Testo

Testo

NATO MULTI-DOMAIN OPERATIONS: CHALLENGES FOR THE EUROPEAN LAND FORCES

Written by
Ludovico Caprio
Melanie Garcia Flores
Riccardo Angelo Grassi
Caterina Toti

Supervised by
Marina Tovar i Velasco

This document was commissioned by the Warfare Branch of the UK Land Warfare Centre.

Written by: Ludovico Caprio, Melanie Garcia Flores, Riccardo Angelo Grassi & Caterina Toti

Supervised by: Marina Tovar i Velasco

Edited by: Rosário Freda

Cover design by: Gaia Durante Mangoni and Melanie Garcia Flores

This Food For Thought paper is a document that gives an initial reflection on the theme. The content is not reflecting the positions of the member states but consists of elements that can initiate and feed the discussions and analyses in the domain of the theme. All our studies are available on www.finabel.org

TABLE OF CONTENTS

Director's Editorial

As Finabel's managing director, it is an honour to present this extensive and strategic analysis of "NATO Multi-Domain Operations: Challenges for the European Land Forces". This paper comes at a time when Multi-Domain Operations (MDO) doctrine is transforming the dynamics of warfare by offering a transformative approach to how military operations are planned and executed. As threats and challenges evolve, like the extension of warfare into new domains, NATO Member States are required to reconsider and re-evaluate their defence strategies to address these emerging threats in a multi-domain battlefield. The Warfare Branch of the UK Land Warfare Centre commissioned this paper to FINABEL to analyse possible challenges faced by European Land Forces in adopting the new NATO Doctrine.

NATO's shift to Multi-Domain Operations outlines the Alliance's strategic and tactical shift to focus on interoperability and integration. The paper's analysis remarks and highlights how NATO's European land forces must adapt to the changing landscape by placing their efforts in developing their doctrine and operational capability. This shift requires to jointly implement technological advancements as well as the incorporation of new tactics. However, the focus is on encouraging a cultural switch within NATO's armed forces to foster collaboration across all domains.

The paper calls for a holistic and organisation-wide approach to MDO, challenging the Alliance to think how to leverage the best organisational structures. It draws from the strengths of all domains to achieve the strategic objectives outlined in the 2022 Strategic Concept. In the case of NATO's land forces, this comes with diverse complexities and advantages. NATO's 32 Member Countries permit an extended diversity of perspectives; while it partakes an abundance of experiences, it also requires a high degree of coordination and consensus-buildings. Precisely, this paper articulates the challenges associated with this and offers recommendations on how to tackle and overcome them. Consequently, this work is more than just a study of NATO's Multi-Domain Operations and the challenges for the European land forces; it is an opportunity to reconsider the current structures and challenges and utilise the tailored recommendations to advance in the establishment of MDO.

Sincerely,

Mario Blokken

Director

Abstract

The paper analyses NATO's move towards Multi-Domain Operations (MDO), where cyber and space domains are incorporated into conventional warfare, moving beyond joint operations. The paper highlights the primary challenges NATO faces in implementing MDO: operational adaptability, institutional coordination, technological disparities, and command-and-control structures. Consistent military doctrines within NATO Member States, recognising their historical events and cultural differences, are necessary to avoid doctrinal impediments, stressing the importance of a shared structure and vocabulary to improve coordination and efficiency in operations. The paper outlines the institutional obstacles, like NATO's absent role in coordinating the implementation of MDO, and how this translates into diverging pathways to operationalise the concept. Furthermore, challenges in technological disparities and budgetary contributions are outlined, followed by an analysis of the command-and-control structures indicating the need for Europe to seek models to develop an MDO-capable fighting force. The paper ends with a key findings section outlining the primary challenges and providing specific solutions to tackle them.

LIST OF ABBREVIATIONS

Anti-access/Area-denial	A2AD
Aperture Radar, Ground Movement Target Indicator	AGS
Command and Control	C2
Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance	C4ISR
European Defence Agency	EDA
Electronic Warfare	EW
Emerging Defence Technologies	EDTs
European Union	EU
Global Navigation Satellite System	GNSS
Information and Communication Technology	ICT
Multi-Domain Operations	MDO
Permanent Structured Cooperation	PESCO
Research and Innovation	R&I
Signals Intelligence	SIGINT
United Kingdom	UK
United States	US
Unmanned Aerial Vehicles	UAVs
US Army Training and Doctrine Command	TRADOC

Introduction

As the Allied Joint Doctrine for Land Operations underlines, a multi-domain approach is required to fight successfully on the contemporary battlefield (NATO Standardization Office, 2022). A reason for this is the developments in two relatively new domains of warfare: Cyber and Space. Activities in the Cyber and Space domains, recognised as operational domains by NATO in 2016 (NATO, 2023a) and 2019 (NATO, 2024b) respectively, profoundly impact the traditional domains by increasing the amount of data available on the battlefield and enhancing communication (US Army, 2022). The Multi-Domain Operations (MDO) doctrine aims to effectively integrate actions across all domains to deter enemies below the threshold of conflict and defeat them when necessary. The US Army first introduced the doctrine in 2018, as the theoretical successor to the 1980s AirLand Battle doctrine (Diaz de Leon, 2021). The AirLand Battle doctrine is delineated in the Field Manual (FM) 100-5, while the MDO doctrine is described in the FM 3-0 and the US Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-1.

The most apparent evolution from the 1980s doctrine to the most recent one is the inclusion of Space and Cyber in addition to the three conventional domains. As the FM 3-0 States:

> "The proliferation of space and cyberspace capabilities further requires leaders who understand the advantages those capabilities create in their operational environment. The ability to integrate and synchronize space and cyberspace capabilities at the most effective tactical echelon expands options for creating advantages to exploit." (US Army, 2022, p. 1-3)

Nevertheless, reducing the MDO doctrine to a mere addition of cyber and space to AirLand would be an oversimplification. Other conceptual developments illustrate the innovativeness of the MDO doctrine.

For starters, AirLand Battle recognised that war could no longer be fought based on the idea of a clear line of contact with the enemy. Therefore, it prescribed fighting in depth to destroy non-engaged enemy units, thus isolating and outmanoeuvring forward-deployed echelons. Deep coordination between Land and Air forces was needed to achieve this result, with friendly airpower striking the enemy in depth and providing Close Air Support, and friendly Land forces outmanoeuvring hostile forces (US Army, 2020). In contrast, the MDO acknowledges that potential rivals have developed sophisticated Anti-Access and Area-Denial (A2AD) capabilities designed to asymmetrically oppose American ability to strike in depth while simultaneously targeting friendly forces with long-range fires. The penetration and disintegration of enemies' A2AD capabilities allow freedom of manoeuvre to destroy enemies at close range. MDO doctrine is required to oppose short-, medium-, and long-range enemy fires (US Army, 2018).

Another difference is the level of conflict considered. The AirLand Battle doctrine is mainly concerned with all-out war. While the doctrine identifies multiple potential enemies, such as terrorists or Soviet-sponsored insurgents, the AirLand Battle was conceived with the threat of Soviet invasion of Europe in mind (US Army, 2020). The MDO doctrine emphasises the importance of fighting below the threshold of open conflict to deter enemies and disallow a negative *fait accompli*. As such, MDO doctrine stresses the importance of Information Warfare and the political, economic, and social variables of the operational environment (US Army, 2022).

At a more theoretical level, AirLand Battle and MDO doctrines include different tenets upon which their respective fighting philosophies are built. AirLand Battle identifies four major tenets: Initiative, Depth, Agility, and Synchronisation. Following these tenets would result in an aggressive and decisive fighting force capable of destroying the enemy on a nonlinear battlefield. The technological developments of the late Cold War, such as guided ammunition and improved communication and sensors, enabled the adoption of the AirLand Battle tenets, especially synchronisation (US Army, 2020). For the MDO doctrine, instead, the TRADOC Pamphlet identifies three different tenets: Calibrated Force Posture, Multi-Domain Formation, and Convergence. A calibrated force posture involves a "dynamic mix of different types of forces that adapt and change as dictated by the strategic environment: forward presence forces (…), expeditionary forces (…), and national-level cyberspace capabilities, space-based platforms, and strike capabilities" (US Army, 2018, p. 17). This tenet is necessary both below the threshold of violence, to deny the enemy the ability to shape the context to its advantage, and in open conflict. The Multi-Domain Formation tenet stresses the need for all Army formations to operate across multiple domains, granting resilience when manoeuvring independently and separated from other supporting units. Finally, convergence refers to the ability to operate across all domains in a fully integrated manner. In other words, it is not just two different branches that operate in a coordinated manner, but autonomously. Rather, all units operate across the different domains as a unified force. In this, the MDO doctrine goes beyond the synchronisation prescribed in the AirLand Battle doctrine.

Full integration of all domain capabilities yields two fundamental results: Cross-domain synergy, which "enhances the effectiveness and compensates for the vulnerabilities of the others (domain) to establish superiority in some combination of domains that will provide the freedom of action required by the mission" (US Army, 2018, p. 20), and layered options, providing the friendly decision-maker with multiple possible pathways to achieve a given objective, increasing the complexity of opposing friendly activities (US Army, 2018). The FM 3-0 accepts the tenets of Agility and Depth from FM 100-5 and the tenet of Convergence from the TRADOC Pamphlet, while introducing Endurance, defined as "the ability to persevere over time throughout the depth of an operational environment" (US Army, 2022, p. 3-6). This is derived from the Multi-Domain Formation Tenet. Consequently, MDO doctrine is a more sophisticated and comprehensive approach to warfare than the AirLand Battle doctrine, born out of more complex contexts and enemies. This higher level of sophistication means that the requirements for the Armed Forces adopt such doctrine are much greater.

NATO's shift towards MDOs stems from acknowledging the evolving threat landscape and its increased complexity. The national and international security environments have been deeply transformed by globalisation and informatisation, making capabilities, like rapid communications and movements of goods increase, and threats multiply because of relying on Information and Communication Technology (ICT) (Štrucl, 2022). For instance, these interconnected networks have amplified the vulnerabilities to cyberattacks to infrastructure, energy and transportation and, consequently, require more robust security measures. In this new landscape, the boundaries of warfare have outgrown their traditional perimeter to incorporate newer threats, including cyberattacks and disinformation campaigns. With the May 2023 Concept for Multi-Domain Operations, the Alliance underlines its desire to remain competitive and stay ahead of the challenges posed by modern and future warfare (NATO, 2023). By integrating the five domains, –maritime, land, air, space, and cyber– NATO aims to enhance its success and effectiveness in addressing these compound and complex threats. This will allow for coordinated and multifaceted responses to threats, leveraging strengths across different areas to create a more resilient and adaptable force.

NATO's 2022 strategic concept highlights the investments of strategic competitors in innovative and sophisticated technological capabilities and the resulting security threats to the alliance (NATO, 2022a). The document specifically mentions China and Russia, highlighting their political, technological and military abilities. China's economy, technological advancements, independent microelectronics industry and role in investing and implementing artificial intelligence position the country to be a major player and resourceful competitor (US Army, 2018). Furthermore, China has long been investing in the space sector, developing a Global Navigation Satellite System (GNSS) and direct-ascent anti-satellite missiles (Bowe, 2019). Similarly, Russia's capabilities in the cyber domain have long been recognised and its ability to shut down financial networks, power grids and other crucial infrastructure poses a significant risk (Connable, *et al.*, 2020). The war between Ukraine and Russia provides numerous examples of modern warfare shaped by new technologies. For instance, Russia's widespread use of Signals Intelligence (SIGINT) and Electronic Warfare (EW) capabilities has deeply impacted Ukrainian command and control as well as the radio connections to its Unmanned Aerial Vehicles (UAVs) (Barry, *et al.*, 2023). Similarly, the day before the invasion, threat actors close to the Main Intelligence Directorate targeted Ukrainian systems regarding government, energy, media and finance to gather intelligence and weak Ukrainian capabilities (Jones, 2022).

In confronting these threats and operating in this new warfare landscape, NATO is moving towards MDO, which NATO defines as "the orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to deliver converging effects at the speed of relevance" (NATO, 2022b). This definition underlines the importance of convergence and symmetrical cooperation to seamlessly integrate the five domains and multiple actors within the operations. NATO's commitment to this project is evident, outlining MDO as one of its three strategic priorities (NATO, 2023).

However, while NATO's Allied Command Transformation focuses on innovation to improve alliance capabilities and synchronisation, and some Members have started to improve their interoperability and allocating resources to technology to conduct MDO, NATO still needs to take concrete actions to tackle challenges and ensure readiness (Kramer, Dailey & Brodfuehrer, 2024). These actions include developing clear guidelines for MDO implementation, enhancing interoperability among Member States, and investing in advanced technologies to bridge the current capability gaps.

This paper aims to provide an in-depth overview of NATO's efforts towards MDO and the main challenges in the process. It is divided into four sections, each addressing a fundamental pillar for successfully conducting MDO. The first chapter focuses on the MDO concept's doctrinal challenges and the impact of cultural differences on operational adaptability. The discussion proceeds in the second chapter analysing the institutional implications and the lack of NATO's guidance in implementing MDO and its operationalisation by NATO Member States. The third chapter outlines the technological gap within the alliance which could hamper the success and the execution of the operations, while the last one focuses on the Command-and-Control structure (C2) necessary to conduct multi-domain operations. Each section highlights the challenges within the macro-area and provides tailored recommendations.

Operational Adaptability

Introduction

NATO Multi-Domain Operations (MDO) have raised concerns among NATO Members as MDO represents an intellectual challenge for national Land Doctrine Centres. This is due to differing interpretations of what doctrine is for and a lack of clear definitions and practical applications to translate MDO into actionable doctrine. To address the problems associated with the inclusion of MDO into NATO's operations, it is necessary to review the challenges posed by MDO and two related issues. First, NATO Members have divergent military doctrines, which are developed based on historical experiences, geographic positions, and national priorities. These doctrines guide how each country conducts operations and rationalises military objectives (Barry, 1996). If MDO is to succeed, the first step is to evaluate how each Member of the alliance views doctrine in its military, as operational effectiveness lies in doctrinal cohesion and the standardisation of objectives. Therefore, Member States need to reach an agreement by grasping the doctrine's essence and purpose, what it is and what it is for. Second, cultural differences present diverse challenges during joint operations, training or exercises. Hence, to achieve operational adaptability, it is necessary to ensure **operational compatibility** among forces (Barry, 2008), accomplished by acknowledging cultural differences and creating operational frameworks around them.

The first section of this chapter analyses the doctrinal challenges preceding MDO based on the theory of Harald Høiback (2011)[1], introducing the first challenge for NATO in defining doctrine. The second section explores the divergent doctrines among NATO's Member States, offering examples and an overview of different strategic approaches, and outlining the role of cultural differences in shaping national interests and priorities. The third section reviews the impact of doctrinal and cultural differences on the operational adaptability of MDO. Finally, the last section offers specific recommendations for enhancing doctrinal and cultural alignment.

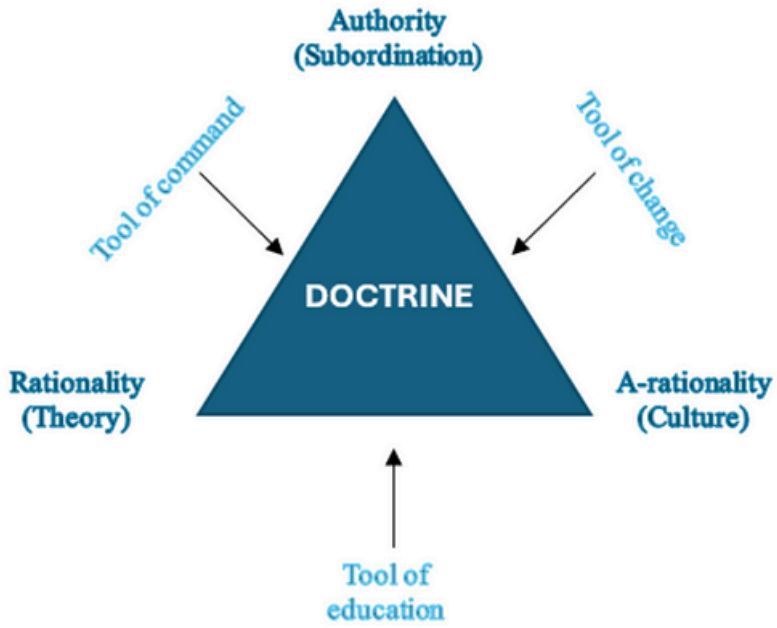
[1] Lieutenant Colonel and lecturer at the Norwegian Defense University College in Oslo. MPhil (University of Oslo); MPhil in History (University of Glasgow). PhD Philosophy (University of Oslo) on the epistemological justification of military doctrine.

Doctrinal Challenges

Doctrine has not reached a universal consensus (Palazzo, 2008), posing a problem for organisations like NATO, where doctrine has various interpretations in different countries. According to Høiback (2011), doctrine presents two essential problems: it is not good at defining principles and often suffers from a lack of references. The texts are generally written simplistically, usually based on "best practices" rather than solid references that allow the armed forces to effectively study and internalise concepts, resulting in a generic doctrine. Consequently, MDO could be workable only if NATO Member States agree first on what doctrine is and what it will be for. The main problem in defining what doctrine *is* relies on defining its purpose and scope, as the way to define its purpose depends on how each country constitutes *the threat*. For this, Høiback (2011) States that doctrine should not and cannot be the same for every country because it must be relevant to the people that are going to use it. Consequently, MDO needs to include a common language and framework of reference, which are key for it to gain authority and relevance.

Doctrine is not the only way to interpret war and operational challenges, but it is still essential for success. Høiback (2011) offers a formula to produce doctrine, which needs a type of *theory*, on what leads to victory, based on reason rather than mere opinions. Second, doctrine needs to consider cultural elements. Third, doctrine must carry some form of *authority.* Consequently, based on how these elements are balanced, doctrine-makers can expect three ideal types of doctrine: 1) doctrine as a tool of education; 2) doctrine as a tool of command; and 3) doctrine as a tool of change (see figure 1).

Figure 1. The anatomy of doctrine and the utility span



Source: Adapted from “What is doctrine?” by H. Høiback, Journal of Strategic Studies, 2011.

In the first place, doctrine as a tool of command specifies what the armed forces should do in various situations. Secondly, doctrine as an educational tool helps soldiers learn how think about and approach war. Finally, leaders can use doctrine as a tool of change to set a new direction for the military (Høiback, 2011). Altogether, this theory can serve as a starting point for improving MDO and determining how this doctrine should be used based on common objectives and capabilities while considering national differences.

Doctrinal and Cultural Differences within NATO

When considering how to approach doctrine, it is essential to understand how countries have historically used it. Countries that have engaged in expeditionary wars will know the exact geography where they will be fighting and will tend to see doctrine as a tool of education by which armed forces learn how to apply some abstract principles in unpredictable situations. The United Kingdom (UK) and the United States (US) are good examples of educational doctrine, compared to Germany, which has confronted homogenous strategic challenges, orienting its doctrine as a tool of command (Høiback, 2011). Yet, military organisations cannot always choose the conflicts they will face, and contemporary threats are increasingly unpredictable, rendering doctrine generic and inoperable. Hence, NATO must address national differences and adopt a regional-oriented framework to navigate diverse challenges across the alliance. Palazzo (2008) suggests that such a framework can reduce the danger of short-warning attacks. Therefore, defined, agreed upon and collectively established priorities will help suppress national agendas for the common good.

As NATO's complex multi-tier structure tends to be divided rather than unified, Noetzel and Schreer (2009) argue its Member States are now split into reformist, status-quo, and reversal-oriented groups. This fragmentation hinders strategic cohesion and interoperability because each national doctrine reflects its unique geopolitical context and defence policies. For example, some NATO Member States can be sorted by their strategic orientations as follows (see table 1):

Table 1. Strategic Orientations within NATO

Countires/Regions	Group	Definition
U.S. U. K	Reformist	Countries advocate for modernization and transformation of NATO's operational frameworks. Support proactive policies, promote defence spending and technological innovation to address new security challenges.
Germany Italy (many Western European members)	Status-quo	Countries prefer to maintain the current strategic and operational structure. Generally prioritizing stability and continuity. They are more cautious about rapid changes.
Some Eastern Europe members	Reversal-Oriented	Countries often advocate for restoring NATO's core mission of collective defence by focusing on traditional adversaries like Russia. They tend not to be responsive to invest resources away from this foundational mission.

Note: Elaborated from "Does a multi-tier NATO matter? The Atlantic alliance and the process of strategic change" by T. Noetzel and B. Schreer, Royal Institute of International Affairs, 2009.

The diverse strategic priorities shown in Table 1 may generate challenges to effective interoperability. NATO Member States reflect unique geopolitical contexts, creating obstacles to adopting new approaches, including MDO. Consequently, national doctrines determine how MDO will be integrated into the alliance. For instance, France emphasises autonomy and the rapid deployment of forces, contrasting with the UK's priority on interoperability with the European Union (EU) and NATO. Another significant difference lies in the US's substantial investments in technological development and space capabilities, which might not align with other Member's capabilities and traditional approaches, such as Germany's focus on mechanised land forces. Additionally, Italy and Türkiye's regional orientations can cause imbalances in operational tactics, undermining cohesion and effective coordination and contrast with Poland, which prioritises territorial defence and deterrence due to its proximity with Russia (Barry, 1996). Therefore, NATO must develop new institutional mechanisms for building strategies based on consensus. These should establish achievable goals and realistic objectives that consider the alliance's capabilities overall and delineate how MDO can play a role in the context of national priorities.

Diverse national doctrines are not necessarily obstacles; they present opportunities for innovation (Karber, 2008). The success of MDO will depend on how well it integrates with NATO and national doctrines. Conversely, different national specialisations can benefit the alliance in several ways:

- Sharing knowledge and complementing the alliance's priorities through a holistic approach.

- Geographic-based specialisation to cover all of NATO's flanks. Not all Members need the same capabilities in all domains. Instead, they can focus on their areas of expertise to strengthen NATO and protect all Members of the alliance.

- Enhance functional interoperability. At Europe's Joint Multinational Readiness Centre, diversity promotes functional interoperability to improve capability and capacity. For instance, in a 2014 exercise, the 173 IBCT (A) used a Czech 152mm artillery battery, whose doctrine focused on concealment and movement. This offset the call for fires and their delivery. To fill the gap, the 123 IBCT (A) introduced event-based time triggers enabling successful and accurate joint fires (Derleth, 2015).

Cultural Differences

Cultural differences are inevitable within organisations with a global vision such as NATO. However, while politics may unify culture, it also holds the power to differentiate it (Eagleton, 2000). Accordingly, military strategy and doctrine emerge as products of cultural identity that can hardly be applied universally (Strachan, 2006). Military doctrines are influenced by traditions, language, values and social norms, shaping the behaviour of military organisations and often being the main reason for resisting change (Farrell & Terriff, 2002).

When studying military doctrine, it is necessary to examine cultural determinants and the context of strategy to avoid oversimplifications on how a country understands war and sets military objectives. National stereotypes and cultural ideas about strategy do not provide a deep understanding of national strategies (Strachan, 2006) as these approaches are often ineffective and simplistic. Instead, detailed and nuanced analyses are needed to understand different cultural contexts, also considering how linguistic variations may impact military operability. For MDO, this is a foundational barrier to comprehending military concepts. Conversely, military identity can also facilitate change depending on effective leadership to navigate cultural contexts when implementing changes as relevant as MDOs (English, 2004). The following examples illustrate how studying cultural differences can help determine the type of doctrine a country follows:

- **Canada:** Canadian culture is influenced by its historical roots, mainly its British military heritage. The legacy of the British Army inherited values such as discipline, hierarchy and sense of duty. This influenced Canada's participation in major conflicts resulting in a distinctive combination of readiness and peacekeeping ethics. Honour and loyalty are at the core of their military identity, which aligns with Canada's objectives to promote an image of peace and justice (English, 2004).

- **US:** The Vietnam War led to a transformation of the US Army, profoundly impacting its military culture and approach to war. The Army moved from attritional strategies towards a maneuverist approach and prioritised technological superiority (*e.g.*, the Air-Land Battle doctrine). Moreover, during the 1970s there was a transition to professionalisation and volunteer force, shaping a new cultural military identity. This major shift impacted recruitment and training towards a career-oriented culture, ultimately affecting their operational planning (Farrell & Terriff, 2001).

The first example illustrates how doctrine's background translates into Canada's current understanding of military warfare, whereas the US's case showcases the possibility of doctrinal shifts and their practical effects in the conduct of war. Consequently, these examples highlight the need to study cultural differences to achieve cohesion to delineate common objectives. Without suggesting cultural homogenisation, it is crucial to recognise these differences and formulate doctrines based on sources to which different armies can resort during doctrine instillation, rather than basing doctrine on a single experience or cultural context. Currently, NATO's MDO risks being generic as it seems to be based on one national experience (US), urging an analysis of how they can be or are currently integrated into the *rationale* of the different national doctrines within NATO. The answer to this question can be provided once the disparities in terms of capabilities and technological advances have been analysed in the next chapters.

Challenges for Operational Adaptability

Operational complementarity and adaptability are key in the context of MDO for various reasons. First, interoperability must allow for effective coordination, communication and operation through complementary doctrinal adaptation. For example, "fires" in US doctrine means "integrating and delivering lethal and non-lethal fires to enable joint manoeuvre commanders to dominate their operational environment" (Derleth, 2015). Contrastingly, NATO Members trained with Soviet doctrine understand "fires" in an area or barrage role, including a "hide" location to protect their artillery assets, which makes the fires not readily available. Therefore, there is a difference in the availability of fires. In the US they are available in 3 to 5 minutes, while in NATO they can take up to 25 minutes (Derleth, 2015). This is an example of how different doctrinal concepts can affect interoperability and combat effectiveness. Second, it offers flexible tactics to meet new regional and global challenges that could not have been foreseen through national doctrines alone, which is relevant for continuous innovation and capacity building (Karber, 2008). NATO as an alliance needs to consider all 'flanks', and be adaptable to the needs of its members, who are specialised in certain types of conflicts according to their geopolitical configuration. The wide variety of specialisations and expertise can serve as an asset for alliance development and preparedness for different types of conflict.

Third, it helps to optimise resources efficiently, avoiding duplication and fostering resource-sharinand knowledge exchange (Barry, 1996), allowing NATO to optimise the alliance's power and effectiveness. Fourth, operational adaptability is necessary for the fast deployment of forces, as adapting to different doctrines and MDO procedures would enhance the armed forces' readiness to operate jointly. This is essential to achieve compatibility in logistical support and addressing various types of security challenges. For instance, NATO could draw upon its Combined Joint Tasks Force initiative and organise exercises with various operational theatres to enhance force deployment (Barry, 1996). Fifth, through operation adaptability, NATO can achieve strategic coherence within MDO as it gives purpose and sets clear objectives.

Doctrinal and cultural differences currently undermine the integration of MDO into national doctrines. Unless they reformulate them, they will present challenges for:

1. Communication stemming from differing command and control systems (see Chapter 4).
2. Command and control due to a lack of decision-making agreement and command hierarchies (see Chapter 4).
3. Standardisation of technological equipment affecting logistical and operational coordination.
4. Confusing rules of engagement vary among States, as the know-how to engage in combat requires more than just a set of instructions.
5. Linguistic and cultural differences that decrease levels of active communication and oppose a common operational language. While NATO has an established common language (English or French), it is necessary to address the linguistic differences that inevitably add pre-established meanings to words. For instance, a bilingual Swedish soldier may understand NATO's common languages, but his linguistic understanding of Swedish concepts may affect the meaning he gives to the English word. Therefore, there is a need for a common understanding that embraces linguistic multiculturalism rather than homogenization of the operational language.

The question of how to overcome these challenges will be the prelude to a realistic reformulation of the MDO doctrine. Considering doctrinal and cultural differences will help turn MDO into a practical combat tool.

Conclusion

Current challenges to adaptability come from different doctrines and cultures, with the primary problem being that MDO appears to be an intellectual response to doctrinal issues. Problems arise from national differences and inherent challenges that doctrine has as a tool for understanding war today. While doctrine alone is not enough (Johnston, 2000), and should not be the only mechanism for interpreting the challenges of war (Palazzo, 2008), it requires qualities in the officer corps and the ability to think holistically (Sloan, 2012), time to develop and extensive sponsoring (Høiback, 2011; Kastos, 2021). If one chooses to formulate doctrine, it is necessary to consider that doctrine takes time to develop and requires practical experience to improve it. Consequently, the alliance must change its perspective in analysing the differences between NATO Members, considering these differences as opportunities for innovation and to cover all operational flanks of the alliance. This approach would make MDO more extensive and holistic in meeting global challenges, and most importantly, Member States must agree on what doctrine is and what it is for.

Recommendations

The following general recommendations offer guidance to NATO's MDO producers on national doctrinal and cultural differences to ensure operational adaptability and to improve MDO's practicality.

A. Develop Solid Doctrinal Foundations

1. To overcome doctrinal challenges, Member States should promote exercises of doctrinal cohesion to standardise objectives. Before developing MDO's doctrine, States must decide if the doctrine is to be used as a tool of education, command or change. While doctrine can function in all three dimensions, the balance between authority, culture and theory should ideally lean towards one dominant purpose.
2. To avoid generic doctrine, MDO producers should analyse the origins of national doctrines. Understanding these roots will provide useful references to bring purpose and transform MDO into a relevant doctrine for the armed forces.

B. Convert Doctrinal Differences into Opportunities for Innovation

3. To understand the extent to which NATO's doctrine is embedded in national doctrines, an in-depth analysis on national doctrines must be undertaken. NATO could organise annual Working Group meetings with military experts, space and technological practitioners, and governmental officials. This would serve as a preamble to move to a regionally-oriented framework, reach a consensus to develop a new institutional mechanism that sets achievable goals, and realistic objectives that consider each nation's capabilities and delineate how the MDO would also play a role in national priorities, making the latter encourage meaningful sponsorship. The meetings could start with sessions including only NATO Member States to set objectives and converge national priorities. Following these meetings, including military and technological experts in the discussions, could serve as technical assistance and bring practicality to the alliance's objectives. The meetings' expected outcome could be a Working Plan on how to advance in the continuous implementation of MDO.

4. Boost innovation through an online platform for networking among practitioners within the military, technological and space industry to share knowledge, ask questions, and engage in one-to-one learning experiences. This can be achieved through a methodology like that of DIANA, an organisation set up by NATO to accelerate dual-use innovation capability across the alliance. DIANA has a platform that comprises a network of more than 200 affiliated accelerator and test centres (DIANA, n.d.)

5. Strengthen national capabilities based on geographical and contextual priorities to reinforce NATO's flanks and avoid efforts on homogenising doctrines, instead focusing on complement doctrines.

6. Foster doctrine compatibility and adaptability by implementing an evaluation system of continuous improvement. Create criteria to track development in capabilities and MDO internalisation.

C. Tackle Resistance to Change Through Cultural Acknowledgment

7. Assess cultural differences to standardise the understanding of MDO's basic concepts.

8. To overcome linguistic barriers, NATO should promote cultural exchanges not only to immerse military personnel in fellow Members' contexts but to achieve language diversification. This will enhance communication and interoperability within missions.

9. To achieve coherence within MDO, the need exists to develop multicultural training that prepares armed forces to be flexible and knowledgeable about different military equipment, tactics and operational rationales. One example that illustrates these types of exercises, is the MDO Warfighter Exercise 19-04. The exercise included the III Corps (US) as a training audience, the 3rd Division (UK) as a partner division and fully committed training audience, and the 3rd Cavalry Regiment (US) as a reconnaissance and corps security force (Taylor & Kay, 2019).

10. Create logistical systems to support multinational operations by designing realistic scenarios in training exercises, which would help armed forces learn and adapt to unusual scenarios and familiarise themselves with the practicality of MDO concepts. MDO Warfighter Exercise 19-04 serves as an illustration of operational planning, where the 1st Infantry Division employed operational frameworks as a cognitive tool to display the application of combat power in time, space and purpose. Thus, the 1st Infantry ensured that the actions of brigade teams were conducted logically rather than being a series of unrelated actions. Besides, they ensure that the operational actions fulfilled the commander's end State. All plans must incorporate a "theory of victory" to develop a coherent plan in time, space and purpose (Taylor & Kay, 2019).

Institutional Coordination

Introduction

This chapter addressed the major challenges NATO must overcome when implementing Multi-Domain Operations.Although the execution of MDOs a top strategic priority for NATO, significant shortcomings remain. These include the absence of a coordinating authority to oversee and enforce MDO concepts, as well as a lack of standardised nomenclature, leading different States to interpret and apply MDO concepts differently. Additionally, the absence of a centralised structure for doctrine development results in disjointed implementation efforts. These challenges undermine NATO's effectiveness and interoperability, manifesting themselves in ways such as piecemeal efforts employed by the Allied Command to implement MDO procedures among Member States. This chapter explores these issues and provides recommendations for enhancing coordination, standardisation, and alignment within the Alliance.

NATO's Absent Coordinating Role

The execution of an entirely integrated and effective MDO plan is hindered by the absence of a coordinating authority tasked with monitoring and implementing such plans. For example, while NATO's Allied Command Transformation (ACT) recognises MDO as a strategic priority and has initiated efforts such as the MDO Implementation Team to support operationalisation through war gaming and training, these efforts are inconsistently adopted among Member States (NATO, 2023c). However, not all NATO Member States have routinely implemented or executed them. This inconsistent application of MDO procedures and concepts limits the Alliance's overall effectiveness in implementing MDO.

NATO has released strategic documents including the Alliance Concept for Multi-Domain Operations, which offer a long-term perspective on integrated military operations across all domains (Kramer, Dailey & Brodfuehrer, 2024). Nevertheless, it lacks legally binding mechanisms to ensure uniform adoption and execution among all participating States. Consequently, Member States adopt varied approaches to MDOs based on their capabilities and priorities, leading to a disjointed system rather than a cohesive plan.

Furthermore, operational challenges are based on the differences in the application of MDO techniques among NATO Members. One leading example is the outstanding achievement of the United States Combined Joint All-Domain Command and Control (US CJADC2) plan, which brought together very sophisticated technologies and tactical concepts for the advancement of MDO capabilities (Kramer, Dailey & Brodfuehrer, 2024). Nonetheless, not all Member States are as clear-eyed in their vision of strategic aim or possess the technological capabilities to conduct these exercises (Ellison & Sweijs, 2024).

Part of the reason for this is that NATO has no single coordinating body that can guide consistent implementation and use of MDO. While there have been loose and independent attempts without a centralised body to direct them, MDO capabilities are still not effectively integrated among Member countries of the Alliance. The absence of a strong coordinating function within NATO significantly hampers the effective execution of MDO. For that reason, a centralised command authority needs to be put in place with the mandate to enforce uniformity of standards, enable coordinated efforts, and ensure compliance with MDO policies and practices among all Member States.

Member State Interpretations and Implementation of MDO Concepts

The understanding and practical application of MDO concepts vary significantly among NATO Members, leading to several challenges. Primarily, NATO Members develop and utilise MDO systems in diverse ways. For instance, the proactive approach of the United Kingdom involves creating broad frameworks that integrate MDO capabilities into operational and strategic planning, resulting in increased preparedness and capability development (Kramer, Dailey & Brodfuehrer, 2024). Contrastingly, countries such as Canada primarily focus on military exercises to integrate MDO approaches, resulting in different levels of preparedness across the Alliance (Government of Canada, 2023).

Secondly, Member States exhibit considerable disparities in their application of MDO concepts. For example, France has actively engaged in numerous exercises of the MDO capabilities into its military operations, such the Orion exercise, a multiphase drill culminating in the synchronous operation of capabilities such as tactical vehicles, unmanned aerial systems, and spaceborne sensors in response to a scenario simulating multidomain conflict in the future battlespace (Machi, 2023). Other Member States have not contributed to the same degree or scope, leading to uneven integration in operational effectiveness. This non-homogenisation is a weakness in NATO's collective MDO capabilities because it prevents the Alliance from achieving a unified level of readiness and capacity among its Members. Consequently, these discrepancies undermine NATO’s ability to conduct seamless, coordinated operations across various domains, impacting its overall effectiveness.

Another significant issue is the lack of standardised nomenclature and set of standards for MDO within NATO Member States, resulting in countries using different terminologies to describe their multidomain doctrine (Ellison & Sweijs, 2024). While the US Army refers to its strategy as Multidomain Operations, the US Department of Defense calls it Joint All-Domain Operations (JADO), and the Canadian Armed Forces label their approach as Pan-Domain operations. As NATO’s nomenclature has not been standardised, different ideas and practices can be forwarded by the Member States, making it difficult to train, organise, and operate jointly with diverse doctrine’s definitions that may clash with each other.

Lack of a Centralised Doctrine and Divergent Priorities

The challenges of coordinating and integrating MDOs are further compounded by the absence of a central framework guiding doctrine development within NATO. Currently, the Alliance's current structure allows their Member States to develop doctrines independently from each other since there is no central authority leading and coordinating doctrine development. This situation results in a wide array of national variations in operational methods, practices, and standards. Consequently, these differences often impede interoperability, making it difficult for NATO forces to cooperate effectively during joint operations (Kramer, Dailey & Brodfuehrer, 2024). Operational protocols developed in one nation may not work in another country or otherwise exhibit less efficiency and cause operational problems in international operations.

Rather than following a unified, alliance-wide plan, individual Member States usually influence MDO development within NATO through their experimentation and capability development processes. Although promising, initiatives such as the Latvian Ministry of Defence's joint operational experimentation project with NATO ACT (Gosselin-Malo, 2023) remain largely discrete and have not been applied uniformly across the alliance. Moreover, the lack of a coherent doctrine creates a clear disjunction between strategic and tactical approaches to MDO, which could result in inconsistent operational planning and execution as countries are more inclined to certain elements of MDO based on their independent perceptions of threats and military capabilities. This lack of alignment undermines the readiness and capacity of the alliance to effectively counter emerging threats, significantly impeding coordination across all sectors. For instance, a country whose doctrine gives priority to cyber operations will not share the same perspective with one that prioritises land and sea operations, leading to coordination problems that would result in less effective combined operations (Kramer, Dailey & Brodfuehrer, 2024). Altogether, the core problem in implementing a common and effective strategy for MDO within NATO is that it does not have a centralised structure for the development of doctrine.

Recommendations

A.Establishment of a coordinated authority to monitor and implement the efforts towards MDO: this role could be performed by the NATO Standardisation Office (NSO), already responsible for the development and maintenance of standards throughout NATO, making it the ideal entity to guarantee consistency in standards and the MDO's implementation. The NSO could form specialized Standardization Working Groups (SWGs) focused on MDO, including experts from member states, and conduct regular meetings to discuss, review, and update these standards.

B.NATO should work towards an all-encompassing alliance framework that would establish harmony in MDO definitions, concepts and practices: this would require the development and dissemination of clear guidelines aiming to reduce disparities and improve interoperability. NATO could incorporate these guidelines into current training programs and joint exercises to ensure consistent implementation. To make it easier for Member States to comply, NATO could provide additional support services and advisory teams to help overcome any obstacles in implementing the guidelines.

C.NATO should encourage alignment of strategies and tactics among its Member States: This can be achieved by incorporating the NATO Defence Planning Process with national defence strategies, ensuring the countries' best possible contribution to achieve the collective security objectives set by the Alliance. NATO must hold thorough discussions with member states to understand their national defense priorities and limitations, where Member States should work together to find shared objectives and alignment opportunities. NATO could provide specific instructions and structures for member states to synchronize their national defense strategies with NATO's goals.

D.NATO should invest more in joint training and exercises focused on MDO doctrine: This would facilitate MDO forces of different countries towards a common understanding and application. These initiatives would improve coordination, interoperability and the overall effectiveness and readiness of NATO's multi-domain capabilities. For example, the drills would involve both extensive operations and specialized exercises, using virtual training environments for continuous practice.

Technological Capabilities

Introduction

To successfully conduct Multi-Domain Operations, NATO recognises the critical role of technology, and the need for a digital transformation to enhance its technological capabilities as NATO's current technological capacity poses a barrier to fully implementing MDO (NATO Allied Command Transformation, 2023a, 2023b). The digitisation of defence operations involves executing high-resolution, synchronised digital dashboards and databases that include secure, accurate, real-time data. These advancements aim to achieve real-time situational awareness across NATO's organisations and forces, thereby improving decision-making, operational effectiveness, and efficiency in subsequent military operations (Soare, 2023). For example, NATO has launched several initiatives to foster innovation, including the Data Exploitation Framework Policy to maximise NATO-generated data to achieve information superiority and data-driven decision-making at all levels within the Alliance (NATO, 2021b). Additionally, the Data Exploitation Framework Strategic Plan was also introduced to enhance open-architecture data systems and incorporate Artificial Intelligence into NATO's capabilities (Kudzko & Macko, 2023).

NATO's Defence Planning Process plays a critical role in promoting interoperability and the harmonisation of capabilities within the Alliance (NATO, 2022c). Within this framework, there are six primary components of NATO's digital transformation aimed to enable MDO: gathering data, planning operational effects, integrating risk management and digital mission assurance, implementing new capabilities, strengthening security and protecting personal data, and utilising synthetic environments to improve situational awareness (NATO, 2023). This chapter provides an overview of NATO's main challenges and the critical aspects it faces regarding technological disparities and the enabling of its digital backbone.

The first section outlines the heterogeneity of NATO Members' armed forces and systems that impact communications and integration within the alliance. The second one analyses the disparities between the US and the EU, as well as between EU States in the space and cyber domains. The third section addresses the wide budget discrepancies in defence spending, while the fourth focuses on the consequent technology gap between different allies. The fifth one addresses the challenges in information and data sharing highlighting the political barriers and material capabilities of NATO. The last section outlines the strict timelines of MDO and of the digital transformation that move alongside, even if the implementation of the second one is a critical enabler of the first.

Heterogeneity

The primary problem that NATO faces is the heterogeneity of its armed forces and systems, which entails thirty-two unique military structures and technologies that need to swiftly integrate. Utilising distinct typologies of the same equipment often results in less-than-ideal results because of varied maintenance requirements, different or unique components, and incompatibility with other weapons systems on the battlefield. Compatibility issues are exacerbated by the existence of obsolete Soviet-era equipment (Kudzko & Macko, 2023). These problems arise from the co-presence of dissimilar equipment standards and communication protocols, especially when comparing more sophisticated fifth-generation systems such as the F-35 that uses MADL with older fourth-generation fighters that operate using Link 16 (Richardson, 2019).

The F-35's advanced sensor suite, which includes AESA radar, DAS, and EOTS, generates plenty of data that needs to be processed and combined to build a comprehensive tactical picture. However, the integrated systems and processing capacity required to properly utilise or analyse this data without requiring a significant amount of manual labour are absent from fourth-generation aircraft (Richardson, 2019). Technological discrepancies among allies aggravate this problem, as many varying battle tracking systems with different technical standards are not interoperable (Kudzko & Macko, 2023). Their lack of compatibility hinders the operation's success since the Member States cannot access a unified and clear operational picture. Furthermore, the amount of data that needs to be processed is increasing quickly. For instance, a drone operated by the US Air Force may generate 70 terabytes of data in just 14 hours; for comparison, this is approximately seven times more than the Hubble Space Telescope's yearly data output (Catanzano *et al.*, 2023).

Space and Cyber

The profound technological disparities that challenge interoperability and the successful execution of MDOs are particularly relevant in the operational domains of space and cyberspace. Both domains possess intrinsic characteristics that prevent their simple incorporation into existing joint doctrine since many capabilities are not owned by militaries (Reynolds, 2022). Furthermore, in these domains, Member States' capabilities adopt profoundly different positions. For instance, in the space sector NATO completely relies on its Members for the delivery of space data and while the US has 71 owned and operated military spacecrafts, all the other Members combined have only 30 (Fasola *et al*. , 2024).

NATO Members such as the US, UK and Spain have cyber defence strategies that differ from one another. While the UK uses the National Cyber Force for offence in addition to GCHQ's (Government Communications Headquarters) defence, the US uses the CyberCommand for both offensive and defensive activities (Marrone *et al*., 2021).

While Germany's CIR (Cyber and Information Domain Service) safeguards national ICT under strict constitutional regulations, Spain's MCCE (The Joint Cyberspace Command) prioritises public-private collaboration for resilience, and France's ANSSI (National Agency for Information System Security) manages defence with military support for offence (Marrone *et al*., 2021). These variations highlight the obstacles confronted by NATO's Member States in coordinating cohesive cyber security strategies. These differences and their complexities may complicate the ability to confront cross-border incidents and share intelligence on hypothetical threats at the national level, let alone across Europe and NATO (Smit, *et al*., 2022).

Budget discrepancies

In the creation of a digital backbone for MDOs, not all the allies have access to the same funding, technological capacity and military infrastructure to enable rapid defence innovation, let alone the adoption of emerging technologies (Soare, 2021). While Member States have increasingly increased their investments, The International Institute for Strategic Studies has gathered data that shows that just a fraction of Europe's national defence budgets are devoted to digital capabilities, which include cyber security and digital enterprise (Soare, 2023). As a driver for higher-level innovations, defence spending is crucial and compared to Europe, the US government allocates seven times the amount of money to defence R&D (Smit, et al., 2022). According to recent data from the European Defence Agency (EDA), in 2020, the EDA Members devoted only €2.5 billion (1.2% of their defence budget) to research and technology (Clapp, 2022). This occurred despite pledges made by EU Member States to strive for 2% under Permanent Structured Cooperation (PESCO). On the other hand, the US devotes at least $14 billion, or 2% of its defence budget, to Research and Innovation (R&I) (Clapp, 2022).

The budget's inconsistency does not only regard the differences between Europe and the US, leaders in technological advancements, but also among European States. For instance, the UK is the country that invests the most in digital capabilities with USD 5.3 billion in 2023, while Spain invests the least, with only 0.4% of its annual defence budget going to the development of digital capabilities (Soare, 2023). Furthermore, the value of the global Artificial Intelligence (AI) market, valued in 2023 at €130 billion, is expected to increase to € 1.9 trillion by 2030 and the US dominates the field. In 2023 the US were able to attract €62.5 billion in private investments, while the UK and EU combined only €9 billion (Madiega & Ilnicki, 2024), mostly because of bureaucracy and long security processes (Soare, 2023).

Widening the gap and capabilities

The significant disparities that exist between the US and the EU in the technological field have increased with time, hampering NATO's progress and making the EU become more dependent on the US (Bergmann *et al.*, 2021). For instance, despite having one of the most proficient and prepared militaries for combat and being the United Kingdom the leader in digital transformation, France during its counterterrorism operation in the Sahel depended on the US for air-refuelling flights and intelligence, surveillance, and reconnaissance flights (Bergmann *et al*., 2021).

In 2014, the US had already elaborated a strategy to leverage emerging technologies for military and security purposes. In contrast, EDTs in defence are still primarily a long-term consideration for many countries in Central and Eastern Europe (Soare, 2021). The 2022 US National Defence Strategy similarly highlights that artificial intelligence, quantum science, autonomy, biotechnology, and space technologies can transform warfighting. In many of these technologies development, the United States holds the higher ground with their technological advancements (Sayler, 2024). Conversely, most European States rely on physically fortified on-site and on-board data-storage infrastructure, either because they lack integrated digital defence-data-management systems or because they are still developing them. Many European States find it difficult to maintain and improve their digital systems on a regular basis; some have not updated or upgraded their most important information systems in over ten years due to security concerns (Soare, 2023).

Furthermore, this technological gap does not only refer to the two coasts of the transatlantic ocean, but it also applies to EU countries. For instance, there are only two European countries (France and the UK) that have implemented AI-specific defence plans on the model of the US. Similarly, only a few allies have started to move towards the implementation of strategies for a necessary digital transformation to conduct MDOs. For example, in 2021 the UK released its Digital Strategy for Defence which details its vision, its means and the method that will be followed to achieve a strong digital backbone for Information Advantage and Multi-Domain Integration (United Kingdom Ministry of Defence, 2021). Conversely, the military stocks of Visegrád4 nations are, on average, significantly older and less digitised than those in Western Europe and the amount of architecture changes necessary to integrate new technologies in their defence systems discourages their investment in new technologies (Soare, 2023). Furthermore, another significant problem of the widening technology gap is that not all organisations with resources and knowledge are willing to share them in joint innovation initiatives. For instance, the adoption of Emerging Defence Technologies (EDTs) by major allies such as the United States, France, the United Kingdom, and the Netherlands is mostly centred on national strategies (Soare, 2021).

Information and data sharing

Effective MDO depends on a shared comprehension of the operational environment. This is grounded on a common knowledge of the situation and circumstances, which in turn depend on information sharing (Cannon, 2024). The process of information and data sharing is crucial to create a comprehensive and collaborative understanding that allows to successfully conduct of MDO that can produce combined effects across different operational domains. However, the process of sharing data and intelligence among NATO's 32 Members presents numerous considerable challenges.

NATO has taken some steps to mitigate these challenges and improve the data flow. For instance, the US used to share with NATO allies only 30 points of interest a month, while now shares 3000, and information-sharing regarding F-35 at WEPTAC has also significantly increased (Cannon, 2024). However, policy misalignment within NATO and EU countries keeps hampering the advancements of technological innovations and their adoption. As a case in point, the EU and the US do not have a common approach regarding privacy, and this prevents US major tech companies from fully contributing to European defence (Kudzko & Macko, 2023). Furthermore, the war between Ukraine and Russia has underlined NATO's need to enhance its ability to collect and process intelligence. While NATO owns all-weather sensors in its Synthetic Aperture Radar, Ground Movement Target Indicator (AGS), still lacks electrical-optical, infrared, full-motion video, or SIGINT competencies (Davis Jr., 2023).

Critical Impasse: Timelines and MDOs

To effectively conduct MDOs and navigate the evolving operational environment, NATO urgently requires a strong digital infrastructure. However, the current State of technology capabilities and digital transformation within NATO remains incomplete and insufficient. Recognising this gap, NATO initiated a modernisation process aimed at integrating its command, control, communication, computers, intelligence, surveillance and reconnaissance (C4ISR) architecture. Despite these efforts, challenges persist regarding the timelines for achieving these modernisation goals (Reynolds, 2022). For instance, some countries like Germany anticipate their digitalization initiatives to be completed by 2030, while other countries like Norway expect to take at least a decade to accomplish the transformation (Soare, 2023a).

By 2030, NATO plans to achieve digital transformation, allowing the Alliance to perform MDO and would guarantee cross-domain interoperability, improving situational awareness, and advancing political consultation and data-driven decision-making (NATO, 2023). However, given the current circumstances, it is unlikely that the planned milestones for this modernisation process will be entirely completed within the envisioned timelines, especially considering that many EU projects extend their timelines up to 2035 (Soare, 2023).

It is crucial to note that proponents of MDO emphasise the urgency of adopting a joint operational culture within NATO, like the lengthy process required to establish a unified joint culture among alliance Members in the past (Reynolds, 2022). The project of modernisation, digitalisation and adoption of new technologies undertaken by NATO to conduct MDOs is ambitious and will likely bring high results in the long term, if rightly funded and addressed. However, while NATO acknowledges these challenges and undertakes initiatives to mitigate them, significant technological disparities, particularly between the US and Eastern Europe, are unlikely to be resolved in the short term.

Recommendations

A. Interoperability and Standardisation: to successfully conduct MDO, NATO needs to take a more proactive stance, elaborating and establishing standardised communication procedures and technologies to ensure interoperability. It is important to focus on:

1. Unifying C4ISR Criteria: accelerate the creation of shared standards for C4ISR systems to facilitate data and information sharing,

2. Evaluation, support and implementation: frequently conduct interoperability assessments and checks, aiding other allies to integrate the standards into their processes aimed at the development of technological capabilities. In fact, while NATO enforces the application of standards or profiles for command-funded systems thought planning, implementation and testing phrases, there is no overarching alliance architecture, and each standard is linked to specific elements of the C3 taxonomy. Furthermore, the Defense Planning Capability Survey (DPCS) which collects information on national capabilities and inputs on C3 related capabilities, is often affected by practical constrains like time and money. It is necessary to establish an alliance architecture that integrates the different elements and guides and ensures the implementation of interoperable systems. Furthermore, practical constraints of DPCS need to be addressed, prioritizing critical requirements and developing more quick and effective strategies for implementation.

B. Prioritisation of Digital Transition and Implementation of EDT: NATO's objective to remain competitive, technologically advanced and operationally efficient requires prioritising the research and the adoption of new technologies. Indeed, although adopting AI is currently rising, it is still uneven and dispersed within the alliance. It is important to focus on:

3. Unified regulation: accelerate the process of adoption and revision of AI and data sharing laws, to establish clear ethical principles and uniform standards throughout the alliance and encourage and foster the harmonization of different legal frameworks. For instance, organizations such as the Hybrid CoE work to strengthen resilience against hybrid threats also through EU and NATO joint exercises. Its model entails sharing best practices, providing recommendations, strategic concepts and delivering support to implement them.

4. Research and technology collaborations: To mitigate the technological gaps and further proceed with the adoption and implementation of EDTs it is necessary to strengthen the cooperation with academia and businesses. For instance, in 2021, the Member States agreed to launch the Defence Innovation Accelerator for the North Atlantic (DIANA) which fosters interoperability and collaboration on critical technologies, and promoting innovation (NATO, 2024a).

C. Tackle Budget Differences: the different levels of investments within the alliance need to be addressed to guarantee interoperability and level the existent technological gap that could be exacerbated by the digital transformation and the emergence of newer technologies. It is important to focus on:

5. Resource Pooling: this would allow Members to access technologies and capabilities that could not otherwise afford, partially overcoming the gap with Eastern Europe.

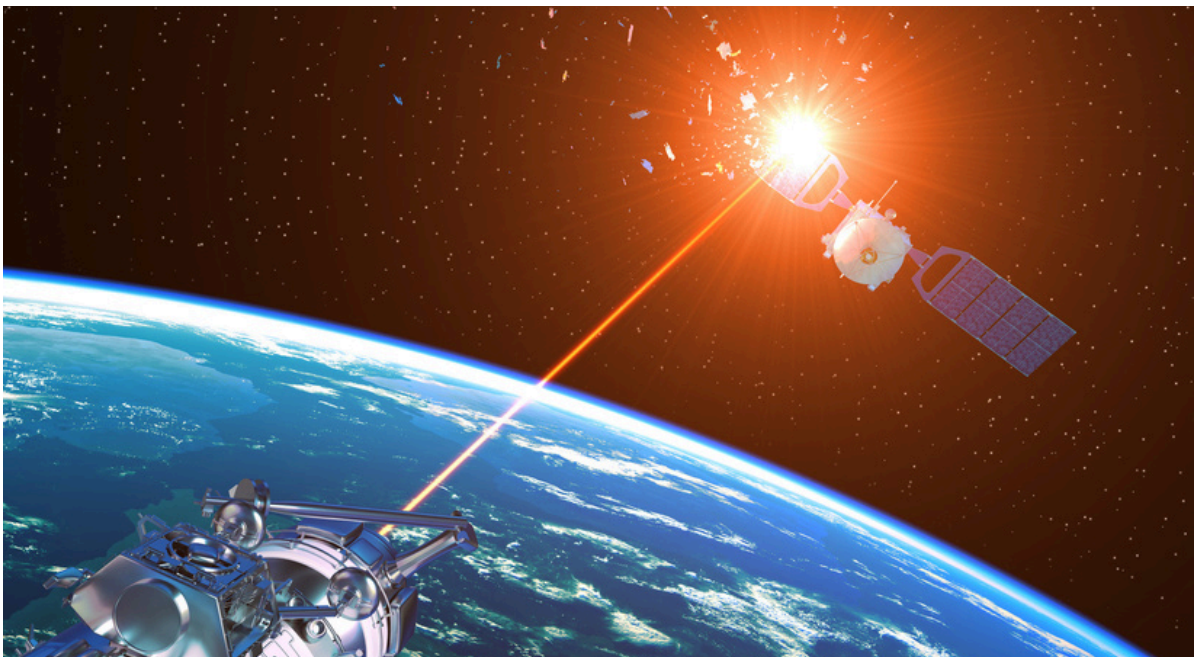
6. Support projects: the creation of financial support projects would incentivise creating the opportunity for resource pooling.

7. Push for Increased Investment: NATO Member States' investment has remained down the 2% threshold, making necessary a more significant investment to improve the MDO capabilities.

D. Boosting data and information sharing: Convergence at the policy and regulation level is required. It is important to focus on:

8. Effective Unified Data Framework and Strategy: While the vision and the desired outcomes are clear regarding NATO's Data Exploitation Framework Policy and the Strategic Plan sets the basis to start working to achieve those goals, policy asymmetries are one of the two factors that keep hampering information, data and intelligence sharing. Furthermore, the Strategic Plan does not mention MDO, which requires integrating data regarding different domains, as well as data sovereignty and ownership, crucial in data exploitation and sharing. Additionally, adopting unified technological standards, like secure communication systems, would booster security and resilience against cyberattacks.

9. Equipment Modernisation: A second obstacle in information and data sharing is the security risk. As Member States do not possess the same cyber-capabilities, the fear of cyberattacks, mismanagement and leaks prevents data sharing. Members need to invest to update their technologies, moving towards secure and advanced technologies that allow secure storage and safe data transmissions, overcoming the trust issue. Furthermore, implementing joint training initiatives, simulating scenarios and possible responses in crisis situations, would further enhance coordination and readiness in responding to cyber threats.



MDO and Europe's Command and Control Structures

Introduction

MDO doctrine leverages capabilities in all five domains, following the three tenets of calibrated force posture, multi-domain formations, and convergence (US Army, 2018). A multi-domain military organisation, however, needs the appropriate Command and Control (C2) structure to integrate its forces and achieve the level of synergy between the different domain-specific capabilities that allows it to be more than the sum of its parts (US Army, 2022). Concerning C2, this chapter identifies two issues that European Armed Forces need to overcome to fully adopt the MDO doctrine.

First, the complexity of MDO necessitates the highest echelon structure, that is Corps and Field Army, to be fully operational. European Armies can deploy their forces at most at the division level, a C2 structure that cannot organise MDO and risks becoming overloaded when coordinating with the other domains (Watling & MacFarland, 2021). Second, there is no homogeneity in NATO for the Armed Forces branch division. While every country assigns each traditional domain to a different service (Army, Navy, and Air Force), there is no standard within NATO for the highest level of Command of the Cyber and Space domains, with a Space specific service present only in the US and in France, and a Cyber-branch only in Germany. This structural inhomogeneity may help explain the different importance given to the Cyber and Space domains and their less-than-optimal integration into Joint Forces. European States may overcome these issues only through a coordinated effort. Subsequently, cooperation, in this case, is not only an enabler or a force multiplier, but an urgent necessity.

The Corps Echelon

MDOs are necessary to effectively fight against near-peer adversaries that have developed stand-off A2-AD capabilities (US Army, 2018). As the AirLand Battle doctrine integrated air capabilities with land capabilities to strike enemy forces in depth (US Army, 2020), the MDO doctrine integrates capabilities from all five domains to defeat an enemy that employs short, intermediate and long-range fires to fix and divide friendly forces (US Army, 2022). MDO can achieve this objective through convergence, that is "the rapid and continuous integration of all domains across time, space and capabilities to overmatch the enemy" (US Army, 2018, p. iii). As the logic map in the Army Training and Doctrine Command pamphlet 525-3-1 summarises, convergence is to be attained at different echelons: from Division, Corps, Field Army, to Theatre Army (2018). While divisions are tasked with close combat, manoeuvre, and some cross-domain capabilities, it is up to the Corps echelon to fight and defeat intermediate and long-range fires, employ large amounts of joint fires, and leverage cyber capabilities at the tactical and operational levels.

Convergence at the Corps level is what enables convergence at the Division level. The reason for the relevance of the Corps in MDO doctrine is that Divisions lack the C2 capacity to fully operate effectively cross-domains (Watling & MacFarland, 2021). Tasked with close combat and manoeuvre, a Division HQ would be likely overwhelmed by the complexity of MDO. Moreover, as Watling and Lieutenant General MacFarland argue, a Corps' structure should integrate many enabling elements, including a signals brigade, an electronic warfare company, a cyber-capable company, an aviation brigade, an air defence brigade, an air support operations group, to name a few (2021). Thanks to its more complex structure, ability to integrate more elements, and the higher capacity of its HQ, the Corps is an essential echelon for MDO doctrine.

Operating at the Corps level is currently impossible for European Armies (Watling & MacFarland, 2021). Following the end of the Cold War, Europe was quick to collect the dividends of peace (Aries, Giegerich, & Lawrenson, 2023), which meant reducing military spending and abandoning conscription (Poutvaara & Wagener, 2011). As a result, many European NATO Members have underdeveloped military capabilities, especially in the land domain, which is relatively more demanding in terms of manpower than the air or the sea (Tuck, 2022). Moreover, many European States do not possess the demographic and economic resources to deploy enough land forces to justify a Corps structure. Therefore, most European Armies are currently structured around the Brigade echelon.

France, Germany, Greece, Italy, Poland, Romania, Spain, and the United Kingdom all employ the division structure, at least on paper (IISS, 2024). In some cases, no brigade units are assigned to the division's HQ (Esercito Italiano, 2024). European Divisions and Brigades on their own would likely be overwhelmed by the complexity of MDO (Watling & MacFarland, 2021). The Corps structure is present in Europe in the form of the NATO Corps HQ. Nevertheless, these HQs have no permanent division assigned to them, few or no of the enabling units that Watling and MacFarland believe necessary, and the only permanent units are at the regiments and brigades' level with tasks such as intelligence, signals, support or Military Police (Watling & MacFarland, 2021; IISS, 2024). NATO Corps are not combat-ready units which, in the eventuality of a conflict, would be able to respond to threats to European territory. Insufficient on their own and not effectively coordinated, European Land Forces cannot operate in a crisis at the Corps level, and therefore their practical application of MDO doctrine is at least questionable. Deeper cooperation is an essential requirement for European States to deploy and organise forces at the Corps echelon level.

Europe must look for positive models to develop an MDO-capable fighting force. One such model is the US Army I Corps (US Army, 2024). Even though America's first Corps area of competence, the Indo-Pacific, is decisively different from the possible battlefields where European Land Forces might be engaged in the future, the analysis of this echelon's structure and philosophy is beneficial, since it can effectively run MDOs. Three divisions compose the I Corps, the 11th Airborne Division, the 25th Infantry Division, and the 7th Infantry Division. Beyond these three main combat units, the Corps comprise a large set of enabling assets: the 1st Multi-Domain Task Force, the 593rd Expeditionary Sustainment Command, the 17th Field Artillery Brigade, the 201st Expeditionary Military Intelligence Brigade, the

22nd Corps Signal Brigade, the 42nd Military Police Brigade, and the 555th Engineer Brigade (US Army, 2024). Thanks to an HQ with greater C2 capacity, the I Corps can simultaneously coordinate its combat and enabling units and assume control over the other US military branches and international partners operating in the region. The more capable structure allows the "Fighting Free" philosophy, in which the Corps HQ Divisions are responsible for the MDO tasks that would overwhelm the Divisions, thus enabling them to fight and manoeuvre agile (Brunson & Walsh, 2023). Finally, the more permanent structure of the I Corps means that military exercises are possible at this echelon level. This is the case, for example, of the Warfighter Exercise that took place in 2023 to test MDO doctrine and improve its practical adoption (Lumbard, 2022).

Domain division of competence

Since European States are unable on their own to deploy forces at the appropriate echelon level, cooperation and coordination are essential requirements for MDO. Nevertheless, there is no standardised structure for the highest level of organisation of the military branches within NATO. While every country assigns the traditional three domains to a different branch within its Armed Forces (Army for the Land, Navy for the Sea, Air Force for the Air), there is less coherence regarding Space and Cyber (IISS, 2024).

The US constituted its Space Force in 2019, right after the recognition by NATO of Space as an operational domain. Although still bonded with the Air Force, (the Space Force reports to the Department of the Air Force), the constitution of the Space Force as a separate branch recognises the importance of this domain for American security and operational readiness (Congressional Research Service, 2024; NATO, 2024a; Erickson, 2024). US Cyber Command was established in 2010 and although capable, from a C2 point of view it is not on the same level as the other branches of the US Armed Forces. Even though the Command was separated from the US Strategic Command in 2017, unlike the other domains, it is not a service of the US Armed Forces. As such, it collaborates with the Cyber-specialised units of each branch of the US Armed Forces. The Cyber Command is strictly linked to the National Security Agency (NSA), with the general at the head of the NSA wearing the dual hat of the commander of the Cyber Command (Warner, 2020). This force structure reflects the virtual nature of this domain, where threats do not follow geographic rules and therefore the Cyber Command is tasked with the defence of domestic as well as forward-deployed assets (US Cyber Command PAO, 2022). Thus, although US cyber capabilities are extensive (IISS, 2021), this domain is not on the same level as the other four from a force structure perspective. A recent report by the Foundation for Defense of Democracies underlines the issues with the current force structure and calls for the formation of the Cyber Force as a separate branch of the US Armed Forces (Lonergan & Montgomery, 2024).

Furthermore, European Armed Forces structures reveal a relative lack of relevance given to the two new domains, especially Space. Unlike the US, no European States have a dedicated branch for Space capabilities (IISS, 2024). The absence is explained by a complete lack of such capabilities from many States, which impacts the perception of threat in this domain, and humble capabilities from other States, which do not justify the creation of a separate branch. Countries with intermediate capabilities, like Italy and Germany, have formed Space Commands (Raju, 2024; Bataille, 2024). A partial exception is France, which possesses the greatest military assets in Space within Europe (Bataille, 2024). In 2020, France changed the name of its Air Force to Air and Space Force (*Armée de l'air et de l'espace*). This symbolic gesture reflects the growing engagement of the French Armed Forces with the Space domain, visible in Space-specific exercises and investments in the sector (Machi, 2022). The European States have instituted Cyber Commands in the last decade to develop their capabilities in this domain. In some cases, the Command is comprised within the Army, while in other structures it is a more independent element, following the American example (Marrone & Sabatino, 2021). Germany, instead, opted to form a separate military branch in 2024 for cyber capabilities C2, the Cyber and Information Domain Service (*Cyber- und Informationsraum*), upgrading the preexisting Command instituted in 2017 (Bundesministerium der Verteidigung, 2024). It is still too early to judge the success of this new military branch. Still, the unique force structure seems to promise the correct relevance to the Cyber domain and thus facilitate its integration within MDO doctrine.

Recommendations

1. **Form combat-ready European Corps:** regarding the inability to deploy forces beyond the division level, three Corps must be created with contributions from each European Member of the Alliance, tasked only with the defence of the European territory. Each Corps must have permanent units assigned to them. These three Corps would constitute the over 100,000 readily available forces (tier 1) that the new multilayered NATO Force Model requires (NATO, 29 June 2022). Furthermore, the three European Corps could be permanently integrated into a Field Army, a role that can be undertaken by one of the NATO Allied Joint Force Commands. The Field Army would be responsible for a higher degree of Multi Domain C2, following MDO doctrine (US Army, 2018) and it could integrate the American V Corps, recently redeployed to Europe (Klecan, 2021).
2. **Individuate the correct force structure among allies:** Regarding the inhomogeneity of the Armed Forces branches division between allies, NATO must carefully and collaboratively study the force structure that better valorises and integrates into MDO doctrine capabilities in the Cyber and Space domain. A standardised force structure might also simplify coordinated actions. Regarding the Cyber domain, Allies must decide whether the preferred structure should be the Command or an altogether separate branch. Regarding the Space domain, forms of cooperation such as the Command Space Operations Initiative, albeit more inclusive than now (Sacchi, 2024), might be preferred to each nation possessing a Space Force. This is due to the disparities in resources and the greater capabilities that can be achieved through cooperation.

Political Hurdles to Corps creation

Cooperation is the only way for European States to achieve the appropriate C2 required to adopt the MDO doctrine. Therefore, the main hurdles to overcome will be of political rather than technical nature. The recommendation to form three European Corps is ambitious but necessary to enact the changes that will enable MDO in the Old Continent. If the European States can find the political will to embark on such an endeavour, three main issues would still need to be addressed:

1. **The role of non-EU NATO Members:** even if the path would still be incredibly complicated, an EU-led initiative to form the Corps might facilitate the process, as the discussion surrounding the possibility of a European Army suggests (Weir, 2024; Andelman, 2022). The fact that the Corps would be used only for the Territorial Defence of the Members, a common objective among all States, might avoid frictions due to different foreign policies and the decision-making process in Brussels (Szewczyk, 2024). However, if NATO were to rely on the EU for the formation of these Corps, that would open the question of how to integrate into this structure non-EU NATO Members, especially capable and important allies such as Türkiye and the United Kingdom.
2. **The Command hierarchy must be chosen professionally and not politically:** top brass positions must not be decided based on nationality and their country's contribution to the European Corps, but rather on the professional merits of the individual. While it is understandable that States might not be willing to deploy their soldiers and capabilities under a commander of a different nation (Watling & MacFarland, 2021), such behaviour must be avoided for these new military units to be effective. At the same time, if positions of power are not to be decided politically, the selection method remains an open question.
3. **Multinational Corps:** different Armed Forces have different approaches to MDO and doctrine in general. If general homogeneity among allies cannot be easily achieved, still the multinational European Corps must share the same doctrine and fighting philosophy. This can be achieved through common exercises at the Corps level.

Conclusion

To achieve a C2 able to sustain MDO European States must cooperate. The current echelon structure employed, divisions and brigades, would be cognitively overwhelmed when trying to apply MDO doctrine on their own. Furthermore, they lack the enabling units required. Thus, Europe must find a way to deploy their forces at least at the Corps level. The only possible way is to combine their capabilities in multinational Corps units. Unlike current NATO corps, these European Corps must not be only C2 Headquarters which in time of crisis can coordinate units but have permanent Divisions and enabling units assigned to them. The continuous sharing of training and exercises will shape them into a formidable fighting force. Regarding the division of domain competence at the branch level, there is no consensus on best practices.NATO allies should collaboratively agree on the best structure for the Cyber and Space domain. Once the allies have decided on the best standard which will better integrate the capabilities in these new domains, they should adopt it as quickly as possible, thus enabling better intranational communication and coordination.

Key Findings

NATO's adoption of Multi-Domain Operations presents challenges for its Members in terms of capabilities and as an intellectual challenge for national land doctrines due to differing interpretations of what doctrine is for, an absence of clear definitions, and the practical applications to translate MDO into actionable doctrine. This paper delved into the challenges associated with the integration of MDO into national doctrines hindering interoperability and offered recommendations on how these problems can be addressed.

Operational Adaptability

- **MDO seems to be an intellectual response to doctrinal issues.**

Addressing doctrinal challenges requires understanding the intrinsic complexities of NATO's MDO and considering two preceding issues. First, NATO Member States must agree on the definition and purpose of the doctrine base, whether it serves as a tool of command, change or education (Høiback, 2011). Second, each nation interprets doctrine based on its unique historical context and establishes military objectives according to national priorities (Barry, 1996). Therefore, there is a need to overcome doctrinal differences among NATO's Member States to develop a successful NATO MDO doctrine. Adding to these challenges, cultural disparities play a key role in the level of integration of MDO within national doctrines (Eagleton, 2000). Adapting operations according to cultural differences within the alliance is crucial to ensure operational effectiveness from doctrine development to practical training. The level of integration of MDO within national doctrines depends on building doctrinal cohesion and standardising objectives across the alliance.

Institutional Coordination

- **NATO lacks coordination in implementing MDO**

Despite NATO's ACT recognising that MDO is one of the main strategic outcomes, there is still a lack of unified understanding and coordination among Member States. NATO requires a central authority to ensure consistency in standards and execution of MDO procedures. Furthermore, Member States have different interpretations and implementations of MDO concepts, resulting in disjointed efforts. This disparity is exacerbated by the absence of a centralised framework for doctrine development, which undermines interoperability and operational effectiveness. To overcome these challenges, NATO should create a comprehensive framework for MDO, aligning definitions and practices, incorporating defence planning into national strategies, and supporting joint training programs to boost Alliance interoperability and effectiveness.

Technological capabilities

- **MDO serves as a justification for developing a digital backbone**

NATO has recognised the digital and technological transformation needed to conduct MDO. However, at present Member States' technological capabilities are insufficient and require further homogenisation to enhance decision-making processes and operational effectiveness (Soare, 2023). The main challenges include heterogeneity, space and cyber disparities, budget discrepancies, technological gaps, information and data sharing barriers, and strict timelines to integrate MDO.

Despite NATO's efforts to counter technological disparities among Member States (Kudzko & Macko, 2023), capabilities still vary significantly among allies. Differing cyber defence strategies (Fasola *et al*., 2024) hinder coordination, and budget discrepancies (Soare, 2021) add to the challenges of developing a digital backbone necessary for operations at the level of MDO. For example, there is a significantly lower digital defence investment in Europe compared to the US (Smit, *et al*., 2022). The unbalanced dependence on technology and capabilities increases the technological gap and raises questions about the practicality of MDO within NATO. While information sharing is essential to face these challenges, divergent policies are impeding a seamless technological development. NATO has committed to a complete digital transformation by 2030 (Cannon, 2024), although meeting these deadlines seems unlikely due to the absence of a pre-existing digital backbone, adding to the apparent inconsistent timeframe with the MDO's implementation objectives.

MDO and Europe's Command and Control Structures

- **European-level cooperation is a necessity for a fully integrated MDO**

MDO requires an adequate C2 structure to integrate its forces and achieve the synergy needed between the different domain-specific capabilities (US Army, 2022). To effectively apply MDO to their national doctrines, European armed forces must overcome two main challenges: the need for an operational C2 structure at the Army Corps level (Watling & MacFarland, 2021) and the lack of homogeneity in the structure for the Cyber and Space domain at the branch level. Current structures of European armies are limited to divisions and brigades, hampering the application of MDO (Watling & MacFarland, 2021). Therefore, a deeper multinational cooperation will serve as a facilitator, and is a necessity to develop a capable Army Corps with permanent divisions and support units. European armies could reference the US Army I Corps, as an example that demonstrates the ability to coordinate MDO effectively through its structure and operational philosophy (US Army, 2024). Moreover, the European Armed Forces do not have a dedicated branch for Space capabilities (IISS, 2024), impacting the perception of threat in this domain. Likewise European forces have a dissimilar Cyber domain structure (Marrone & Sabatino, 2021). Thus, a standardised organisation of the Cyber and Space domains among NATO allies will improve coordination, intranational communication and operational effectiveness.

Summary of Recommendations

Operational Adaptability

A. Develop solid doctrinal foundations: Promote exercises of doctrinal cohesion to standardise objectives and determine how doctrine would be used.
B. Convert doctrinal differences into opportunities for innovation: Perform an in-depth analysis of national doctrines to shift to a regional-oriented framework and foster doctrine compatibility.
C. Tackle resistance to change through cultural acknowledgement: Evaluate cultural differences to standardise the meaning of MDO's basic concepts.

Institutional Coordination

A. Establish a coordinating authority: to monitor and implement the MDO concepts
B. Set and elaborate an all-encompassing alliance framework: to harmonise MDO definitions, concepts and practices.
C. Invest further in joint training and exercises.

Technological Capabilities

A. Interoperability and Standardisation: Establish standardised communication procedures and technologies.
B. Prioritisation of Digital Transition and implementation of EDT: Prioritise research and adaptation of new technologies.
C. Tackle budget differences: To guarantee interoperability and fill the technological gap there should be an agreement on the level of investments within the alliance.
D.Boost data and information sharing: This is required to have convergence at the policy and regulation level.

Command and Control Structures

A.Establishment of an integrated European Corps to enhance defence: To strengthen defence within Europe by promoting integration and coordination to achieve MDO.
B.Standardisation and Integration of Cyber and Space Capabilities: To improve effectiveness and coordination within MDO doctrine through collaborative decision-making.

Recognising that the recommendation to create three European Corps is ambitious, this paper presented the main obstacles to overcoming the policy challenges to achieving the appropriate C2 required by the MDO and how they can be addressed:

A. Comprehensive EU-NATO synergy strategy: An EU-led initiative to form the Corps could facilitate the process.
B. Professional Command Hierarchy Selection: The Command hierarchy must be chosen based on professional merits to avoid political influence in the selection process of positions within the European Corps.
C. Multinational Corps: Perform Common exercises at the Corps level to reach higher cohesion in doctrine and fighting philosophy understandings.

Bibliography

Andelman, D. (2022, March 23). *Putin just made the case for a European army.* CNN. https://edition.cnn.com/2022/03/23/opinions/european-army-defense-strategic-compass-putin-andelman/index.html.

Aries, H., Giegerich, B., & Lawrenson, T. (2023). The Guns of Europe: Defence-industrial Challenges in a Time of War. *Survival,* 65(3), 7–24. https://doi.org/10.1080/00396338.2023.2218716.

Barry, B., Boyd, H., Giegerich, B., Gjerstad, M., Hackett, J., Michel, Y., … & Tong, M. (2023). *The Future of NATO's European Land Forces: Plans, Challenges, Prospects.* International Institute for Strategic Studies. https://www.iiss.org/en/research-paper/2023/06/the-future-of-natos-european-land-forces/.

Barry, C. (1996). NATO's combined joint task forces in theory and practice. *Survival,* 38 (1), 81-97. https://doi.org/10.1080/00396339608442832.

Bataille, M. (2024). NATO and the Space Domain: Coordinating National Capabilities as a Pathway to Success? In Space: Exploring NATO's Final Frontier, NATO Allied Command Transformation, Università Di Bologna, *Istituto Affari Internazionali,* pp. 48-61. https://www.iai.it/sites/default/files/9781954445024.pdf.

Bergmann, M., Lamond, J., & Cicarelli, S. (2021, June 1). T*he Case for EU Defense a New Way Forward for Trans-Atlantic Security.* Center for American Progress. https://www.americanprogress.org/article/case-eu-defense/.

Bowe, A. (2019, April 11). *China's Pursuit of Space Power Status and Implications for the United States. US-China Economic and Security Review Commission.* https://www.uscc.gov/research/chinas-pursuit-space-power-status-and-implications-united-states.

Brunson, X. & Walsh, L. (2023). *How I Corps Fights: Pivoting to Meet Threats in the Indo-Pacific. Association of the United States Army.* https://www.ausa.org/articles/how-i-corps-fights-pivoting-meet-threats-indo-pacific.

Bundesministerium der Verteidigung. (2024). Bundeswehr der Zeitenwende: Kriegstüchtig sein, um abschrecken zu können [Bundeswehr of the turning point: Be ready for war in order to be able to deter]. https://www.bmvg.de/de/aktuelles/bundeswehr-der-zeitenwende-kriegstuechtig-sein-um-abzuschrecken-5765386.

Cannon, S. (2024). The Alliance's Transition to Multi-Domain Operations. *The Journal of The JAPCC*, 37. https://www.japcc.org/wp-content/uploads/JAPCC_J37_Art-02_screen.pdf.

Catanzano, K., Nappi, K., Vrielink, K., Keyal, A., & Mariani, J. (2023, September 12). From open source to everything as a source: *How militaries can use and protect themselves from information everywhere.* Deloitte. https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-warfighting-in-a-digital-age/military-data-security.html.

Clapp, S. (2022). *Emerging disruptive technologies in defence.* European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733647/EPRS_ATA(2022)733647_EN.pdf.

Clare, P. (2020, February 13). *The Answer is Multi Domain Operations – Now What's the Question?* WavellRoom. https://wavellroom.com/2020/02/13/the-answer-is-multi-domain-operations-now-whats-the-question/.

Congressional Research Service. (2024). Defense Primer: The United States Space Force. *Congressional Research Service.* https://crsreports.congress.gov/product/pdf/IF/IF12610/2.

Connable, B., Young, S., Pezard, S., Radin, A., Cohen, R., Migacheva, K., & Sladden, J. (2020). *Russia's Hostile Measures.* Rand Corporation. https://www.rand.org/pubs/research_reports/RR2539.html.

Davis Jr., G. (2023). *THE FUTURE OF NATO C4ISR - Assessment and Recommendations After Madrid.* Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-future-of-nato-c4isr-assessment-and-recommendations-after-madrid/.

Derleth, J. (2015). *Enhancing interoperability: the foundation for effective NATO operations.* NATO Review. NATO. https://www.nato.int/docu/review/articles/2015/06/16/enhancing-interoperability-the-foundation-for-effective-nato-operations/index.html.

DIANA. (n.d.). *Defence Innovation Accelerator for the North Atlantic*. https://www.diana.nato.int/index.html.

Diaz de Leon, Lieutenant Colonel J. (2021). Understanding Multi-Domain Operations in NATO. The Three Swords Magazine, 37, pp. 1-4. https://www.jwc.nato.int/download_file/view/1661/277.

Eagleton, T. (2000). *The Idea of Culture.* Blackwell Publishers, pp. 7-34; 52-67. https://edisciplinas.usp.br/pluginfile.php/4929921/mod_resource/content/1/Terry%20Eagleton-The%20Idea%20of%20Culture-Wiley-Blackwell%20%282000%29.pdf.

Ellison, D., & Sweijs, T. (2024, January 22). *Empty promises: A year inside the world of multi-domain operations.* War on the Rocks. https://warontherocks.com/2024/01/empty-promises-a-year-inside-the-world-of-multi-domain-operations/.

English, A. D. (2004). Understanding Military Culture: A Canadian Perspective. *McGill-Queen's University Press.* http://www.jstor.org/stable/j.ctt80gt7.

Erickson, S. (2024). Existing International Governance, Current Multilateral Efforts and Contemporary Space Security Developments and Trends. In Space: Exploring NATO's Final Frontier, Nato Allied Command Transformation. *Istituto Affari Internazionali,* pp. 14-27. https://www.iai.it/sites/default/files/9781954445024.pdf.

Esercito Italiano. (2024). Divisione "Vittorio Veneto" [Vittorio Veneto Division]. https://www.esercito.difesa.it/organiszazione/capo-di-sme/COMFOTER/Divisione-Vittorio-Veneto/Pagine/default.aspx.

Farrell, T., & Terriff, T. (2002). *The sources of military change: Culture, politics, technology.* Lynne Rienner Publishers. https://www.rienner.com/title/The_Sources_of_Military_Change_Culture_Politics_Technology

Gosselin-Malo, E. (2023, August 31). NATO to Test 5G Capabilities in Latvia with Virtual Reality, Drones. *Defense News.* https://www.defensenews.com/ global/europe/2023/08/31/nato-to-test-5g-capabilities-in-latvia-with-virtual-reality-drones.

Government of Canada. (August 10, 2023). *Joint Experimentation at the Canadian Joint Warfare Centre. Government of Canada.* https://www.canada.ca/en/department-nationaldefence/maple-leaf/defence/2023/08/joint-experimentation-canadian-joint-warfare-centre.html.

Høiback, H. (2011). What is Doctrine? *Journal of Strategic Studies,* 34(6), 879-900. https://www.tandfonline.com/doi/abs/10.1080/01402390.2011.561104.

International Institute for Strategic Studies. (2024). The Military Balance 2024 (1 ed.). Routledge.

Johnston, P. (2000). Doctrine is not enough: The effect of doctrine on the behaviour of armies. *Parameters,* 30(3). https://doi.org/10.55540/0031-1723.1991.

Jones, S. (2022). *Russia's Ill-Fated Invasion of Ukraine - Lessons in Modern Warfare.* Center for Strategic and International Studies. https://www.csis.org/analysis/russias-ill-fated-invasion-ukraine-lessons-modern-warfare.

Karber, P.A. (1986). NATO doctrine and national operational priorities: The central front and the flanks: Par 1. *The Adelphi Papers*, 26 (207), 12-33. https://doi.org/10.1080/05679328608448728.

Kastos, G.E. (2021). U.S. Joint Doctrine Development and Influence on NATO. *National Defense University Press.* https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2556880/us-joint-doctrine-development-and-influence-on-nato/.

Klecan, D. (2021). Victory in Europe: V Corps reaches major milestone. US Army. https://www.army.mil/article/251719/victory_in_europe_v_corps_reaches_major_milestone.

Kramer, F. D., Dailey, A. M., & Brodfuehrer, J. A. (2024). *NATO multidomain operations: Near- and medium-term priority initiatives.* Atlantic Council. https://www.act.nato.int/article/mdo-in-nato-explained/.

Kudzko, A., & Macko, P. (2023). *The future of digital deterrence in Central and Eastern Europe*. GLOBSEC. https://www.globsec.org/what-we-do/publications/future-digital-deterrence-central-and-eastern-europe.

Lonergan, E. & Montgomery, M. (2024). *United States Cyber Force: A Defense Imperative*. Foundation for Defense of Democracies, Washington, DC. https://www.fdd.org/wp-content/uploads/2024/03/fdd-report-united-states-cyber-force.pdf.

Lumbard, T. (2022). *I Corps tests distributed mission command concepts in the Indo-Pacific.* US Army. https://www.army.mil/article/254414/i_corps_tests_distributed_mission_command_concept_in_indo_pacific.

Machi, V. (2022, March 14). *France puts space at top of national — and European — security priorities*. Defense News. https://www.defensenews.com/space/2022/03/14/france-puts-space-at-top-of-national-and-european-security-priorities/

Machi, V. (April 14, 2023). *French Forces Prep for Final Phase of Major Multidomain Exercise.* Defense News. https://www.defensenews.com/global/europe/2023/04/14/french-forces-prep-for-final-phase-of-major-multi-domain-exercise.

Madiega, T., & Ilnicki, R. (2024). *AI investment: EU and global indicators.* European Parliamentary Research Service.
https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/760392/EPRS_ATA(2024)760392_EN.pdf.

Marrone, A. & Sabatino, E. (2021). *Cyber Defence in NATO Countries: Comparing Models.* Istituto Affari Internazionali. https://www.iai.it/en/pubblicazioni/cyber-defence-nato-countries-comparing-models.

Marrone, A., Sabatino, E., & Credi, O. (2021). *Italy and Cyber Defence.* Istituto Affari Internazionali. https://www.iai.it/sites/default/files/iai2112_en.pdf.

United Kingdom Ministry of Defence. (2021, May 27). *Digital Strategy for Defence - Delivering the Digital Backbone and unleashing the power of Defence's data*. https://www.gov.uk/government/publications/digital-strategy-for-defence-delivering-the-digital-backbone-and-unleashing-the-power-of-defences-data.

NATO. (2021a). *NATO 2030 Factsheet.* NATO, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106-factsheet-nato2030-en.pdf.

NATO. (2021b). *Summary of NATO's Data Exploitation Framework Policy.* NATO. https://www.nato.int/cps/en/natohq/official_texts_210002.htm.

NATO. (2022a). Strategic Concept. NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

NATO. (2022b). Multi-Domain Operations: Enabling NATO to Out-pace and Out-think its Adversaries. NATO. https://www.act.nato.int/article/multi-domain-operations-enabling-nato-to-out-pace-and-out-think-its-adversaries/.

NATO. (2022c). *NATO Defence Planning Process.* Retrieved June 2024, from https://www.nato.int/cps/en/natohq/topics_49202.htm.

NATO. (2023a). Cyber defence. NATO. https://www.nato.int/cps/en/natohq/topics_78170.htm.

NATO. (2024a). *Emerging and disruptive technologies.* NATO. https://www.nato.int/cps/en/natohq/topics_184303.htm.

NATO. (2024b). *NATO's overarching Space Policy.* NATO, https://www.nato.int/cps/en/natohq/official_texts_190862.htm.

NATO Allied Command Transformation. (2023a). *ACT Leads a Digital Transformation Workshop.* NATO. https://www.act.nato.int/article/act-leads-a-digital-transformation-workshop/.

NATO Allied Command Transformation. (2023b). *Empowering NATO's Multi-Domain Operations Through Digital Transformation.* NATO. https://www.act.nato.int/article/empowering-nato-mdo-through-digital-transformation/.

NATO Allied Command Transformation. (2023c). *MDO in NATO explained.* NATO. https://www.act.nato.int/article/mdo-in-nato-explained/.

NATO Allied Command Transformation. (2023d). NATO Multi-Domain Operations Conference 09-11 October. NATO. https://www.act.nato.int/article/mdo-conference-2023-starts/.

NATO Allied Command Transformation. (2023e). *Ongoing Military Transformation, Leading to NATO 2030 – Multi-Domain Operations, Deterrence and Defence, Improved Understanding.* NATO. https://www.act.nato.int/article/ongoing-military-transformation-leading-to-nato-2030-multi-domain-operations-deterrence-and-defence-improved-understanding/.

Noetzel, T. and Schreer, B. (2009). Does a multi-tier NATO matter? The Atlantic alliance and the process of strategic change. *International Affairs,* 85 (2), 211-226. https://doi.org/10.1111/j.1468-2346.2009.00790.x.

Palazzo, A. (2008). *From Moltke to Bin Laden, The Relevance of Doctrine in the Contemporary Military Environment.* Australian Government, Department of Defence, Land Warfare Studies Centre. https://researchcentre.army.gov.au/sites/default/files/sp315_from_moltke_to_bin_laden-albert_palazzo.pdf.

Poutvaara, P. & Wagener, A. (2011). Ending Military Conscription. *CESifo DICE Report*, 09(2), pp. 36-43. https://www.econstor.eu/bitstream/10419/167036/1/ifo-dice-report-v09-y2011-i2-p36-43.pdf.

Raju, N. (2024). *Strengthening NATO's Deterrence and Defense Posture in Outer Space.* In Space: Exploring NATO's Final Frontier, NATO Allied Command Transformation, Università Di Bologna, Istituto Affari Internazionali, pp. 92-105. https://www.iai.it/en/pubblicazioni/space-exploring-nato-final-frontier.

Weir, K. (2024, January 7). Italian foreign minister calls for the formation of an EU army. Reuters. https://www.reuters.com/world/europe/italian-foreign-minister-calls-formation-eu-army-2024-01-07/.

Reynolds, J. (2022, December). Adapting Beyond Joint Doctrine. *The Three Swords*, 38, pp. 1-5. https://www.jwc.nato.int/application/files/3516/7092/4186/NATO_MultiDomainOperations2022DEC.pdf

Reynolds, J., & Lightfoot, J. (2020). *Digitalize the Enterprise.* Atlantic Council. https://www.atlanticcouncil.org/content-series/nato20-2020/digitalize-the-enterprise/.

Richardson, W. (2019). Leveraging capability: A study of the interoperability of fourth- and fifth-generation NATO fighter aircraft. *Journal of Military and Strategic Studies*, 19(4). https://jmss.org/article/view/68871

Sacchi, M. (2024). *The Combined Space Operations Initiative: an Opportunity for European States?* FINABEL – European Land Forces Commanders Organisation. https://finabel.org/the-combined-space-operations-initiative-an-opportunity-for-european-states/.

Sayler, K. M. (2024, February 22). *Emerging Military Technologies: Background and Issues for Congress*. Congressional Research Service. https://sgp.fas.org/crs/natsec/R46458.pdf.

Sloan, G. (2012). Military doctrine, command philosophy and the generation of fighting power: genesis and theory. *The Royal Institute of International Affairs,* 88 (2), pp. 243-263. https://ciaotest.cc.columbia.edu/journals/riia/v88i2/f_0024615_20260.pdf.

Smit, S., et al. (2022). *Securing Europe's competitiveness - Addressing its technology gap.* McKinsey Global Institute. https://www.mckinsey.com/~/media/mckinsey/business%20functions/strategy%20and%20corporate%20finance/our%20insights/securing%20europes%20competitiveness%20addressing%20its%20technology%20gap/securing-europes-competitiveness-addressing-its-technology-gap-september-2022.pdf.

Strachan, H., & Beckett, I. F. W. (2006). Big Wars and Small Wars. *The British Army and the Lessons of War in the 20th Century (*Abingdon, UK: Routledge 2006).

Soare, S. R. (2021). *Innovation as Adaptation: NATO and Emerging Technologies.* The German Marshall Fund.https://www.gmfus.org/sites/default/files/Soare%2520%2520NATO%2520emerging%2520tech.pdf.

Soare, S. R. (2023a). *Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age.* International Institute for Strategic Studies. https://www.iiss.org/en/research-paper/2023/08/digitalisation-of-defence--in-nato-and-the-eu/.

Soare, S. R. (2023b). European military AI: Why regional approaches are lagging behind. *In The AI Wave in Defence Innovation* (pp. 80-111). Routledge. https://api.taylorfrancis.com/content/chapters/edit/download?identifierName=doi&identifierValue=10.4324/9781003218326-5&type=chapterpdf.

Štrucl, D. (2022). Russian aggression on Ukraine: Cyber operations and the influence of cyberspace on modern warfare. *Contemporary Military Challenges/Sodobni Vojaški Izzivi*, 24(2), 103-123. https://sciendo.com/pdf/10.33179/bsv.99.svi.11.cmc.24.2.6.

Szewczyk, B. (2024, March 27). Why a European Army Makes No Sense. Foreign Policy. https://foreignpolicy.com/2024/03/27/europe-eu-nato-european-army-russia-ukraine-defense-military-strategy/.

Taylor, C., & Kay, L. (2019, August 27). *Putting the enemy between a rock and hard place: Multi-Domain Operations in practice.* Modern War Institute. https://mwi.westpoint.edu/putting-enemy-rock-hard-place-multi-domain-operations-practice/.

Tuck, C. (2022). Understanding Land Warfare. Part II. Routledge, London, 2nd edition.

U.S. Cyber Command PAO. (2022). *CYBER 101 - U.S. Cyber Command Mission*. US Cyber Command. https://www.cybercom.mil/Media/News/Article/3192016/cyber-101-us-cyber-command-mission/.

US Army (2018). The U.S. Army in Multi-Domain Operations 2028: TRADOC Pamphlet 525-3-1. https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf.

US Army. (2020). *FM 100-5 Operations 1982: Training and Doctrine Command*. https://cgsc.contentdm.oclc.org/digital/collection/p4013coll9/id/976/.

US Army. (2022). *Field Manual 3-0. Operations.* Department of the Army. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf.

US Army (2024). *America's First Corps.* https://www.army.mil/ICorps.

Warner, M. (2020). US Cyber Command's First Decade. *Hoover Institute*, Aegis Series Paper No. 2008. https://www.hoover.org/sites/default/files/research/docs/warner_webready.pdf.

Watling, J. & MacFarland, S. (2021). *The Future of the NATO Corps.* Royal United Services Institute. https://rusi.org/explore-our-research/publications/occasional-papers/future-nato-corps.