbearable heartache, was the Ukrainians attempt to protect own citizens by writing big inscriptions with the Russian word ĐĐĐĐ (Eng. Children) on the rooftops or before the buildings where the population was hiding before the Russian bombardment. The results? Clearly, for Russians it was a well-defined target, and they did not hesitate to use this opportunity to strike those targets and kill innocent people – civilians specially protected by the Geneva Conventions, further treaties, and above all customary law where the norm *jus cogens* (peremptory norm of general international law) forbids such extrajudicial killing.

Indeed, collateral damages occur at probably every military operation. Yet, expecting that the perpetrator would act while protecting our values is naïve and devastating not only to our military plans but foremost to the lives and state of health of those most vulnerable – civilians. Since the aggression of the Russian Federation against a sovereign state – Ukraine – on the 24th February this year, states in the Central Eastern Europe, brutally "liberated" by the Soviet Army, were certain this war will reveal deliberate targeting civilians as the main tactics of Russian troops. What Russian soldiers perform now in Ukraine, examples include raping, torturing, stealing and destroying interiors, is indeed frightening, nonetheless, it does show that the standards of the Russian army have not changed since the Soviet Union. Officers know they will not be disciplined or punished, either by their superiors or held criminally responsible, by the national courts. More importantly, there is no basic respect for another person's dignity and life. Not only for Russia but also in other authoritarian regimes such as China, Syria, North Korea, Belarus or Venezuela, human life does not matter, while PoC seems like another absurd political concept created by the West. Again, for the democratic world Russian actions in the Ukraine are inhumane. Conversely, looking from their perpetrators perspective, it is all well justified to spread own values and fight back against our "Western" values.

That is why understanding the principally different mindset, or rather using the perpetrator's lens is crucial in protecting civilians. Only then we will be able to prevent war criminals before they can deliberately target non-combatants. Multi-Domain Operations conduct is needed to combat large-scale operations underpinning the credibility of the Alliance's deterrence, and to provide the basis for the defence of the Euro-Atlantic Area. Here the keyword is indeed deterrence. We must not expect the enemy to use the same language as we speak. Deterrence does not mean diplomacy or other soft tools to Russia or China. They understand strength, they fear strength and only (military) strength is able to halt them. The governments in Moscow, Beijing, Minsk, Pyongyang or Damascus violate human rights daily by torturing, raping, abducting, murdering their citizens and other people, people of minority and political opponents. This set of values, illegal, unaccepted, and unbearable for the West is pursued with no exceptions during the armed conflict by undemocratic states, and multitude of NSA.

Mining humanitarian corridors or shooting the Red Cross convoys are additional examples of how the perpetrator (Russia) deliberately targets civilians (Ukrainians) and prevents their protection. Unnecessary damage to civilian infrastructure leads to a high degree of chaos also after conflict, when voluntary refugees would like to come back to their places of origin. This all gives a wide range of activities undertaken by the military when performing MDO, as POC does not terminate with a ceasefire but often only begins. The threat to civilians can in fact increase in situations where the timing of attacks comes in response to certain conditions. For instance, perpetrators may attack when they are about to lose control over a territory, strategic installations, or a population. This situation is observed in regime crackdowns and insurgencies. Perpetrators may also attack when opportunities arise in a post-conflict environment. This type of post-conflict revenge, can be in retaliation for a previous attack, such as in communal conflicts, or by the lack of supplies, as in situations of predatory violence. Similarly, it refers to mob violence, where few civilians would be killed, yet there is potential for much material damage and a widespread perception of fear and insecurity. Desired effects uphold by MDO should be in turn controlling and dispersing violent crowds, while avoiding the lethal use of force and escalation into more violent scenarios such as post-conflict revenge and communal conflict.

CONCLUSION

The protection of civilians is an essential objective most international military operations. In recent years, POC has become an important focus of international relations and international law, particularly in the context of United Nations (UN) peacekeeping operations. Since the early 1990s, the North Atlantic Treaty Organization has conducted operations where the protection of civilians was a central component, yet with varying degrees of success, and in some cases failure. There is no common definition of POC. The failure to adopt a common understanding among 193 Members States of the UN is also a cause of recurring friction between states, intergovernmental and non-governmental organizations. The Western system of values agreed on using the Latin expression of presumption of innocence towards civilians in armed conflict: "When in doubt, consider a person as a civilian".

Yet, we must stop expecting the enemy will use the same laws and customs as we believe in. Alternatively, we must prepare ourselves for the misuse of international humanitarian law where a single human life has been put at the top of the hierarchy of legally protected values. We spend enormous amount of money on saving, searching, helping, and curing one human life. Nonetheless, for Eastern civilisations, the biggest value is indeed society, community creating a nation or a state, where entities must scarify for the benefit of all.

Therefore, POC must be seen differently at each MDO performance, each theatre of operation, and each cultural and legal environment. Tools and measures providing effective, efficient and fullest possible POC must be indeed tailored separately to prevail conditions in a Host Nation, but also to parties involved in an armed conflict: states, NSA, humanitarian actors, all having their own understanding of POC. Thus, MDO decision-makers and commandants should consider those different, depending on the mission, capabilities, and area of operations, policies, doctrines, and guidance, to "operationalize" effective protection of civilians.

REFERENCES

ACEVES W.J.: "When Death Becomes Murder: A Primer on Extra-judicial Killing", Columbia Human Rights Law Review 2018/50.

NORWEGIAN DEFENCE INTERNATIONAL CENTRE (NODEFIC): Course on Human security and the military role.

UNITED NATIONS: Report of the United Nations Secretary-General, "Protection of civilians in armed conflict", S/2022/381, 10th May 2022.

WILLMOT H. AND SHEERAN S.: "The protection of civilians mandate in UN peacekeeping operations: reconciling protection concepts and practices", International Review of the Red Cross 2013/95.

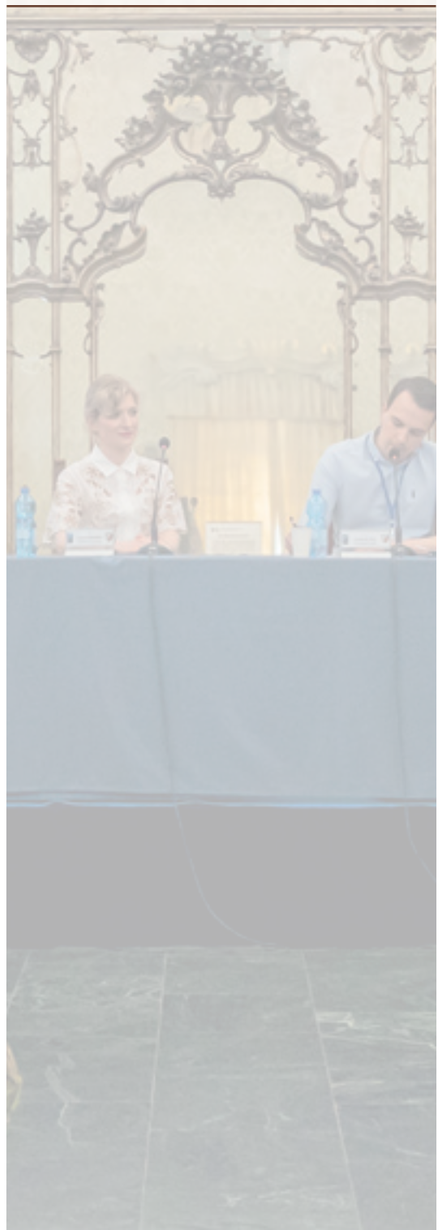
Legal aspects of Multi-Domain Operations

Dr. **Joanna SIEKIERA**

Faculty of Law
University of Bergen, Norway
Legal SME at NATO Stability Policing Centre of Excellence in Vicenza, Italy
& Finnish Defence Forces International Centre in Helsinki, Finland

Multi-Domain Operations (MDO) analysis is occurring nationally with each member state creating a policy. Additionally, the North Atlantic Treaty Organization (NATO) has yet to describe its own interpretation of MDO. This order seems expected and rational from the international law perspective. As states are the central entities in international relations, they have established secondary, derivative actors in the international arena – intergovernmental organizations (IGO), NATO is an example. Despite dramatically changing relations among states and non-state actors (NSA), as well as the growing impact of the latter on law-making and economic and military relation at the global level, states are still responsible for world order.

One of the most fundamental principles in Public international law is the principle of sovereignty. States possess the full scope of legal personality, so they are equipped with unlimited rights and duties. They leverage sovereignty to create their laws and policies in their own territory and in regard to relations they wish to establish and maintain with other international entities. *Jus tractatuum* (also called *jus tractandi*) is the Latin term referring to the right to conclude treaties, thus also establishing IGO whose legal basis is always a treaty. Finally, states create and maintain sets of norms, policies, and doctrines that reflect their interests, which differ much even among the closest neighbours. Again, this phenomenon is embedded in the principle of sovereignty and depends on each state's legal culture. Legal culture can be understood as the entirety of habits and values related to the acceptance, assessment, criticism, but also implementation of the law in force, thus the actual readiness to comply with the norms of such law. National political and social systems guarantee the protection of values and legal goods that are important for a particular society. For each society, the hierarchy of values will differ depending on tradition, religion, philosophical background, history, and natural (geophysical) obstacles.



In this way, citizens legitimise the authorities, which, after all, are the guarantors of social order and ensure development and security - both internal and external, military, energy, and more recently climate security.

Therefore, the understanding that the concept of MDO will differ among NATO's 30 Members States whose legal cultures are different is reasonable. Single terms are assigned to bipolar connotation, which all derives from a different historical background (like the noun *collaboration*, which has a very negative meaning in Central Eastern Europe and Norway) and legal culture (data exchange which might be either harmonised transnationally or be very limited due to national security proceedings).

This appears important when we consider cyber threats in MDO. So far, there is no common definition of a cyber threat. And that works well for states. Why? For the perpetrators - potential and already existing ones - breaching international law and order, thus peaceful coexistence of states in the cyber domain, such a definition would ease their criminal activities. The term threshold, from the legal vantage point, means that criminals would misuse the law by not fulfilling the whole definition of a crime (acting below the definition) thus not being responsible for that crime. Threshold cyberattacks are also hard to define, but most importantly hard to prevent and counter. We do not have any substantial laws at the international level or customary law, as this domain is far too new to obtain any international practice. Yet, we must take advantage of this lack of codification and indeed use any possible legal, political, and military tools. The enemy would use and has not hesitated so far, this legal gap against us and our Western democratic values with the human life at the top.

Inside the meaning of the four principles of MDO, there is also reference to the principle of sovereignty. NATO Member States choose to deploy the potential of MDO correctly and fully into own military doctrine and national procedures. The four overarching principles will be deemed as foundational to the successful delivery of MDO only when 30 legal systems, independent from one another, implement the concept with due diligence and openness to the general need of MDO in securing the North-Atlantic area and beyond.

1) Unity – National perspective, interests, and allies inside and outside NATO might prevail over the common effort. However, it is crucial to obtain unity in pluralism to make the best use of goodwill of the 30 Member States, as every one of them must be confident that diversity is not a source of weakness, but a significant source of strength.
2) Interconnectivity - Shared understanding and interoperability in MDO must be embedded in harmonized norms and proceedings at all domains since all NATO Member States are democratic states who follow the rule of law and transparent government mechanisms. Thus, not only at the military level but also legally, all scenarios need to be agreed and prepared.

3) Creativity – As some scenarios or multiple dilemmas cannot be predicted, the legal basis for MDO ought to have open clauses leaving some space for manoeuvre for both national and NATO decision-makers. Anyhow less important is the role of commanders who would need to command with openness and a creative mindset in order to tailor each MDO for a particular military-political-legal environment.
4) Agility – Required initiative, speed and flexibility relate to the same extent to the existing international norms and national standards as to military proceedings. Yet, it all comes down to the change of mindset from joint to multi-domain operations across all Alliance members, all domains, all dimensions, and levels of command.

As NATO does not act above the will and interest of its Allies, the same is true for creating laws that impose how MDO should be interpreted or be implemented at the national level. The concept, eventually obtaining a form of doctrine, is rather a handbook of MDO good practice that describes the level to which all Members should aim for. Those high standards will more useful for those states who are missing some military and/or political and/or legal arrangements in particular domains, like cyber. In those cases, the NATO concept for MDO will provide clear guidance as to what is expected and will be deployed in the case of armed conflict or threat to peace and security to the territories of the Allies.

Equally, modern warfare uses other than military strategies. Lawfare is gaining more and more importance, yet it is not the Western world getting benefits from it. Russian Federation has mastered lawfare, understood as misusing the international legal system with its norms and principles by damaging it, delegitimizing, or justifying own wrongful acts. The legal consequences of the Russian aggression toward Ukraine are an example. There could be some international criminal options to prosecute Russian war criminals – political leaders starting with the head of state, commandants, officers, and soldiers. The first option is the International Criminal Court. Yet, Russia is no longer a party to this court as it withdrew its membership after unfavourable sentence in 2016 claiming the incorporation of Crimea in 2014 by Russia was illegal and that territory should be returned to the Ukraine. The second option is the International Court of Justice – the judicial body inside the United Nations. It issued a sentence in March 2022 that Russia must halt its aggression on Ukraine. Still, the sentence had no enforcement measure, thus government in Moscow decided to ignore it. These are a few examples from many.

CONCLUSION

The legal aspects of MDO are essential not only to legitimize, and also embed into NATO's further endeavours in the system of international law securing peace and stability worldwide, but also to assist its 30 Member States in establishing their own procedures and striving to achieve the high standards set by NATO.

The impact of NATO using MDO in the future, perhaps in the near future, will most likely be beyond the geographical terrain of its 30 Member States. Undeniably the 21st century is called the Pacific century due to the intersections of the most significant air and maritime communication routes. It is here that the states from the outskirts of the Pacific, the so-called Pacific Rim, are fighting for influence – by keeping the old, post-colonial ties or accessing new markets or gaining political support. However, experts predict that the future of warfare will be wars for raw materials and other resources. An example is the incredible amount of valuable raw materials that lie at the bottom of the Pacific Ocean. So far, the technology has not allowed for their profitable extraction of the seabed. However, technology has been developing at an unprecedented pace, while states are awaiting the exploration of the bottom of the ocean, mainly in the high sea, which, according to the law of the sea, belongs to all humankind. This new international situation will result in not only regional but global conflicts, and one of them might eventually lead to a world war. Additionally, in such unusual, oceanic topography, each Host Nation has a diverse international legal status (dependent states, free association states, dependencies). Hence the role of MDO will play a key role in maintaining peace and stability in the Pacific region, but also globally, where we must defend our Western values that protect life and human dignity.

REFERENCES:

1 GERMAN-NETHERLANDS CORPS: "Corps Operating Concept" January 2022.

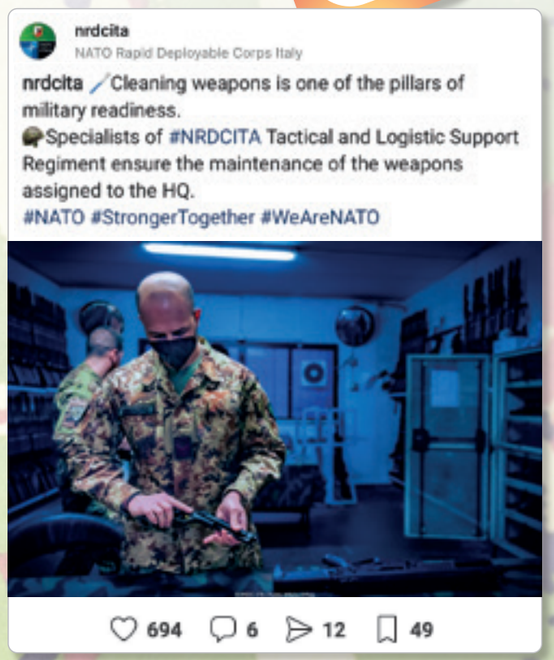
OLSON P.M.: "A NATO perspective on applicability and application of IHL to multinational forces", International Review of the Red Cross 2013/95.

INTERNATIONAL CRIMINAL COURT: "Report on Preliminary Examination Activities" 14 November 2016.

NATO: "Initial Alliance Concept for Multi-Domain Operations", June 2022.

SIEKIERA J.: "The war in Ukraine and international law – what causes its ineffectiveness?" in: Institute of New Europe, 2022: https://ine.org.pl/en/the-war-in-ukraine-and-international-law-what-causes-its-ineffectiveness.

NRDC-ITA on the WEB



Creating Competitive Space Through a Framework of Joint All Domain Maneuver

It is all too easy to suggest that the military needs to be more adaptive and imaginative in the twenty-first century. How to do so is the real question. Again, the answer is a simple matter, but its realization represents extraordinary difficulties because it involves changing military cultures…

Lieutenant General Paul Van Riper, USMC (ret.)

Mr. **Jeffrey M. REILLY**
Director of the Multi Domain Operational Strategist Concentration at the United States Air Force's Air Command and Staff College

Understanding the Requirement for Forging a Joint All Domain Operational Concept

The capacity to synchronize maneuver in multiple domains has been a fundamental cornerstone for success in military operations since antiquities. In spite of the synergy generated by maneuvering in multiple domains, many individuals are skeptical of transitioning to the concept of multi domain operations (MDO)[1]. They view MDO as a rediscovered *Lazarus Taxon* that is simply joint by another name. In the United States, the catalyst for transitioning to MDO has been the Army. What the Army has sensed is that operational environment is changing so dramatically that joint operations may no longer be effective. In 2018, the US Army's Training and Doctrine Command (TRADOC) published TRADOC Pamphlet 525-3-8. This document provides an excellent assessment of the changes in the operational environment that are mandating a transformation in the future of military operations. However, the concept used to convey the Army's vision for MDO stops short of a true transformation. The MDO concept developed by the Army bears an eerie resemblance to the Air Land Battle construct of the 1980s. The overarching approach to operations presented in TRADOC 525-3-8 appears limited to battlefield geometry and converging fires. A visualization of that approach is depicted below at figure 1. On a superficial level, there is very little difference between the Army's MDO approach and current joint operations. This is concerning because the ongoing global technological revolution mandates a greater investment of intellectual energy in the concept before it will be accepted by the military and defense communities within NATO. MDO must explicitly articulate why the concept is necessary, how the concept is different from joint operations, and present a comprehensive framework. To date none of these basic requirements have been fully achieved.

In the ideal, MDO is an advanced form of maneuver warfare designed to meet the demands of the complexity, speed, and precision that are rapidly evolving in our technologically sophisticated global environment. The essence of MDO is creating competitive space through a deliberate synchronization of combinations of domains. This is necessary for several intrinsic reasons. Those reasons involve the number of domains that require synchronization, the massive transformation occurring in civilian and military technology, and the tremendous vulnerabilities associated with the interdependencies between domains. What is being missed in the US Army's explanation of the concept is the underpinning principles of MDO that will guide offensive and defensive operations. An example of this is the interdependencies that exist between domains. The disruption, degradation or destruction of an interdependency between two domains has the potential to collapse entire systems such as command, control, communications, computers, intelligence, surveillance, reconnaissance (C4ISR).

This article has three principal objectives. The first is to provide the main arguments against transitioning to MDO. The second is to explain why transitioning to MDO is essential to future military success. The final objective is to propose an initial framework for developing MDO as a maneuver warfare concept.

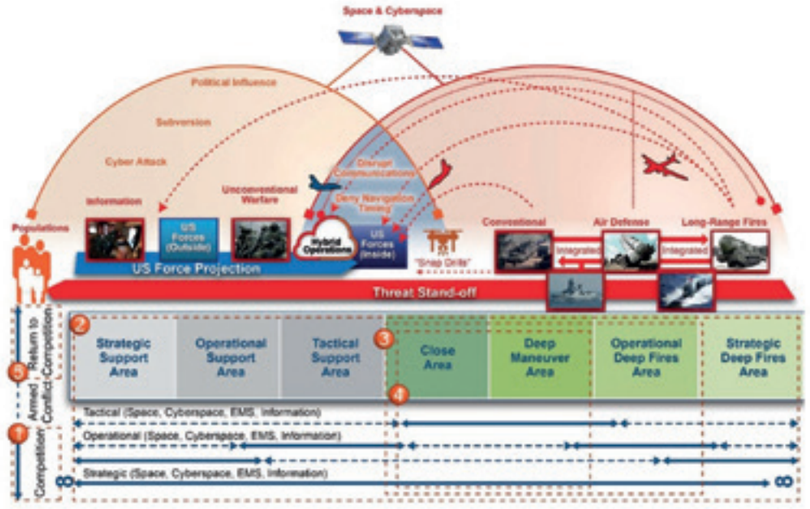


Figure 1. Source: TRADOC Pamphlet 525-3-8 – U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045, December 2018

[1] Note: The US Air Force uses the term Joint All-Domain Operations (JADO) instead of MDO. JADO are actions by the joint force in all domains that are integrated in planning and synchronized in execution, at speed and scale needed to gain advantage and accomplish the mission.

Key Arguments against Transitioning to MDO

Perhaps the foremost argument against transitioning to MDO is the persistent perception that MDO is the same as joint operations. In actuality, this is factually not true. US joint doctrine which initially codified joint operations defines joint as activities, operations, and organizations in which elements of two or more Military Departments participate[2]. Based on this definition, Joint is a concept that revolves around "additive" Service capabilities. Additionally, when the US 1986 Goldwater-Nichols Department of Defense Reorganization Act created joint operations the intent was not develop a new maneuver concept. The primary purpose of the Goldwater-Nichols Act was to enhance Service cooperation and reduce inter-Service rivalry. In contrast, MDO is a transition to a sophisticated, highly advanced form of maneuver warfare precipitated by a rapidly evolving digital ecosystem.

Another argument commonly used against MDO is the fact that multi domain maneuver is nothing new. This is factually correct. Most probably the first recorded multi domain battle is the battle of the Nile Delta which occurred in 1175 BC. In this confrontation, Ramses III, pharaoh of Egypt was threatened by a ferocious confederation of tribes known as the Sea Peoples. This confederation of tribes directed their focus toward the Egyptian empire after successfully destroying the eastern Mediterranean's coastal areas of Anatolia, Cyprus, Syria, and Canaan, In preparation for the Sea Peoples attack, Ramses assessed that the Sea Peoples' ships were technologically superior to the Egyptians and that Egypt could not defeat the Sea People's fleet at sea. To compensate for this technological disadvantage, Ramses deliberately synchronized land and maritime operations. When the Sea Peoples finally attacked in 1178 BC, he allowed the Sea people's fleet to enter into the Nile Delta unopposed. As the Sea Peoples entered the constrained confines of the delta, Ramses simultaneously attacked the Sea Peoples with the Egyptian fleet and archers on land. Unable to maneuver out of the trap the Sea People's

fleet was annihilated by Ramses[3]. Since Ramses' victory at the Battle of the Delta, the basic premise of synchronizing objectives and effects in multiple domains has never changed. What has changed, however, is the operational environment and the computational power that provides the foundation for access to domains. In terms of MDO, advances in technology have always been behind the exploitation of domains for military operations. As mankind developed new technologies, those developments provided access to domains that were previously inaccessible. This is exemplified in the advent of the ship building technology over 4,600 years ago that provided access to the maritime domain and afforded naval forces the ability to bring asymmetric effects on the land domain. In 1903, the Wright brothers flew for12 seconds at Kitty Hawk and ushered in the opportunity to take advantage of vulnerabilities on both the land and maritime domains. This was followed in October and November 1957, by the successful Soviet launches of Sputniks I and II. In the six decades since Sputnik, the entire world has become dependent on space-based capabilities. Additionally, the ongoing revolution in microchip and quantum computing technology is now providing access to the unforeseen power of key properties embedded in another emerging domain, the electromagnetic spectrum (EMS). Access to the EMS combined with advanced computing power is dynamically changing the speed, reach, lethality and sophistication of even the most basic of military operations.

[2] CJCS, DOD Dictionary of Military and Associated Terms, January 2020, p.113.
[3] Eric H. Cline, 1177 B.C.: The Year Civilization Collapsed, Princeton University Press, Princeton, NJ, 2015, p.5.

Why Transition to MDO?

The transition to MDO is a subtle, but very significant evolution in maneuver warfare theory characterized by the ability to operate within the confines of extreme complexity, speed, and precision. However, because the requirement for MDO has been evolving over decades many individuals do not recognize the need to transition or the source of causation. The overriding catalyst for transitioning to MDO revolves around the global proliferation of computing power and its impact on advanced technologies and planning, decision, and execution (PDE) cycles. In 1960, a computer engineer named Douglas Engelbart gave a presentation to the inaugural International Solid-State Circuits Conference on the concept of scaling. His theory was that future electronic circuits would be made smaller, component speeds would increase, they would require less power, and ultimately become cheaper to produce. Sitting in the audience was Gordon Moore, a future cofounder of Intel. In 1965, Moore published an observation that the number of transistors on integrated circuits doubles approximately every two years. Known today as Moore's Law, computer processing power has been doubling every eighteen months to two years and is expected to continue into the future through the processes of monolithic and systems scaling, neuromorphic microchips, and quantum computing[4].

To place Moore's Law in perspective, in 2013 the computer industry was able to place hundreds of millions of transistor on single microchip the size of a fingernail. By 2015 the industry was building 10 nanometer thick microchips capable of holding 20 billion transistors. Researchers have followed this up with 7 and 5 nanometer computer chips with 30 billion transistors. These chips are 40 per cent quicker than previous microchips and save 75 percent in power when running at the speed of current day chips[5]. One company named KnuEdge has developed a chip with 256 cores capable of running different algorithms simultaneously and connecting the cores instantly[6]. This leap in technology significantly enhances the ability to

integrate multiple functions on a single device that may have been previously incompatible or lacked the power to operate the function. The exponential growth of this computing power has created a security environment where the pace of cyber, directed energy, nanotechnology, and hypersonics are eclipsing the normal capacity to predict their effects. This change in the strategic and operational environments is significantly affecting the ability to effectively synchronize maneuver in multiple domains through joint operations alone. Although the world has undergone dramatic technological changes in the past, we are still only in the nascent stages of understanding the impact of the evolving digital ecosystem on future military operations. Additionally, advances in technology have dynamically changed all previous notions of battlespace. This is occurring because as technology has evolved it has formed interdependent relationships between the domains. As a result, access or lack of access in one domain can have cascading effects in one or more domains. The speed and lethality of conflicts in the upcoming decades will crush current PDE cycle standards and offer only limited windows of opportunity to exploit key adversary vulnerabilities occurring in a domain. The side who recognizes and understands the complexities inherent in multi domain operations and has the speed and precision to both protect and exploit domain interdependencies will be the winner in future conflicts.

[4] Monolithic scaling might be referred to as "classic" Moore's Law scaling, with a focus on reducing transistor feature sizes and operating voltages while increasing transistor performance. System scaling improvements are the gains that help us incorporate new types of heterogeneous processors via advances in chiplets, packaging, and high-bandwidth chip-to-chip interconnect technologies. See Robert Chau, A bright future for Moore's Law, Venture beast, January 7, 2020, accessed at https://venturebeat.com/2020/01/07/a-bright-future-for-moores-law/

[5] David Nield, IBM's New Computer Chips Can Fit 30 Billion Transistors on Your Fingertip: The World's first 5-nanometer Chip, Science Alert, 6 June 2017, accessed at https://www.sciencealert.com/new-computer-chips-can-fit-30-million-transistors-on-your-fingertip

[6] Jelor Gallego, An Ex-NASA Chief is Making Chips that use the Same Biological Principles as the Brain, *Futurism*, June 15, 2016 accessed at https://futurism.com/ex-nasa-chief-reveals-knuedge-a-neuro-computing-startup/

Initial Framework Recommendations for Creating a Viable MDO Concept

Developing a viable operational concept requires the examination of three basic structural elements. The first element is codifying a clear definition of what constitutes a domain. The United States' joint doctrine specifically defines the air, land, maritime, space, and cyberspace domains, however, it does not define domain. This oversight limits the inclusion or exclusion of other items that may assist in clarifying a conceptual framework. In other words, there may be other entities that should be considered as domains that are not currently identified in our doctrine. A clear definition can also limit the inclusion of miscellaneous entities such as the information or cognitive domains that may only serve to create unnecessary complexity.

The foundations for building an operational definition of domain can be found in the origins of the word. The word domain evolved from English, French, and Latin roots in the 15th century and it was used to describe what an individual, federation, or confederation controlled. In today's context, however, the traditional sense of control and the superiority it provides may be outdated by virtue of emerging offensive and defensive weapon systems. As a result, the term domain may need to include a more holistic descriptor such as "access or control." The reason this is important is if a force has access to a domain when it needs access, absolute control may not be necessary. Additionally, if we are to develop an advanced maneuver concept based on domains, the term domain must be directly correlated to the vision in the concept. Consequently, the key elements in the definition that should be present are maneuver space, access and control, and the superiority necessary to successfully accomplish the mission. A recommended definition of a domain is a "critical macro maneuver space whose access or control is vital to the freedom of action and superiority required by the mission." Based on this definition, there are six critical maneuver spaces that will dominate the future development of advanced maneuver warfare theory. Those spaces are the electromagnetic spectrum (EMS), space, air, land, maritime, and human.

This designation of maneuver spaces deviates from the evolving US doctrinal concepts being developed for MDO. The rationale for this deviation is if you have access to or control of these maneuver spaces your chances of success are significantly enhanced. Conspicuously absent

from this framework proposed in this article is cyberspace. The reason for this is cyberspace operates within the EMS. If you control desired segments of the EMS, you control the ability to employ cyberspace tools. Thus, both cyberspace operations and electronic warfare are capabilities that operate within the EMS. This does not mean that cyber operations are not important. It simply means that the desired maneuver space is what gives you the necessary access or control to accomplish the mission.

This is confusing because there are a number of misperceptions about both cyberspace and the EMS. First, cyberspace and cyber operations are not magic. Successful cyber operations require a painstaking process of gaining access to a system. This process, especially for peer competitors like Russia, can take literally years. Once a cyber-operator has access to the system, the operator must develop a tool to operate within that system. However, even with access and a tool specifically designed for a targeted system, a simple software update or change of a router can block the access to the system.

The EMS in contrast is a physics-based maneuver space that is essential to control the operational environment during all military operations[7].The spectrum represents the range of wavelengths or frequencies over which electromagnetic radiation extends. The significance of this is almost every advanced military system and concept programed for the future is dependent on access to the EMS. This includes advanced C4ISR systems, radars, missiles, aircraft, naval vessels, as well as concepts such as intuitive sensing, edge computing, hyper-automation, and almost all maneuver operations in the space domain. A representation of the EMS is below in figure 2 (page 20).

[7] Joint Publication 6-01, Joint Electromagnetic Spectrum Management Operations, 20 March 2012, p. 1-1.

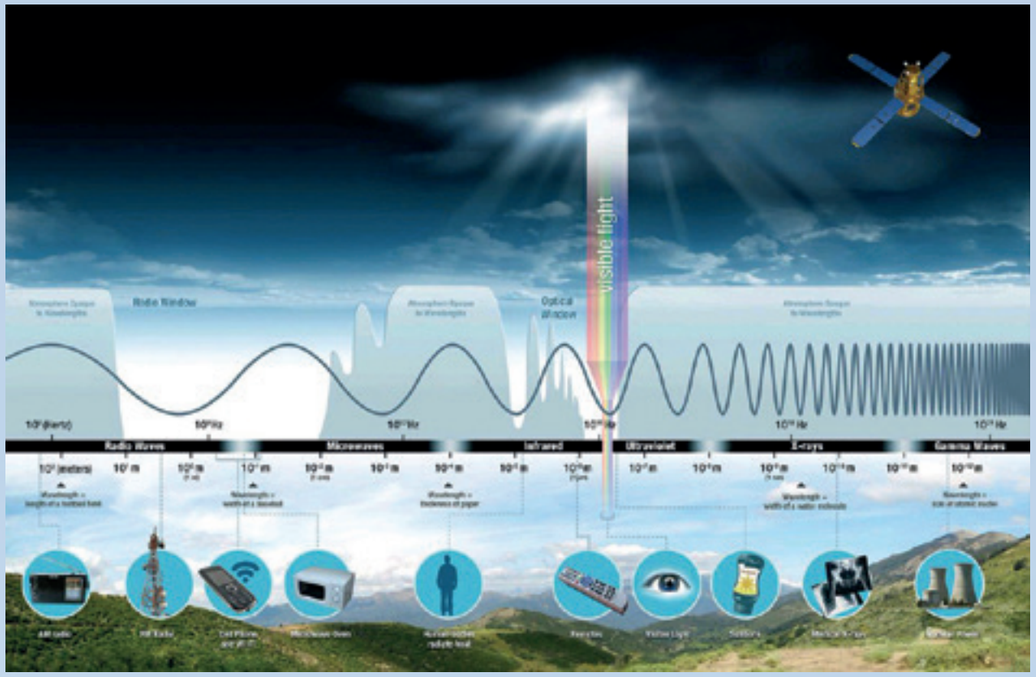


Figure 2. The Electromagnetic Spectrum. Source[8].

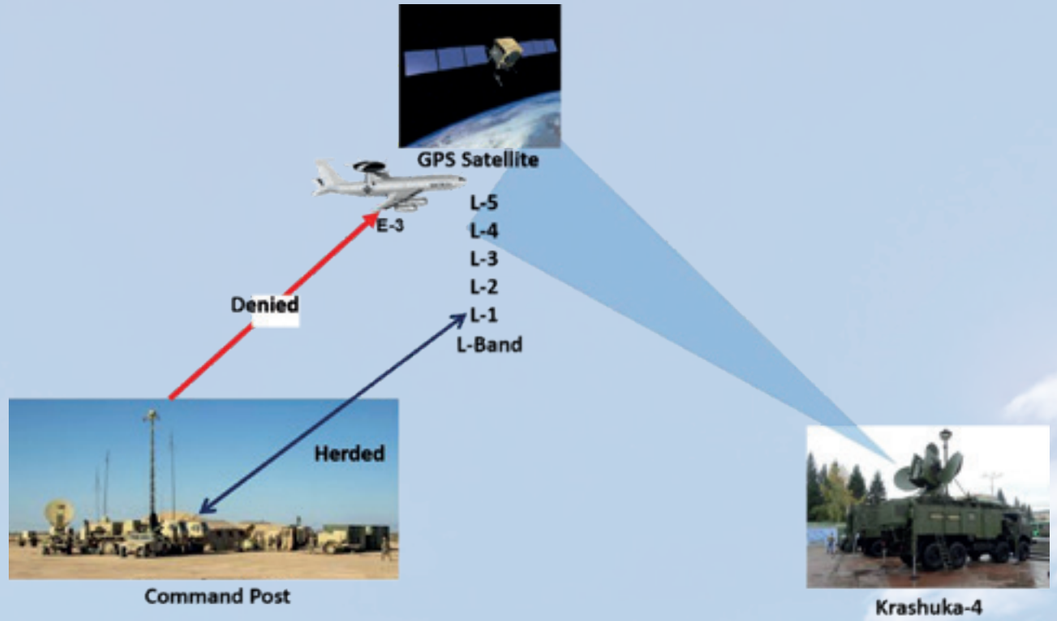


Figure 3. Example of Maneuver in the Electromagnetic Spectrum

The preeminence of the EMS is recognized by both the Russian and Chinese militaries. As far back as 1973, Russian Admiral Sergei G. Gorshkov stated, "The next war will be won by the side that best exploits the electromagnetic spectrum." Over the past decade, Russia has invested heavily in systems such as the Krasukha-4 which reportedly creates a dome that is

impenetrable to electromagnetic waves. A number of Chinese authors echo Admiral Gorshkov's assertion about the EMS. One of those authors is Wang Zhengde. In the book, *On Informationalized Confrontation*, Wang explores warfare in the electronic realm and argues "both sides in any conflict want control of the electromagnetic spectrum."

Despite the intrinsic value of the EMS there are a large number of individuals who view access to the EMS as simply a bandwidth allocation problem. Although bandwidth allocation is exceptionally important, it ignores the maneuver operations that are occurring in the EMS.

Figure 3 is an illustration of how Russian assets could create maneuver options in the EMS against US and NATO forces. In this example, a Krasukha-4 broadband multifunctional jamming station is disrupting GPS signals in L-Bands 4 and 5 from low Earth orbit (LEO) satellites. They are deliberately employing the Krasukha to control NATO's access to the EMS and herd NATO's GPS signals onto L-Band 1. This affords the Russians options to either exploit, spoof or overcrowd L-1 and slow NATO's PDE cycles. This basic example of forcing maneuver within the EMS is just one of many potential ways our adversaries will use the EMS to maneuver and achieve sophisticated objectives. This example of the EMS illustrates why a comprehensive definition of a domain is necessary. Based on the dependence of advanced technologies on the spectrum, the EMS is arguably the most important domain for future maneuver concepts. However, without a comprehensive definition of what a domain is, the EMS is either relegated to a lesser status or potentially omitted.

The failure to define domain also has repercussions on how we perceive the effect of operations on human beings. Any doctrinally approved definition of a domain must be sufficiently holistic to include desired human outcomes. One of the biggest omissions of current US and NATO doctrine is the absence of the human domain. Ironically, the "*theory of victory*" begins with an understanding of humans. In fact, all military operations from humanitarian assistance to major combat operations are inherently human endeavors. Despite this importance,

most militaries avoid the complexity of human behavior. The focus instead tends to be on information and cognition. Information is a tool used to support military operations and cognition is the process of learning. This focus, however, loses sight of the fact that military operations are directed at changing human behavior. Generally speaking, military operations revolve around three forms of behavioral change. Those changes are deterrence, compellence, and suasion. The overarching intent is to use information and cognition to influence decision making at specific behavioral focal and create the conditions for behavioral change. One military that does this well is Russia.

The Russians wage holistic campaigns across the human domain by using digital, cognitive, and psychological means to manipulate an adversary's perception of reality. Their objective is to misinform the adversary's perception and interfere with the decision making processes of individuals, organizations, and governments[9].They accomplish this through integrated information strikes that serve as a tool of coercion and create a form of reflexive control. By definition, reflexive control is "a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action[10]." It is also important to emphasize that reflexive control has long been taught at various Russian military schools and training programs, and is codified as Russian national security strategy in the Gerasimov Doctrine. An illustration of this is Russia's involvement in the Ukraine[11].

[8] The Electromagnetic Spectrum. Source: National Aeronautics and Space Administration, Science Mission Directorate (2010). Introduction to the Electromagnetic Spectrum. Retrieved March 9, 2019, from NASA Science website: http://science.nasa.gov/ems/01_intro and https://smd-prod.s3.amazonaws.com/science-pink/s3fs-public/thumbnails/image/EMS-Introduction_0.jpeg

[9] Dmitry Adamsky, "Cross-Domain Coercion: The Current Russian Art of Strategy" Proliferation Papers 54, p.27 (2015), accessed at http://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf. Accessed 26 May 2020

[10] Thomas, Timothy L. "Russia's Reflexive Control Theory and the Military." Journal of Slavic Military Studies, 2004, vol. 17, p. 237.

[11] Maria Snegovaya, Russia Report 1 Putin's Information Warfare In Ukraine Soviet Origins of Russia's Hybrid Warfare, *Institute for the Study of War*, 2015, p. 7

The key elements of Russia's reflexive control techniques in Ukraine have been:

- Denial and deception operations to conceal or obfuscate the presence of Russian forces in Ukraine
- Concealing Moscow's goals and objectives in the conflict
- Retaining superficially plausible legality for Russia's actions by denying Moscow's involvement in the conflict
- Threatening the West with military power
- Employing a vast and complex global effort to shape the narrative about the Ukraine conflict through formal and social media.

Russia's emphasis on decision making and reflexive control provides them with a unique advantage in exploiting key aspects of MDO. This is because they advocate modeling the enemy's impression about the activities of the decision-maker himself. This is combined with an understanding of the enemy's decision making processes, organizations, goals, and plans, to formulate one's own preemptive goals and plans[12]. The US fails to think in this manner because US doctrine focuses on information operations and cognition versus a holistic understanding of the human domain. Developing a taxonomy for the human domain would significantly enhance the effectiveness of US information operations.

An example of a human domain taxonomy at the operational level is shown at figure 4. A taxonomy is the practice and science of classification of things or concepts, including the principles that underlie such classification. This example highlights four salient considerations for the human domain. Those are the methods for approaching avenues of influence, establishing

key avenues for influencing decision making, focusing on behavioral change, and directing actions at specific behavioral focal points. This type of analytical model is not intended to be prescriptive. The model will change based on a number of factors including the mission, type of environment, and whether the focus is it at the strategic, operational, or tactical level. Additionally, it is vital that we precisely target specific behavioral focal points to change human behavior. In general, there are three major focal points in the human domain. Those are leaders, organizations that support the leaders, and the population. The key is understanding how humans translate into maneuver space and a recognition that the human domain is ultimate decider of success for all military operations.

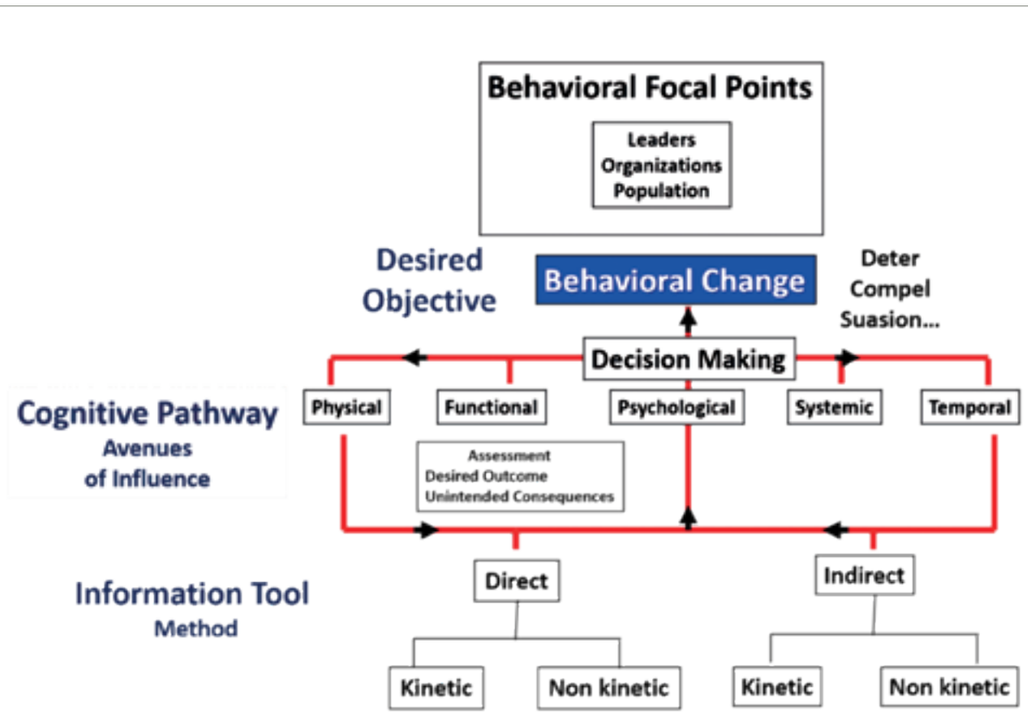


Figure 4. Taxonomy of the Human Domain

[12] Timothy L. Thomas, Russian Military Thought: Concepts and Elements, MITRE, August, 2019, p. 4-7

Based on an examination of future military operations, advanced technology, battlespace, and the definition of a domain, both the EMS and the human domain merit inclusion the emerging MDO construct. However, the real evidence for this inclusion exists in second structural element for forging a holistic MDO vision. The second structural element is a clear articulation of the interrelationships between domains. This is extraordinarily important because domains function within a continuum or whole system. This means that when one domain conducts an action or is acted upon, the impact of that action must be assessed in relation to the effects on the other domains. Understanding the arrangement of domains provides insights into how friendly and enemy systems function and the initial vision for domain priority of effort. This is significant because emerging technological efficiencies are providing access to multiple domains at the same time. This development in turn has generated deliberate interdependencies between domains. These interdependencies are highly exploitable and if left unprotected can collapse entire systems and create catastrophic consequences. This has an obvious importance for both offensive and defensive operations and is intrinsic to the success of capitalizing on fleeting opportunities. The key to implementing effective MDO schemes of maneuver is understanding how the continuum of domains functions. The Continuum of Domains is a construct that emphasizes thinking of maneuver as a whole. The continuum exists as an interconnected relationship between six key domains: the EMS, space, air, land, maritime and human. In general the EMS enables all domains. Space enables the air, land, and maritime domains which influence the human domain through access, control, exploitation of interdependencies, and protection of interdependencies between domains. A simplistic, linear illustration of the continuum of domains is at figure 5. In this illustration, the EMS attacks a critical space satellite that provides positioning, navigation, and timing (PNT) for forces in the air, land, and maritime domains. The denial of PNT affects the air domain's ability to provide close air support (CAS) and air interdiction (AI) to the land domain. It also has an impact on a Missile Defense Surface Action Group that is providing defensive counter air (DCA) to the air domain. The cumulative effect of this action is temporary paralysis of the leadership in the human domain. This temporary paralysis enables the attacking force to employ preplanned combinations of domains in either asymmetric maneuver or mass the domains for convergence at a critical point. The result is the destruction of the adversary's system and the submission of the adversary's will.

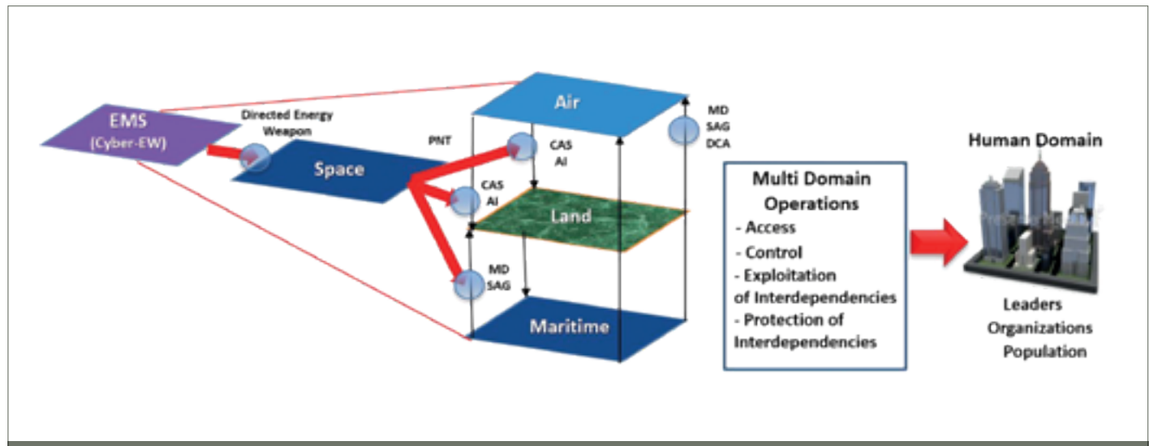


Figure 5. Domain Interrelationships within Continuum of Domains

At this juncture in the article, it is important to stress that the example of domain relationships in figure 5 is only one of many arrangements that can be employed within the continuum. The real objective is using combinations of domains to thrust complexity on the adversary and expose their interdependencies. Establishing a comprehensive vision for how domains interact within the continuum provides a crucial baseline for the third structural element for effective MDO. This element is the development of both offensive and defensive deliberate combinations of domains designed to destroy the adversary's systems and defeat their will. The US Army's approach to this is through the power of convergence. The Army defines convergence as: *Rapid and continuous integration of capabilities in all domains, the electromagnetic spectrum, and information environment that optimizes effects to overmatch the enemy through crossdomain synergy and multiple forms of attack all enabled by mission command and disciplined initiative*[13].

[13] TRADOC Pamphlet 525-3-1, GL-2

TRADOC Pamphlet 525-3-1, GL-2 A conceptual illustration of this concept is shown below at figure 6. Convergence is a very effective and lethal mode of maneuver that leverages the synergy of all domains at a critical place and time. The challenge with convergence is it diminishes the effectiveness of asymmetric domain operations that occur at the operational level. Additionally, convergence can actually simplify problem sets for an adversary when we should be imposing complexity on them. Although future operations should be thought of as a continuum or whole, it does not mean that domains must act at the exact same time or place. Actions taken within domains that dislocate or disrupt the adversary's forces can be very effective means of achieving key objectives without the risk associated with convergence. The integral element of MDO is not the convergence of domains. It is how the domains are synchronized that determines success. Even though a commander's goal may be convergence of domains or synergy between domains, the gateway to effectiveness will invariably be synchronization. The basic principle of synchronization will be one of the most dynamic components of executing successful combinations of domains and effective MDO. This will take the form of deep neural networks which will optimize the synchronization of domain actions into holistic maneuver. A framework example for a deep neural network is illustrated below in figure 7.

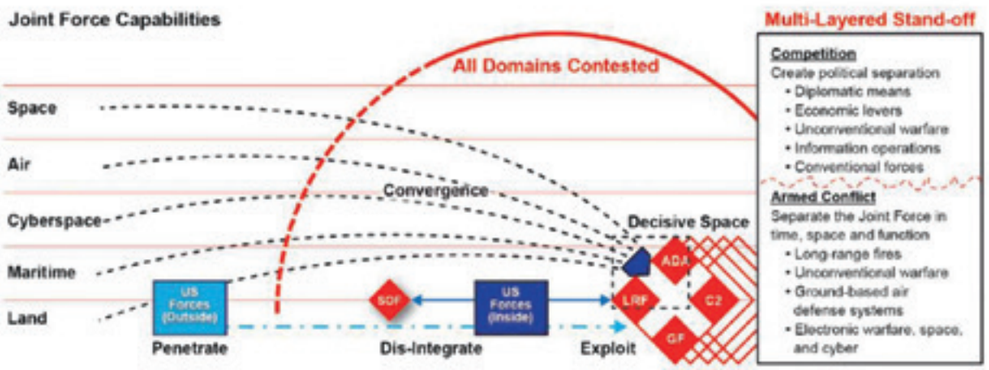


Figure 6. Convergence[14]

Factor	EMS	Air	Land	Maritime	Space	Human
Objectives						
Effects						
Adversary's Objective						
Adversary's Strengths						
Adversary's Interdependencies						
Barriers						
Time						
Distance Factors						
Risk						
Operational Actions required						
Summary Notes: Lunar Data, Sea State, Solar, Space Weather...						

Figure 7. Framework for a Joint All Domain Deep Neural Network[15]

[14] Ibid., p.26
[15] Jeffrey M. Reilly, Joint All Domain Strategist Concentration, Air Command and Staff College, Maxwell Air Force Base, AL, 2014.

This neural network synchronizes the objectives and effects between domains, assesses the adversary's use of domains, determines barriers, time, and distance factors, identifies risk, and establishes the potential operational actions required. Additionally, this network can examine factors such as lunar data, sea state, and terrestrial/space weather that impact operations. The calculations in this network can be manually calculated or computed through machine learning or augmented intelligence. The intent is not to make decisions for commanders. The goal is to speed up PDE cycles by providing commanders with potential synergies between domains. It is important to note that Russia already uses nomograms to calculate critical operational factors and speed up their PDE cycles. The Russians are also investing heavily in artificial intelligence. As a result, we cannot rely on an outdated observe, orient, decide, act (OODA) loop designed to react to an adversary. We are already at OODA point and we must realize that the ability to deal with the complexity, speed, and precision required by MDO depends on a proactive PDE cycle that shapes OODA point[16]. The key is understanding what domains are, how they interrelate, and how to synchronize them to achieve synergy and convergence.

CONCLUSION

The transition to MDO will continue to be debated in many circles in both the US and NATO. The actual transition to MDO, however, is exceptionally prudent. Our strategic and operational environments are changing so dramatically that we must develop a maneuver concept that goes far beyond "*additive Service capabilities*." Potential adversaries are leveraging emerging technology and developing operational concepts to directly challenge our approach to joint operations. Although multi domain operations is far from a new maneuver concept, the ability to deal with the emerging complexity, speed, and precision required for successful operations mandates a new operational theory. This theory must be translated into a clear operational pathway that enables NATO's forces to operate in compressed PDE cycles and proactively synchronize combinations of domains to deter and if necessary, defeat adversaries that threaten NATO. Establishing an operational pathway will require an intellectual investment far beyond battlefield geometry and fires. To be fully accepted by NATO member nations MDO must provide a framework that defines domain, explains the interrelationships between the domains, and develops advanced concepts for synchronizing combinations of domains. Until this occurs, MDO will simply be joint by another name.

[16] OODA Point refers to the compression of future planning, decision, and execution cycles.

Integrating the cyber domain in multi domain operations

The future development of military Cyberspace Operations

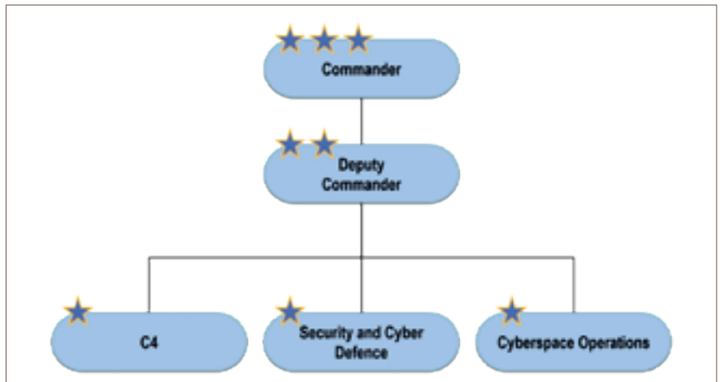
Brig. Gen.
ITA Army
Giuseppe TORTORELLI
Joint Command
for Network Operations

Throughout the history of warfare, military forces have tried to coordinate actions by land, sea and air, to acquire battlefield advantages. Now, with the development of modern technologies, the contemporary challenge is to insert and coordinate actions cyberspace into the multi domain battle. This will require new doctrinal concepts, new training programs and facilities and finally obtaining and maintaining new skills and capabilities.

Cyberspace is commonly recognized as the Fifth Operational Domain and is now part of the current warfare equation together with the conventional domains. Accordingly, the Italian Ministry of Defense (MoD)[1] , in 2020, established the Joint Command for Network Operations, to provide and manage C4/ICT[2] services, ensuring a robust cyber defense capability for the Italian Defense networks and, nonetheless, the capability to plan and conduct cyberspace operations as part of multi-domain operations.

This three-star Command centralizes competences, responsibility and chain of command of both the network infrastructure and cyber capabilities. Since last year, the Command has been fully involved in the military operations stakeholders, under the control of the Joint Operational Headquarters, along with two other two Joint Commands: Space and Special Operations.

The JCNO[3] has three Departments (see picture 1). The C4 Department provides a 24/7 service, based on the integration of NOC[4] SOC[5] and IOC[6]. The Cyber Defence & Security Department is responsible for the CERT[7] of Italian MoD, synergistically working with the aforementioned integrated operations center, to prevent and react to events and security incidents. Finally, the Cyber Operations Department plans and conducts full-spectrum cyberspace operations in counter possible threats or adverse actions against Defence Networks, Systems and Services.



Picture n.1 - Joint Command for Network Operations.

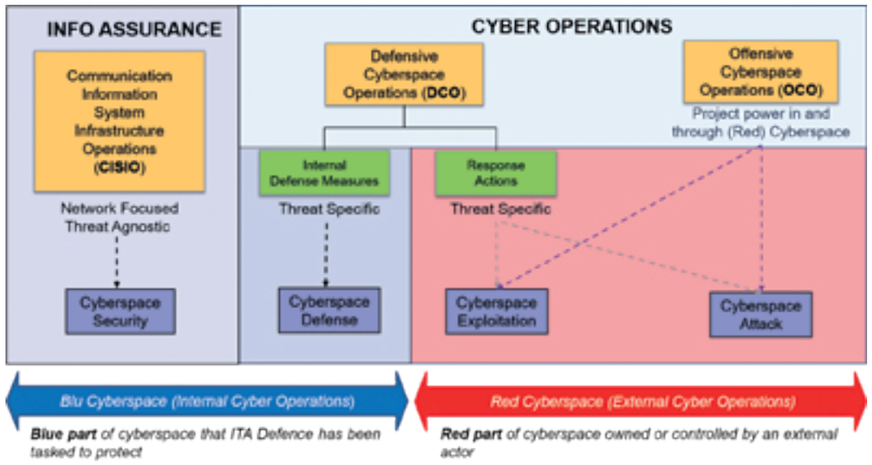
[1] Ministry of Defence
[2] Command, Control, Communication, and Computers / Information Communication Technology
[3] Joint Command for Network Operations
[4] Network Operations Center
[5] Security Operations Center
[6] Infrastructure Operations Center
[7] Computer Emergency Response Team

In the context of Military Operations, we are comfortable in referring to a joint model. However, to understand the real significance of Multi Domain Operations, we first need to understand the paradigm shift, which distinguishes these operations from traditional joint operations. Joint operations are based on the need to achieve superiority in the domain of competence.

Alternatively, the essence of Multi Domain Operations in the awareness that it is not possible to maintain supremacy in all domains. Therefore, their goal is to maintain freedom of movement in all domains to exploit any opportunity by taking advantage by the convergence of effects to be achieved through the synchronization of cross-domain actions. Carrying out Cyberspace Operations is actually a powerful enabler as an "effect" contribution to multi-domain operations. So, Cyberspace Operations should be addressed to these cross-domain purposes and better support the chain of command with increased situational awareness.

Currently it is possible to identify a series of assets, capabilities and activities that rely on cyberspace. Technologies and systems like radar sensors or logistic information platforms are critical to military operations. Most of the CNI[8], such as power grids or fuel pipelines, are controlled and supervised by specific hardware and software also called ICS[9]. Furthermore, substantial amounts of data are exchanged daily through human interactions by mean of digital tools are essential for development, commerce and services to citizens. All those mentioned technologies, assets and capabilities could be possible targets for effects like denial of services, data exfiltration, data manipulation and, in general, actions that could influence public opinion or, even worst, political decisions. Therefore, those assets and capabilities, if friendly, must be defended and in case they are enemy assets, they could be exploited.

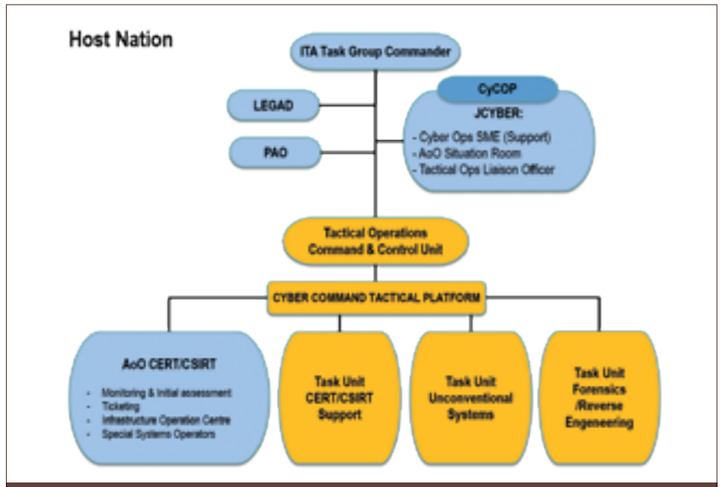
Cyberspace Operations can be split in operations that are carried out inside the boundaries of an internal infrastructure and operations that are carried beyond those boundaries (see picture 2). Hence, we identify the "Blue Cyberspace" where to conduct proactive DCO[10] and guarantee Info Assurance trough the CISIO[11] and the "Red Cyberspace" where to conduct reactive DCO without excluding the possibility to conduct OCO[12] with the aim to generate specific effects and to reach the desired end-state.



Picture n.2 - Blue cyberspace and Red cyberspace.

[8] Critical National Infrastructure
[9] Industrial Control System
[10] Defensive Cyberspace Operations
[11] Communication Information System Infrastructure Operations
[12] Offensive Cyberspace Operations

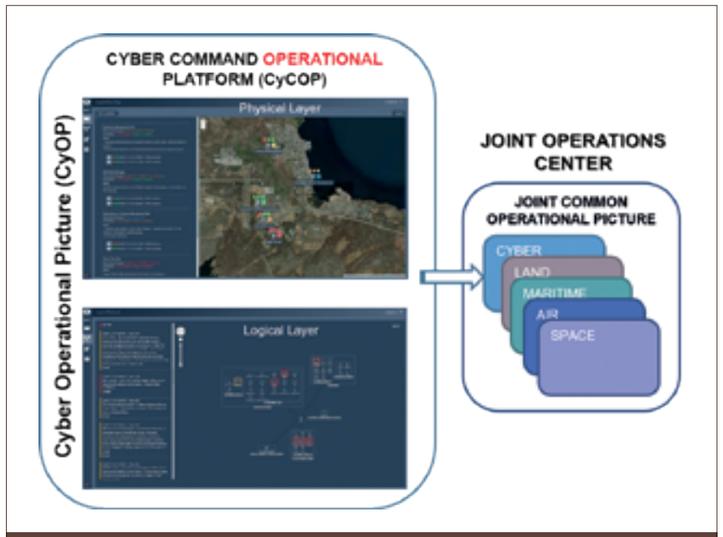
Picture 3 is an example on how a deployed Task Group can be organized, in a crisis context, to carry out Cyberspace Operations.



Picture n.3 - Deployable Cyber Task Group.

Particularly the Command Staff will be composed by SMEs[13] that include Officers for Informative Support, personnel for the Operation Control and LNOs[14] are the tactical level. The Staff will produce a recognized Cyber Operational Picture that will be shared with the JCNO, providing a reach back capability. The JCNO will receive and collect CyOPs[15] from all the active scenarios and this collection will inform a complete CyOP.

The CyOP, combined with the pictures coming from the other domains and from functional areas, will be one of the pillars sustaining the overall project of the Joint Common Operational Picture that is currently under development. The CyOP will provide the necessary bit of information concerning the Cyberspace Domain to the overall scenario of the Multi Domain Operations. See picture 4.



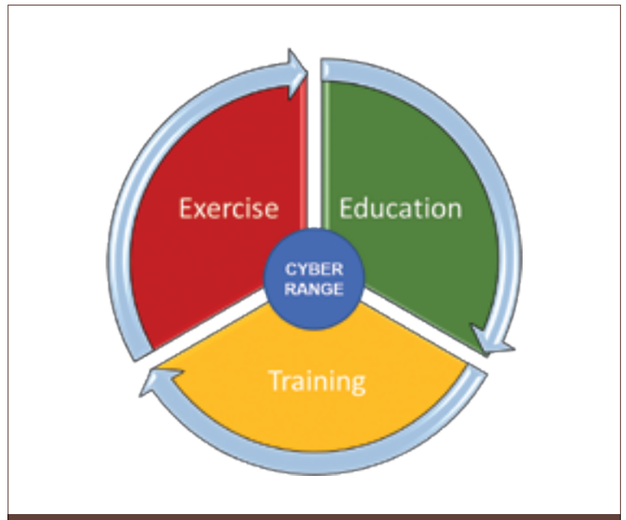
Picture n.4
Cyber Command Operational Platform and Joint Common Operational Picture.

[13] Subject Matter Experts
[14] Liaison Officers
[15] Cyberspace Operational Picture

At the tactical level, several tools like MISP[16] and others that are normally used to fulfil the internal standard procedures are grouped under the Cyber Command Tactical Platform. This platform will inform the operational tool called the CyCOP[17]. This platform will provide an updated representation of the Physical and Logical layers for the benefit of the Situation Room. In the MDO context, the CyOP will be the cyber layer of the Joint Common Operational Picture that will be displayed in the Joint Operations Center.

In summary, all the relevant information composing the Cyberspace Operational Picture are graphically represented in the Situation Room of the Joint Command for Network Operations.

Integrating the cyber domain in the MDO means not only to developing advanced technological assets but also highly professional personnel within a well-defined qualifications system, that identifies specific knowledge, skills and abilities in terms of adapting to the rapid and continuous evolution of relevant threats.



Picture n.5 - Cyber Range facility.

Additionally, a so-called "Cyber Range" is essential to long-tern success. This training tool is an opportunity to provide tailored education and simulations in which cyber professionals can perform hands-on and specialized activities to improve their knowledge.

Importantly, this need extends beyond the national level. In particular, the JCNO can be involved in several international events, selecting the most relevant ones (NATO, UE, CCD COE, International) in terms of different level of engagement (technical/tactical or operative) and specific competences required (Blue/Red Team plays).

Moreover, another future opportunity includes deploying of a Cyber Operations Component Command. That certainly needs deeper analysis and developments together with the new concept of the Cyber Rapid Reaction Teams, a high readiness Unit that could be deployed to face specific cyber issues.

IN CONCLUSION, integrating the cyberspace domain into Multi Domain Operations requires attaining and maintaining an adequate level of technical and operational capabilities. This long-term requirement is critical especially when cyber military assets are deployed abroad to support our National contingents, through the execution of Defensive Cyber Operations and mission critical IT systems hardening procedures. The JCNO is working with a group of Italian Universities and Industries, on behalf of the Defense Staff, to develop proper training facilities.

[16] Malware Information Sharing Platform
[17] Cyber Command Operational Platform

Complex Interdependence and Securitization: From International Relations to Corps Operations

Mr. **Nathan COLVIN**
Security Analyst

The narrative of Great Power Competition as a companion to Multi-Domain Operations (MDO) seems to indicate a renewal of realist international thinking. However, ideas such as complex interdependence and securitization, more analogous to constructivist thinking, reveal a more nuanced understanding for Corps and other military personnel.

Introduction

Uri Friedman observed that when the United States began closing operations in Iraq and Afghanistan, a narrative of *Great Power Competition* reemerged to describe the future international environment[1]. This narrative seems to connect to the international relations theory known as realism. The invasion of Ukraine by Russia seemed to reinforce the classic idea of Great Powers moving to control their desired spheres of influence. Certainly, this is the narrative that Vladimir Putin hoped to paint as he attempted the de-nationalization of Ukraine. However, most western security documents paint a more complex picture than the simple weighing of military power that realism relies. Although realism is adequate at times, concepts borrowed from constructivism, such as securitization, or independent ideas like complex interdependence can provide insights at the policy, strategic, operational, and tactical levels.

Figure 1 - Key U.S. Security Documents

Great Power thinking is notably outlined in the United States' *National Security Strategy* (NSS) and the 2018 *National Defense Strategy* (NDS), but also various other publications[2]. Documents such as the National Intelligence Council's *Alternative Worlds*, the Joint Chief of Staff's *Joint Operating Environment*, and U.S. Army Training and Doctrine Command's *The Operational Environment (2021-2030)* use Great Power language to describe threats which then shape military concepts and doctrine. Foundational threat documents are informed by research, experience, and study in a variety of fields, some of which include history, military affairs, intelligence studies, regional studies, and international affairs.

Understanding components of International Relations theory may seem disconnected from the operational and tactical considerations of a Corps. Clausewitz points out though that, "war is not merely a political act, but also a real political instrument, a continuation of political commerce, a carrying out of the same by other means[3]". Policy and the theory that underlies it is not just adjacent to strategy and operations, they run throughout. On one hand, international theory drives the foundation of the policies being set by political actors. On the other, theory either consciously or unconsciously informs the subject matter experts. Although not all-inclusive, examining the ideas of *securitization* and *complex interdependence* highlight that Multi-Domain Operations (MDO) are more than a return to realism's past. Instead, it is a concept that can flex to a dynamic operating environment.

Complex Interdependence

According to Keohane and Nye, political realism holds "that state behavior is dominated by the constant danger of military conflict"[4]. However appealing to a military audience, risks of nuclear exchange, resistance by technologically-enabled populations in weaker countries, disruption to economic goals, and domestic opposition to use force conspire together to erode hierarchies of military power[5]. While military power maintains certain superiorities, expense grows increasingly higher, nearing the point of cost prohibition. Traditional sources of power are still important, but not exclusively so. Complex interdependence explains this through three characteristics.

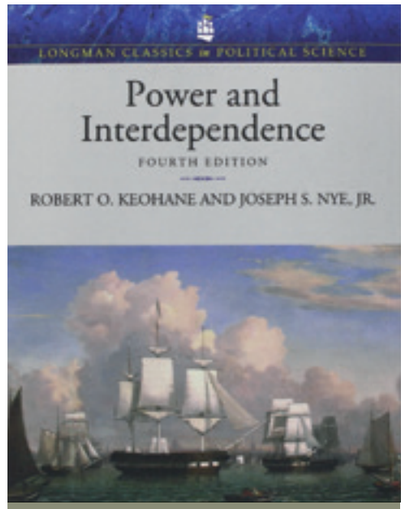


Figure 2 - Keohane and Nye's landmark Work - Power and Interdependence

First, there are multiple channels of action among interstate, transgovernmental, and transnational actors. Beyond traditional interstate relations, transgovernmental relations explain how states are composed of various stakeholders in different divisions and levels, which may have conflicting viewpoints[6]. Transnational actors include interest groups, businesses, and organizations that coordinate outside of state policy or leadership. Although driven by different values, groups from multinational corporations to the Islamic State belong in this group. These actors can create outcomes more unexpected than in strict state-on-state interactions.

Second, policy goals are not organized into stable hierarchies of most important to least important. Instead, goals are fungible and subject to trade-offs[7]. What could be a redline one day, might be subject to negotiation the next, depending on what is on the bargaining table. There is also competition in domestic and foreign affairs, meaning what is good for the military may not always be on the top of the agenda. Coalitions across governmental levels determine what issues gain preeminence.

Third, military force is not the primary determinant of issue resolution in complex interdependence blocs. For example, partners do not threaten each other with an attack to resolve internal disputes. With flexible international security agendas, existential threats are not seen as particularly likely in many countries. Therefore, force is not appropriate to solving their top challenges. In other words, having the most military capability does not provide a distinct advantage, especially if your values prevent you from applying it to important situations. Military options can also be overstretched by the breadth of complex security agendas.

In contemporary security challenges, hybrid operations and "win without fighting" strategies leverage complex interdependencies to bypass traditional military power. They do this by building asymmetric interdependence and then weaponizing that interdependence. One example is when a state like Russia creates a narrative of transnational cultural group repression by other states. To understand the power of asymmetric interdependence, one should assess the sensitivity and the vulnerability of a particular relationship. For sensitivity, "how quickly do changes in one country bring costly changes in another, and how costly are those effects?"[8] Similarly, "the vulnerability dimension of interdependence rests on the relative availability and costliness of the alternative that various actors face". In other words, sensitivity measures the costs of disruption of interdependence, whereas vulnerability measures the costs of forming self-reliance or a new interdependence. Both of these factors help determine what a policymaker may decide is most critical to elevate the security agenda. However, the preferences of a security actor do not create the security agenda alone. Instead, these preferences compete in a process known as securitization.

[1] Uri Friedman, "The New Concept Everyone in Washington Is Talking About," The Atlantic, August 6, 2019, https://www.theatlantic.com/politics/archive/2019/08/what-genesis-great-power-competition/595405/.

[2] Carl von Clausewitz, On War, trans. Michael Howard and Peter Paret, Princeton Paperbacks (Princeton, NJ: Princeton University Press, 1989).

[3] Clausewitz

[4] Robert O. Keohane and Joseph S. Nye, Power and Interdependence, 4th ed (Boston: Longman, 2012), 261.

[5] Keohane and Nye, Power and Interdependence.

[6] Keohane and Nye.

[7] Keohane and Nye.

[8] Keohane and Nye, 11.

Securitization

As previously outlined, there is no shortage of official security-related literature. These works are more than guidance; they represent a *securitizing move*. The process of securitization relies on a *securitizing move* to be put forth in a *favorable external context* and *accepted by the relevant decision audience*. Simply put, "securitization is the process by which issues become part of the security agenda[9]". In other words, actors can set the security agenda to what they think is a threat, by simply speaking about it.

Similar to Clausewitz's claim, Buzan claimed that "security is a particular type of politics" in the military, political, economic, environmental, and social sectors. The importance of securitization is that it explains the security environments constant reconfiguration. For one reason, as domestic leadership changes, they are likely to reprioritize. Security concerns can vary dramatically from country to country as well. Each nation's particular alignment of security goals may play out in operational differences of capability levels, interoperability, or caveats of use. Securitization also helps explain the spectrum of operations, since the importance of threats is subject to the eye of the beholder. Security threats ebb and flow as the environment changes. While large-scale warfare may be the most significant current threat relatively speaking, it does not eliminate the threat of smaller conflicts. Securitization helps us understand why large-scale war, terrorism, and climate change might all be addressed in a single security document.

The more developed a society, the more that they have to lose. This creates a proliferation of competing threats, which also increases the competition for resources to deal with them. For example, the economic and social benefits of the internet are widely known, which creates the impetus for guarding space and cyberspace domains. Less than a century ago, these domains would not have even entered into the mind of security actors – either as domains to protect or to be leveraged to carry out security affairs. These domains were securitized as they gained importance. As technology growth continues, it is likely that new domains of warfare will emerge. While the debate continues about the differentiation of domains, MDO goes a long way to introduce and explain "new" domains.

On the battlefield, it is important to note that securitization is not dependent on states, it can and does happen at multiple levels, by state and non-state actors alike. As the cohesive power of an adversary state dissolves, it is much more likely that securitization will splinter amongst local powerbrokers, along different issue sets. The disintegration of the adversary may increase the complexity a particular unit may face in its area of operations. This requires nuanced understanding and agile responses to maintain positions of advantage which can be exploited for further success. These operational and tactical considerations circle back to MDO.

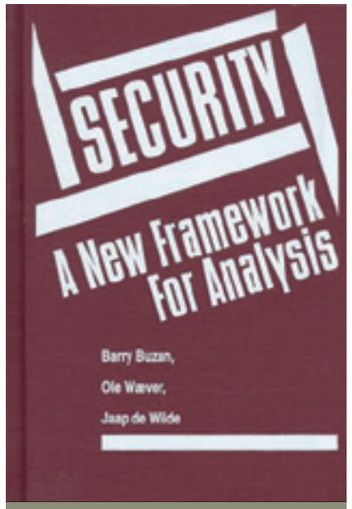


Figure 3 - The introduction to Securitization came in - Security: A New Framework for Analysis

[9] Jonna Nyman, "Securitization," in Security Studies: An Introduction, ed. Paul D. Williams and McDonald, Matt, Third edition (London ; New York: Routledge, 2018).

Relevance to MDO

The MDO concept is built as a counter to peer and near-peer military threats, which employ "stand-off" through anti-access, area-denial complexes. Looking through the concept allows for some connections to be made with complex interdependence and securitization.

First, Great Power Competition can be considered a successfully securitized topic. Among other sources, the NSS and NDS represent securitization moves that were later mirrored by other security documents. Increasing aggressiveness, especially by Russia's continued invasion of Ukraine, created an acceptable environment and audience for securitization. As long as the narrative of peer and near-peer threats survives, MDO's justification should endure as well. Corps personnel need to stay abreast of the continuous process of securitization to anticipate new security agendas the political arm may try to solve through military power.

Second, MDO is meant to challenge adversaries' ability to employ stand-off, especially during competition short of armed conflict. Adversaries attempt to separate partners politically, physically, and functionally. As complex interdependence might predict, not only does this happen through political, economic, diplomatic, and information channels, but also with military means of long-range weapons, cyber, information, unconventional, and other conventional systems. These multiple channels often overlap, as in deterrence, which is an application of military means to change political decision-making. Corps personnel can seek to understand those seemingly non-militarized ways and means that may be securitized and then used as weaponized interdependencies so that they can adapt their training and readiness appropriately. Allies will be targeted at their seams.

Third, *competition short of armed conflict* reinforces complex interdependence's idea that armed conflict is increasingly costly, especially amongst nuclear-armed states. This is why adversaries use all domains and all components of national power, many of which do not rely on traditional military capabilities. Using economic, informational, and social ways and means, they attempt to create asymmetries, which they can weaponize as needed. Not only does this highlight complex interdependence's explanation of "multiple channels," it demonstrates how different components of the environment can be securitized. In these circumstances, military professionals need to realize that they are part of an integrated or whole-of-government approach, especially during competition. Shifting between civilian and military means can be complicated, but necessary. Also keep in mind that military units are often better resourced than civilian capabilities, creating the possibility they will be used for security measures outside of strictly military uses, such as stability policing.

Fourth, securitization and complex interdependence can be used with the three tenants of MDO, which include *Calibrated Force Posture*, *Multi-Domain Formations*, and *Convergence*. For example, within *Calibrated Force Posture*, *Forward Presence Forces* and *Authorities* are primary considerations. In many cases, where forces are positioned and their authority for use takes one form when considered only from a military lens. When viewed from the multiple channels of complex interdependence, these locations may be better placed outside of the best military option, for informational or diplomatic effects. Therefore, Corps commanders and staff must be prepared to dialogue on the risk and rewards of such differences. A second example concerns *Employing Cross-Domain Fires* from a *Multi-Domain Formation*, to achieve *Convergence* of desired effects. If a military-only perspective is taken in targeting, then unintended consequences can occur. This is hardly a new phenomenon, but it can occur more frequently as complexity increases in the operational environment. Mitigations must be determined which balance unintended consequences with initiative.

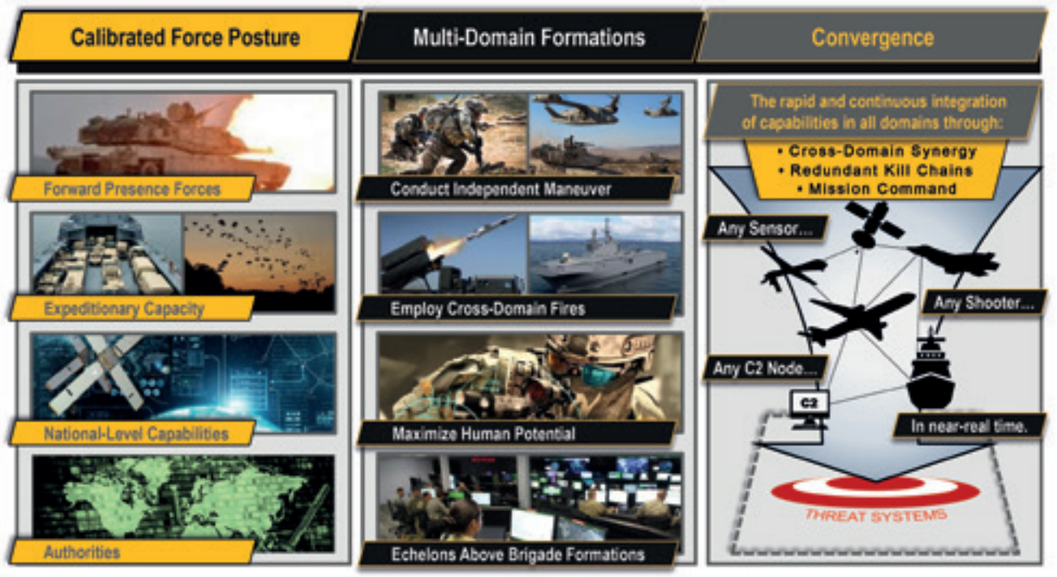


Figure 5 - The Tenants of MDO can be thought of through a wider lens than only the military element of power.
From TRADOC Pamphlet 525-3-1 *The U.S. Army in Multi-Domain Operations 2028*

CONCLUSION

Great Power thinking and threat-based approach to modernization seem to indicate an operating concept inline to a simple, realist approach to the operating environment. However, when one applies factors of complex interdependence and securitization, a more robust and complex understanding emerges. While these concepts come from an international relations perspective, they can be applied to the transition from policy to strategy and help frame conditions that operational and tactical leaders may face on the battlefield.

Complex interdependence helps commanders and staffs recognize multiple channels of power. Ambiguity is likely to emerge from the intersection of these channels. Military action may or may not be a solution to a particular security problem. Likewise, securitization helps explain the transition of the political to the military, explains the proliferation of security concerns across domains, and accounts for security issues from terrorism to large-scale warfare. Neither complex interdependence nor securitization is a magic bullet of understanding. However, when taken with other tools, these ideas can help military practitioners at all echelons develop a more complete situational awareness of the strategic and operational environment.


#WEARENATO
er
verywhere apidly
nrdc-ita.nato.int