CINAMIL
MILITARY ACADEMY RESEARCH CENTER

# Shaping the Holistic Concept of Multi-Domain in a Legal Vacuum. A Tricky Issue

Marco Marsili

## Introduction

The recognition by the US and NATO of ‘new’ domains of operations, namely the cyber and (outer-)space, plus the information and the electromagnetic spectrum (EMS), makes the traditional partition of physical domains of land, air, maritime obsolete (Marsili, 2019a). While classic domains are generally well understood conceptually, to the extent that joint doctrine does not feel the need to define them, the new domains are much more difficult to conceptualize and bound within a constructive definition (Donnelly & Farley, 2019, p. 9).

## Framework

Since the cyber has been recognized by NATO as a domain of operations (July 2016), and the Alliance has approved the first-ever space policy (June 2019) – a step towards the acknowledgment of space as a warfighting domain, as President Trump has officially characterized it (August 2019) – the doctrine has speeded the integration of all domains (Marsili, 2019a).

The concept of cross-domain operations is not new, but multi-domain has increased in popularity over the past decade as military services, those of the US, inter alia, have sought to codify their approach to warfare beyond the traditional confines of land, sea, and air (Marsili, 2019; Reilly, 2019, p. 16). What they are committed to are converging military capabilities across the joint force with continuous integration across multiple domains (Marsili, 2019a; Townsend, 2019, p. 29).

## Challenges

The discussion about ‘Multi-Domain Operations’ (MDO), i.e. how operations are conducted in time and space with synchronization of the other domains, has been stimulated since new domains such as the cyber and space have emerged next to the traditional domains of air, land and sea — emerging and disruptive technologies have further complicated the operational environment (OE).

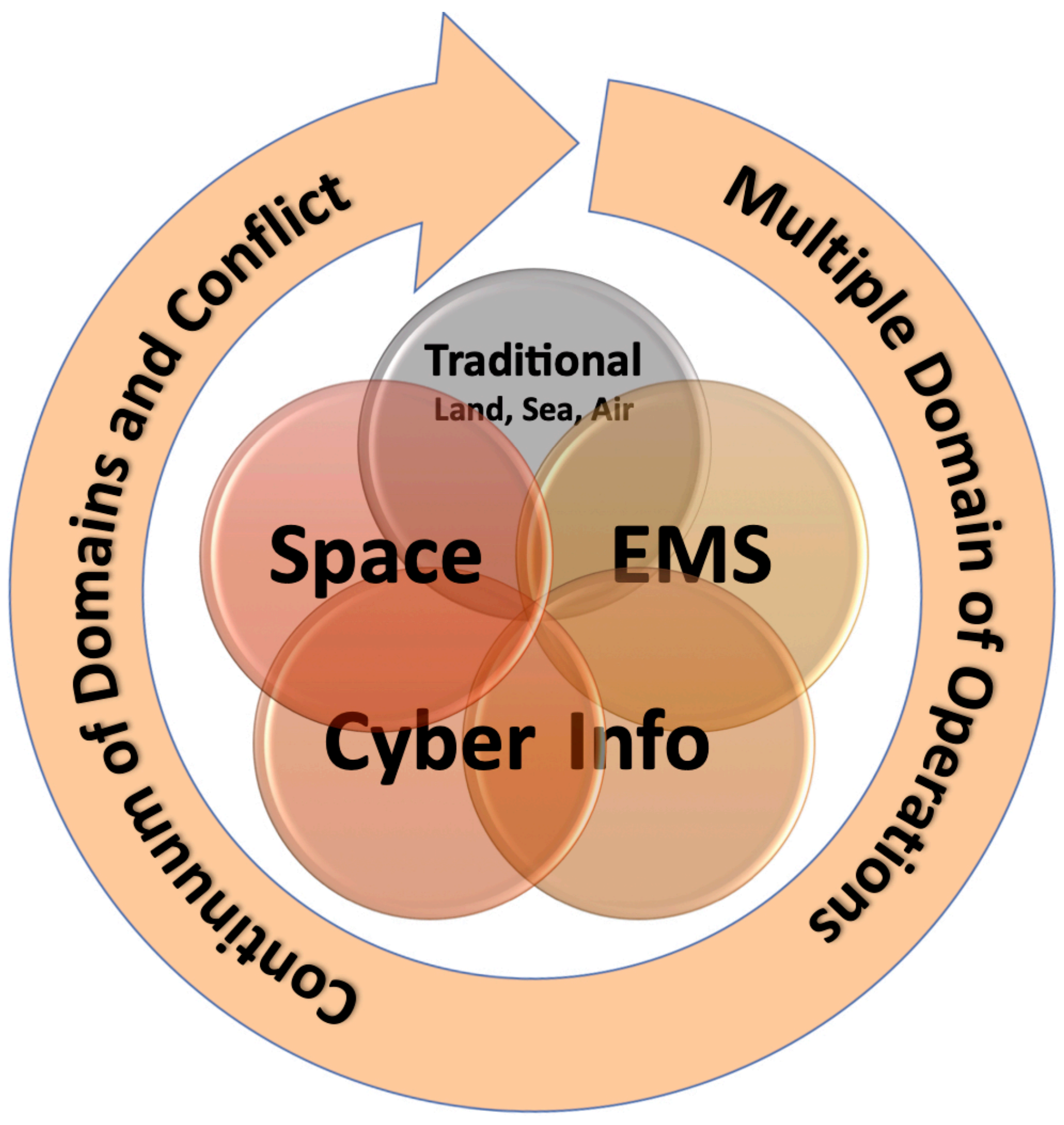
We then moved quickly from a concept of cross-domain to multi-domain (Marsili, 2019), without the time to define any of the new domains — neither of the classic domains. Rather, the doctrine does not provide us with any definition of the basic term ‘domain’, and this further complicates the scenario. Before coming to a definition of ‘Multi-Domain Operations’, it is necessary to define, not only the correlation between domains, but also the same non-traditional domains (Marsili, 2019).

The battlefield has become undefined, and virtually unlimited (Marsili, 2019b, p. 191). The high-tech evolution of warfare – artificial intelligence (AI), machine learning (ML), lethal and non-lethal unmanned systems, lethal autonomous weapon systems (LAWS), quantum computing and big data, to name a few – imposes the need to operate across all domains (Marsili, 2019). Not yet defined the basic term ‘domain’, as well as the new domains added to the traditional ones, we are asking what’s after joint. It is like making a double somersault pike with screwing immediately after learning leapfrogging.

While the doctrine can define more or less easily these concepts, the question of their legal definition it has yet to be addressed and fixed (Marsili, 2019ab). It is no small matter, as it comes to adapting the doctrine to current public international law, or to modify the latter to fit the first — in this case, the problem would be very difficult to solve. Positive and customary international law – multilateral and bilateral treaties, the law of war, international humanitarian law (IHL) – are put to the test in this challenge (Marsili, 2018).

Given the complexity of modern warfare, the field of hybrid and asymmetric conflicts expands dramatically, and it should be limited by setting a threshold (Väljataga, 2018; Marsili, 2019a). Rules are necessary to impose legal limits on the use of lethal force, to avoid an escalation, and to protect civilians (Marsili, 2019a; 2019b). Moreover, while the space domain involves only the states, given the necessary capabilities, other domains – e.g., the cyber, the information, and the EMS – are accessible also to non-state entities, such as insurgents and terrorist groups, and this poses further ethical and legal questions that should be timely addressed by the international community (Marsili, 2019a; 2019b).

Multiple domain of operations and Continuum of domains and conflict (CoD/CoC) can be represented with Euler-Venn diagram and formulas:


Continuum of Domains and Conflict
Multiple Domain of Operations
Traditional
Land, Sea, Air
Space
EMS
Cyber
Info

**Multiple Domain Operations: Holistic View of the Continuum of Domains and Conflict**

$T=\{\text{land, sea, air}\} \subset MDO$; $MDO=\{\text{Land, Sea, Air, Info, Ems, Cyber, Space}\}$; $MDO=Traditional \cup Info \cup Ems \cup Cyber \cup Space$; $CoD/CoC=Traditional \cap Info \cap Ems \cap Cyber \cap Space$.

For a discussion on the visual representation of the continuum, see e.g.: Dempsey (2015, p. 4); Parkinson (2019, p. 42); Donnelly & Farley (2019, p. 9).

New concepts of operation, fueled by technological advances, have facilitated interconnectivity across different domains of warfare (Marsili 2019; Canovas, 2019, p. 47). It’s not only the capacity to integrate and operate in all domains simultaneously to get the greatest advantage possible against adversaries. The two camps – the western of the US-led NATO, and that of the adversaries, firstly China and Russia – seek to derive mutual benefit from the absence of standards and legally binding norms.

The North Atlantic Alliance is also focused on developments in the field of automation, in the integration of AI and the design of unmanned vehicles capable of operating in multiple domains, and in technological convergence, i.e. the integration of multiple research fields in the identification of the solution to a technological challenge (Marsili, 2019). Therefore, domain integration is an exceptionally tricky issue that poses challenges on several layers: technological, legal, political, military, operational, strategic, tactical (Marsili, 2019).

The purpose of this contribution is not to address the strategic and/or tactical implications of these concepts to the battlespace, which this paper does not provide any, rather than turning on a light on the risks posed by the lack of standard definitions (Marsili, 2019ab).

This also calls into question the traditional division between civil and military, that is between combatants and non-combatants, and the consequent application of international law (Marsili, 2018; 2019a; 2019b). Therefore, it’s not only a holistic view of the OE, that should be explored, but also the ethical and legal implications should be taken into account (Marsili, 2018; 2019a; 2019b).

## Conclusions

Political and military leaders are mainly focuses on the development of strategic and tactical concepts, and they neglect the importance of a binding legal framework — this leaves hands free. The liaison between political and operational levels in decision-making process requires that the norms be well defined, also to ensure accountability (Marsili, 2019a). This paper aims to raise questions that could be useful to policymakers and military leaders to open up political space to get deals done.

## References

Canovas, J. (2019). Multi-Domain Operations and Challenges to Air Power. In Joint Air Power Competence Centre [JAPCC] (Ed.), *Joint Air & Space Power Conference 2019. Shaping NATO for Multi-Domain Operations of the Future. Read Ahead* (pp. 47-54). Kalkar: JAPCC.
Dempsey, M. (2015). *The National Military Strategy of the United States of America 2015*. Washington, DC: Joint Chiefs of Staff.
Donnelly, J. & Farley, J. (2019). Defining the ‘Domain’ in Multi-Domain. In JAPCC (Ed.), *Joint Air & Space Power Conference 2019. Shaping NATO for Multi-Domain Operations of the Future. Read Ahead* (pp. 7-12). Kalkar: JAPCC.
Marsili, M. (2018, December 18). The Twenty-First Century Conflicts. Poster session and paper presented at the EAI&DCM 2018, Instituto Universitário Militar, Lisboa, Portugal. doi:10.5281/zenodo.1992458; 10.5281/zenodo.2173544.
Marsili, M. (2019a). The High-Tech Evolution of Warfare in the Twenty First Century. Considerations and Implications on Policy and Doctrine [manuscript scheduled to be published in *Military Cyber Affairs*, *4*(2)].
Marsili, M. (2019b). The War on Cyberterrorism. *Democracy and Security*, *15*(2), 172-199. doi: 10.1080/17419166.2018.1496826.
Parkinson, J. (2019). Is Fluidity the Key to Effective Multi-Domain Operations?. In JAPCC (Ed.), *Joint Air & Space Power Conference 2019. Shaping NATO for Multi-Domain Operations of the Future. Read Ahead* (pp. 39-45). Kalkar: JAPCC.
Reilly, J.M. (2019). Multi-Domain Operations. In JAPCC (Ed.), *Joint Air & Space Power Conference 2019. Shaping NATO for Multi-Domain Operations of the Future. Read Ahead* (pp. 15-24). Kalkar: JAPCC.
Townsend, S. (2019). Accelerating Multi-Domain Operations: Evolution of an Idea. In JAPCC (Ed.), *Joint Air & Space Power Conference 2019. Shaping NATO for Multi-Domain Operations of the Future. Read Ahead* (pp. 27-31). Kalkar: JAPCC.
Väljataga, A. (2018). *Tracing Opinio Juris in National Cyber Security Strategy Documents*. Tallin: NATO CCD COE.

Poster supported by Fundação para a Ciência e a Tecnologia (FCT) through national funds under grant SFRH/BD/136170/2018

Poster presented at the II Encontro Anual Investigação e Desenvolvimento em Ciências Militares (EAI&DCM2019), Nov. 27, 2019, Escola Naval, Almada, Portugal

DOI: 10.5281/zenodo.3473959

UNCLASSIFIED

FCT
Fundação
para a Ciência
e a Tecnologia

Marco Marsili
http://www.marcomarsili.it
Email: info@marcomarsili.it
Twitter: @marcomarsili1
Facebook: @marco.marsili1

CENTRO DE INVESTIGAÇÃO E DESENVOLVIMENTO DO INSTITUTO UNIVERSITÁRIO MILITAR
CIDIUM
I&DCM 2019
CIDIUM