ITALIAN DEFENCE GENERAL STAFF





The Italian Defence Approach to Multi-Domain Operations

© All rights reserved – MINISTRY OF DEFENCE – Defence General Staff Title: "The Italian Defence Approach to Multi-Domain Operations", 2022 Ed. Original title: Approccio della Difesa alle Operazioni Multidominio, Ed.2022 Translation by: Defence General Staff Language Services

FOREWORD BY THE CHIEF OF THE DEFENCE STAFF



As Defence operates in a highly competitive and complex environment, it will need a predictive and integrated perspective and try to preserve its efficiency and credibility, two decisive factors on the modern battlefield.

Hybrid threats, disinformation campaigns, variable intensity conflicts and socalled natural shocks – i.e. natural disasters, pandemics, etc. – characterise the trends of the future. They will require integrated, timely and synergetic responses that can benefit our entire national system. This is especially true in times

dominated by a state of permanent competition between state actors that can operate indiscriminately in multiple domains and use all available resources.

Defence has an inescapable need for true multi-domain capabilities capable of synchronising actions and effects. Through such capabilities, it will also be able to see through and understand the surrounding threats, and manage effective, timely responses to generate stable effects over time in all domains, namely land, sea, air, cyber and space, as well as in the information and cognitive environments.

However, a concrete multi-domain Defence capability will not be achieved without pushing jointness forward in decisive and coordinated manner, for jointness is bound to be overtaken and incorporated into the Multi-Domain Operations (MDO) concept itself.

Such integration can no longer be postponed. It is a fundamental intermediate step in terms of planning, training and overall approach. It must be pursued with unwavering determination, while respecting the competences and specificities of each single-service component, and overcoming reluctance to change and anachronistic partisan logic.

That said, there is a clear need to define a shared, unified and cross-cutting national strategic vision that defines the perimeter for the execution of operations. We need to overcome rigid conceptual separations with impetus and give coherence to the information we gather. We will have to implement a fully multidomain Command and Control structure as the basis for ensuring timely decisions and operational effectiveness. In this regard, the process will rest upon the principles of integration and interoperability between systems, sensors, processes and actors involved in the different domains, both nationally and internationally. Furthermore, it is important to foster inter-departmental and inter-agency discussion, exchange and coordination, as well as pragmatic dialogue with private sector entities and actors in order to stimulate synergies and shared, structured actions, thus achieving a genuine whole-of-government approach.

In parallel, we will have to define the new role of human beings with respect to the evolution of the emerging technologies. With respect to such a role, a renewed process of selection, training and valorisation of human capital, i.e. the technical skills and education of leaders, will be strategic.

Leadership is called upon, therefore, to update its idea of operations, move beyond sector logic, and consciously embrace the idea of interconnectedness. This is the only possible key to rethink how to conduct operations and to adapt – with courage, responsiveness and foresight – processes and organisations. Such an approach, moreover, will underpin the necessary renewal of policies, doctrines, procedures and innovative tactics to better address the changing environment and potential threats.

This document represents a significant step in the evolution of Defence strategic thinking that has already been underway for some time. It contributes to spreading awareness of the need to develop and pursue an effective and uniform national approach among institutional actors, with respect to a multidimensional scenario that is rapidly changing and transforming and therefore requires necessarily systemic responses.

This is the foundation for a coherent reflection on the subject, so that Defence can swiftly implement effective, convergent and relevant multi-domain operations and thus multiply the positive returns for the country, including through adequate action and deterrence capabilities.

Enjoy your reading!

Ammiraglio Giusep

TABLE OF CONTENTS

TABL	E OF CONTENTS	1
INTRO	DUCTION - UNDERSTANDING THE MULTI-DOMAIN CO	NCEPT1
THE I	DEA OF MULTI-DOMAIN	1
RELA	TIONS AMONG DOMAINS	2
THE I	DIMENSIONS OF EFFECTS	3
DIME	NSION-RELATED ACTIONS AND EFFECTS	3
CHAP'	FER 1 - THE COMPLEXITY OF THE SCENARIO	5
1.1	EVOLUTION OF THE FRAMEWORK	5
1.2	THE COMPETITION CONTINUUM	6
1.3	COMPLEXITY AND MULTIDIMENSIONALITY	7
1.4	THE NEW CHALLENGES OF COMPETITION	9
CHAP'	FER 2 - THE ITALIAN APPROACH	
2.1	DEFINING A MILITARY PROBLEM	17
2.2	THE RISK FACTORS	
2.3	CONFLICT FACTORS	
2.4	THE NATIONAL SECURITY STRATEGY AND THE ROLE OF DEFENCE	20
CHAP'	FER 3 - DEFENCE IN MULTI-DOMAIN OPERATIONS	21
3.1	DEFENCE ORGANISATION ACROSS DOMAINS	21
3.2	MULTI-DOMAIN OPERATIONS (MDO)	23
3.3	NATIONAL INTEGRATION IN MANAGING NEW DOMAINS	
CONC	LUSIONS - GUIDELINES	
MULTI-DOMAIN: A NEW PARADIGM		
GENERAL GUIDELINES		
DEFE	NCE GUIDELINES	
ANNE	X	
Annex A - INTERNATIONAL PERSPECTIVES		
Annex B - GLOSSARY		
Annex C - RESEARCH METHODS AND REFERENCES		

INTRODUCTION UNDERSTANDING THE MULTI-DOMAIN CONCEPT

THE IDEA OF MULTI-DOMAIN

The term multi-domain (MD) has become increasingly common in recent years. Some countries, mainly Western ones, have tried to codify their approach to military operations

beyond the traditional domains of land, sea and air, and to add the new cyber¹ and space² domains. This attempt to expand the battlefield aims at countering the strategies of potential peer-competitors. It is precisely these

DOMAIN of operations

A set of capabilities and activities applied to the battlefield in a target environment (maritime, land, air, cyber, or space).

competitors who want to deny the other side the chance to respond, and pursue their strategic interests unchallenged through the coordinated use of all instruments of power within the competition continuum³.

Despite the widespread use of the term, there are multiple definitions, leaving ample room for interpretation. Since its first conceptualisation, a broad international debate has

ENVIRONMENT

The surroundings in which forces operate, including air, water, land, space, *cyberspace*, natural resources, flora, fauna, human beings, and their interrelation. The environments where military operations take place are: maritime, land, air, space, cyber, plus the information and the electromagnetic environments.

information environment has become increasingly important. Within this framework, the multi-domain concept is naturally evolving into the ability to generate effects in all possible dimensions of confrontation (physical, cognitive and virtual), started, leading to the development of different approaches on the subject, which can be traced back to the need to cope with a hybrid aggression by potential peercompetitors.

The effect of robust disinformation campaigns has also highlighted how crucial the electromagnetic **environment** is and the importance of the cognitive **dimension** of confrontation to such an extent that the

DIMENSION of effects

The conceptual scheme for assessing the effects that military operations must achieve in the three dimensions of the battle space, i.e. physical, virtual and cognitive.

regardless of the official recognition of the existence of a new domain.

¹ NATO recognised cyber as a domain at the Warsaw Summit in 2016. It acknowledged that a cyberattack can go so far as to cause damage comparable to an armed attack and, therefore, become a case for collective defence under Article 5 of the Washington Treaty.

² In view of its relevance for deterrence and defence, from navigation to intelligence to threat detection, the Foreign Ministers of NATO recognised the space domain at their meeting in Brussels in 2019.

³ NATO Allied Joint Publication - AJP-01-F (draft).

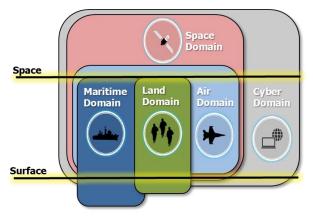
Knowing that superiority in traditional domains may not be easily attainable in an era when technologies available to state and non-state actors proliferate, the need for a paradigm shift towards a new multi-domain approach arises. Such a shift must be inspired by the need to generate lethal and non-lethal effects not just to achieve supremacy in a single domain, but to maintain freedom of action by generating effects in all dimensions of confrontation and to improve understanding of the interests and actions of potential adversaries while limiting their action through enhanced strategic anticipation and situational awareness.

Moreover, although born and consolidated in an exclusively military context to develop the capacity to penetrate possible adversary Anti-Access/Area Denial (A2AD) bubbles, the Multi-Domain approach is expanding well beyond the Defence domain alone. It extends to the ability of a State or an Alliance to employ its power projection through the synchronised deployment of all instruments of national power (Diplomatic, Informational, Military, and Economic - DIME) within the competition continuum, influence adversaries, and counter their actions by protecting its own interests. In this regard, multi-domain should be understood as the need to combine the use of the military instrument of Power (MIoP) with the other Instruments of Power (IoP).

RELATIONS AMONG DOMAINS

Drawing a distinction between the domains of operations is useful to plan and conduct military operations. However, such a classification does not take into account the full spectrum of capabilities available to individual components and the possibility of generating effects in other domains through cross-domain actions.

Although the five domains of



operations have different characteristics, they are strongly interlinked. The three classical domains – land, maritime and air – are traditionally connected to the respective components. They have no clear-cut boundaries but areas where they connect or overlap. Reference is to, among others, coastal and littoral areas between land and maritime domains, air platforms of the land and maritime components operating in the air, air platforms generating surface effects, etc.

The space domain is global and autonomous, but at the same time is an enabler for the classical domains (civil and military sectors are deeply dependent on space services) and for the delivery of critical functions such as satellite communications and positioning, navigation and timing systems.

Finally, the cyber domain is characterised by its virtual nature and ubiquity and is transversal to all other domains.

THE DIMENSIONS OF EFFECTS

Starting from the relationships between the domains, actions are planned and conducted with a clear understanding of what dimension will be influenced or in which dimension the desired effects fall in order to achieve the mission. The dimensions are as follows:

- Physical, where physical activities take place and physical effects occur through the interaction between geography, infrastructure, flora and fauna, individuals, states, cultures and societies. The physical dimension has been shaped by humans over time and can only be further manipulated with considerable effort requiring time and energy.
- Virtual, where intangible activities are carried out by non-tangible entities. The latter may be virtual (e.g., social media) or software. This dimension may be manipulated as it is artificial.
- Cognitive, i.e. pertaining to the sphere of perceptions and decisions, in which social and psychological effects can be brought to bear that influence an individual's behaviour, thereby achieving a lasting result.

DIMENSION-RELATED ACTIONS AND EFFECTS

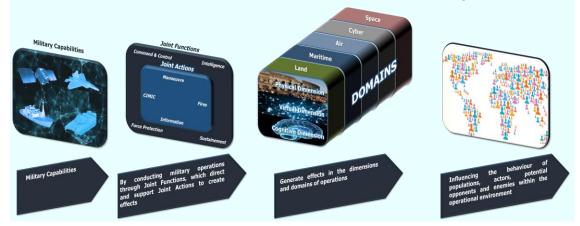
Multi-domain is not simply the sum of individual domains and, therefore, individual capabilities. In this new perspective, the boundaries between domains blur, resulting in a single environment where, in order to achieve multi-dimensional effects, one must harmonise the instruments of national power and orchestrate the actions of different capabilities. More specifically, the domains of operations are seen as a single, interconnected setting, in which the synchronised conduct of actions and modulated efforts achieve more than in the single domain view. On the basis of the objectives to be achieved, the effects to be realised are determined by influencing the actors in the operational environment in several dimensions. The effects result from actions and activities conducted through the available capabilities in the different domains, including the electromagnetic and information environments. These actions, thanks to the permeability of the domains and the characteristics of the information environment, can be further amplified.

In this perspective, it is necessary to detect how actors' perceptions and behaviour change in order to be able to influence them at the right time through interrelated kinetic and non-kinetic actions, which produce effects in the physical, cognitive and virtual dimensions.

A multi-domain operations (MDO) approach must overcome the vertical and physical separation of the individual components. It must also seek and improve the understanding and deployment of different military and civil capabilities and resources to simultaneously develop multiple convergent actions and produce multiple effects in the different dimensions. The reiteration of this posture over time, combined with surprise and deception, will allow the initiative to be won and maintained. The opponent will therefore have to adopt a cautious and defensive posture in all domains and dimensions.

When applying the joint actions framework to the conduct of military operations, therefore, one must take into account the relationship between joint functions – namely intelligence, command and control, manoeuvre, fires, information, CIMIC⁴, force protection and sustainment – multi-dimensional objectives, and domains. The joint functions provide the structure for commands and units to concentrate military capabilities at the most appropriate place and time and to effectively conduct operations in the competition continuum at any level of intensity, thus ensuring force protection and sustainment. The achievement of effects in the physical, cognitive and virtual dimensions is achieved through the synchronisation and harmonisation of the four effect-generating joint actions – notably manoeuver, fires, information, and CIMIC – under the guidance of the Command and Control function.

Joint Actions in a Multi-dimensional and Multi-domain Perspective



⁴ Civil Military Cooperation.

CHAPTER 1 THE COMPLEXITY OF THE SCENARIO

1.1 EVOLUTION OF THE FRAMEWORK

The framework of reference is influenced by multiple dynamics of a political, social, demographic, environmental, economic and technological nature, usually referred to as mega-trends. There is also the presence, or in some cases the resurgence, of threats and challenges that will substantially affect the world's geopolitical balance in the years to come, fuelling situations of pervasive and persistent instability⁵. In a context characterised by dynamic and volatile phenomena, manifest and latent forms of competition involving state and non-state actors are continuing and will continue to increase.



The number of peer/near-peer competitors and the increasingly interconnected nature of the international system are the main factors contributing to the disorder and uncertainty of the geopolitical environment, making the current system increasingly complex. An uncertain geostrategic balance, the emergence of new state and non-state actors on the international scene, the resurgence of the Great Power Competition, the ongoing race to exploit energy resources, and the ease of access to emerging technologies multiply the forms of international competition. Within such a competition, all actors seek to protect their national interests by applying soft, hard, or smart power instruments⁶ and by weaving a dense network of interactions with other actors.

Compared to the past, when an opponent was as dangerous as its political value and military potential, the weight and role of potential competitors in today's uncertain, unstable, ambiguous and congested context are difficult to ascertain. They are the result

⁵ Italian Defence General Staff - Future Scenarios Concept, 2021 ed.

⁶ Hard power involves the use of military and economic instruments of coercion to influence the behaviour of other actors, while soft power involves the use of attractive (diplomatic, cultural and historical) instruments. Smart power combines hard and soft power, including through the strategic use of diplomacy, persuasion, influence, capacity building and power projection according to a model of social and political legitimacy.

of various elements combined, not all of which are linked to the political and military institutional framework. Among the main factors contributing to this change are:

- globalisation, which facilitates the creation of networks economic, religious, political, lobbying, cultural, etc. at a once unimaginable speed and capillarity;
- technological development, meaning the increasingly easy and affordable access to systems of power – including unconventional weapons and/or weapons of mass destruction – and the availability of new technologies to operate from anywhere on the globe, in domains and environments such as cyber and information where attackers are not easily identified,.

We are therefore witnessing a confrontation that unabashedly crosses the entire spectrum of competition. Across this spectrum, the main protagonists fall into two categories, as mentioned earlier. These are:

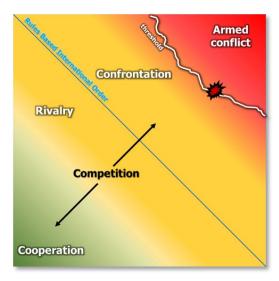
- state actors with renewed assertiveness, including formerly minor countries that take on increasingly important roles globally thanks to rapidly expanding economies;
- non-state actors, that is, non-governmental entities capable of playing a decisive, if not equal, role in the definition of international disputes, or in influencing opinions, masses, and economic interests, and being sometimes more effective than governments themselves. Within fragile state frameworks, characterised by weak institutions, non-state actors have been spreading who have conducted and may continue to conduct insurrectional, terrorist, criminal, sabotage, subversive and even cyber offensive actions against states.

1.2 THE COMPETITION CONTINUUM

Given the changing context, a system of international relations characterised by permanent competition is emerging. The NATO model of the so-called competition continuum on four different incremental levels well represents the attitude and behaviour of the actors. It starts from Cooperation and Competition, which represent condition of peace. a to Confrontation and Armed Conflict.

In more detail, these levels can be described in the following terms:

- Cooperation occurs when the attitude of



actors on a given issue is one of alignment and cooperation to achieve common goals:NATO is an example of cooperation to protect and defend the security of nations.Cooperation provides the ideal basis for lasting stability.

- Competition is when two actors are in a state of peace but have conflicting goals or visions. The actors compete while remaining in compliance with the Rules Based International Order (RBIO), the latter being a shared commitment by all countries to conduct their activities in accordance with agreed rules that multinational treaties fine-tune over time. Competition is the normal state in international relations and,

when brought within the RBIO, can be beneficial to all parties and to the international system as a whole. Examples of rivalry include UN rules on global commons or freedom of navigation.

- Confrontation occurs when actors in a state of crisis adopt hostile behaviour or attitudes in the form of threats and violence as a means of competing to resolve issues in their favour. There is no defined threshold separating confrontation from armed conflict, since many actors intentionally try to cover or blur the distinction. Actors will consciously seek to expand or restrict the threshold in an attempt to increase or limit freedom of action. Proxy warfare⁷, terrorism and economic coercion are all examples of activities below the threshold of armed conflict. In response, other states will either conduct deterrent and defensive actions to reduce the confrontation or escalate activities to armed conflict.
- Armed Conflict starts when one or the other actor decides to use military force.
 Armed conflict includes acts of direct violence and therefore causes an escalatory effect on the cognitive dimension⁸.

The boundaries between Cooperation and Competition, and the threshold between Confrontation and Armed Conflict are complex and dynamic. Their progression is neither linear nor easily defined. Moreover, inter-state relations are typically sectoral in nature. States may cooperate in one area, confront each other in another, and potentially fight an armed conflict in yet another.

1.3 COMPLEXITY AND MULTIDIMENSIONALITY

The current paradigms of *jus ad bellum*⁹ and *jus in bello*¹⁰ (Law of War) are far from being solid, especially because competition develops in a 'grey zone'. Moreover, the process of globalisation correlated with technological development and cross-cutting digital connectivity is transforming societies. It generates a system of aggregation that overcomes the tendency towards separation and redefines the concept of national borders. It creates a scenario in which relationships bring different milieus into a single, complex system of systems where variables are not independent, but influence each other and create new complexities. Therefore, one needs to understand what relationships characterise the complexity of the operating environment and what risks are associated with the attitude of actors who may attempt to manipulate the system to their own advantage.

⁷ An armed conflict between two states or between non-state actors acting on provocation or on behalf of other factions that are not directly involved in the hostilities.

⁸ The exponential nature of the effects of an armed conflict on the cognitive dimension is considered so relevant that NATO has included a specific study on '*Warfighting Effects on the Cognitive Dimension*' in the Lines of Deliveries descending from the NATO Warfighting Capstone Concept.

⁹ A set of rules and principles that states are obliged to respect before they can engage in armed conflict or take part in an existing conflict.

¹⁰ A set of rules and principles that apply to an armed conflict.

1.3.1 A Multi-domain Operational Environment

The complexity described above requires a definition of the operational framework of reference in which to exercise the action of the instruments of national power through modelling efforts incorporating environments, domains, dimensions and systems. In this regard, the new operational framework of reference must be considered as an evolving element. Its variations bring it to a new state other than the initial one. To better understand this complexity, it is useful to clarify how the different components interact and influence each other. To do this, we use the threedimensional figure below to portray the components on its faces, notably:

- the domains of military operations (land, sea, air, space, and cyber);
- the three dimensions of effects (physical, virtual, and cognitive);
- political, military, economic, social, informational and infrastructural systems (PMESII)¹¹;
- the additional 'information' and 'electromagnetic' environments where, in addition to the five fundamental domains, military operations are already being being conducted. In the former two, the new future challenges and threats.



However, these elements are not to be considered as separate factors, but a part of a single 'system of systems' in which all aspects are linked via relationships and nodes located on different planes. Such is the multi-domain operating environment.

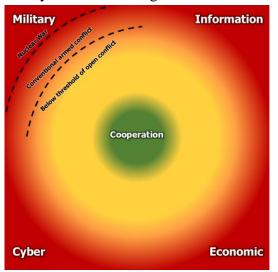
2.3.1 The Stakeholders' Attitude

From the complexity of the multi-domain operational environment comes the possibility for certain actors to maintain an ambiguous and aggressive attitude. They can resort to all instruments of their national power – diplomatic, informational,

¹¹ An analysis model that identifies six system elements: political, military, economic, social, information and infrastructure (PMESII). It allows the socio-political organisation of the population in the operational environment to be defined.

military and economic (DIME) – across all operational domains and information and electromagnetic environments to exploit their opponents' vulnerabilities across the entire PMESII spectrum, and generate effects in the physical, virtual and cognitive dimensions. Their goal is to create friction between peoples, nations, organisations, and undermine peoples' trust in their governments, institutions, and their allies and partners, and thus pursue their own interests, while denying their opponents the opportunity to respond.

In this context, it should be noted that the exploitation of the information environment is a key and determining factor in influencing the decision-making processes of the



multiple actors present. For instance, one can use available information quickly and flexibly to one's advantage, gain superiority in the collection, processing and dissemination of information, or in preventing similar activities by adversary elements or forces. One understands, therefore, how non-military means sometimes constitute the main instruments chosen by aggressors to achieve their strategic objectives. In this case, the linear concept of military escalation is no

longer valid. Actions undertaken in the dimensions of competition below armed conflict pose a significant threat to national security on a par with purely military threats.

Therefore, the modern threat appears to be **multidimensional** and **cross-cutting** in nature, capable of weakening the entire national system, even by striking a single vital interest, because of its capacity to produce effects in any other dimension. The complexity of the system and of the relationships between the factors involved and the multidimensional and cross-cutting nature of the threat require us to increasingly think of security and defence according to a whole-of-government and whole-of-society approach, in which all interests are linked and interdependent.

1.4 THE NEW CHALLENGES OF COMPETITION

The speed of development and dissemination of innovative, emerging and disruptive technologies is profoundly changing the character of competition and extending its scope far beyond traditional physical boundaries. In this regard, competition in the new cyber and space domains and the effects generated by and within the 'information' and 'electromagnetic' environments are particularly relevant.

1.4.1 The Cyber Domain and the Virtual Dimension



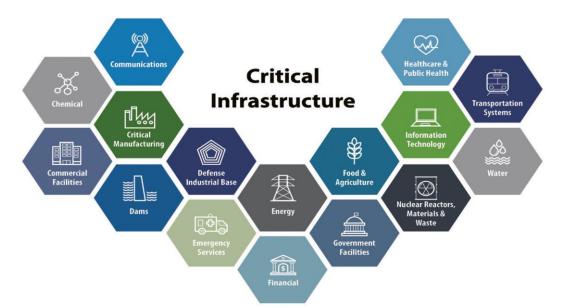
Unlike traditional domains, the cyber domain is intangible and transversal. It is becoming increasingly important, including on a geostrategic level. The development and security of a nation increasingly depend on the accessibility of information. Controlling the flow of digitised data has been a focus of attention for quite some time now, and such flows are inevitably related to technologies exposed to the Internet, or at least connected to each other in the broadest sense. In this perspective, since the cyber dimension is pervasive, the control of networks and data is required to ensure essential services and, more generally, to defend a nation. The malicious use of such technologies could lead, on the one hand, to the collapse of essential systems and services and on the other , unleash destabilising potential, which would affect the cognitive dimension and contribute to conditioning public opinion through control of networks and data.

The ability to manage such vast amounts of data will be one of the fundamental parameters in determining the weight of each actor in the economic and political spheres. In fact, we speak of digital sovereignty - i.e. the possibility that subjects, even private ones, will be able to intercept data and use them to rewrite the geostrategic balance and impose new rules on an Internet-based reality.

It follows, therefore, that mastering data management is the basis of military superiority, since, by facilitating the management of information, it facilitates the exercise of command and control and the conduct of operations. Moreover, the increasingly pervasive use of software within weapon systems, combined with the growing demand for connectivity and interoperability between them, has increased the vulnerability to threats coming not only from the traditional domains but also from the cyber domain, hence requiring new approaches and additional measures to protect the operational capabilities of the armed forces.

A better understanding and awareness of the impact of technological development will be a cornerstone of the ability to protect critical infrastructures, whose physical or virtual networks and systems are considered so vital that their destruction or inefficiency could debilitate public security, the economy, health, or any combination thereof.

Cyberspace makes it possible to preserve the anonymity of actors due to the objective difficulty of tracing the source of attacks: thanks to the possibility of operating through fake IPs and foreign servers, attackers enjoy relative impunity (non-attribution). This leads to dematerialisation, deterritorialisation, decentralisation and



denationalisation of relations. It is a fluid domain, which changes and reconfigures extremely rapidly, crosses geographical borders and expands across the globe. Moreover, the cyber domain is the only one where all the instruments of national power can be found: diplomatic, military, economic, and those concerning media control and information management. In order to meet the challenge posed by the multiple forms of evolving cyber threats, starting with state-based ones, Italy has established the 'National Cyber Security Perimeter' (Law 133/2019) to improve the resilience of networks, information systems and IT services of national public and private actors that perform an essential function or service of the state, or are strategic to the country's interests.

¹² Critical infrastructures are the physical resources, services, information technology systems, networks and infrastructure assets that, if damaged or destroyed, would cause serious repercussions to the crucial functions of society, including the supply chain, health, security and the economic or social well-being of the state and the population.

1.4.2 The Space Domain

Strong technological development and renewed interest in space exploration and exploitation have helped expand the possibilities of access to space, and created new opportunities and new challenges.



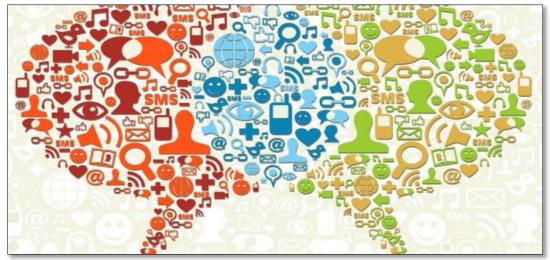
Traditional financial and technological barriers in the satellite field are steadily diminishing and, thanks to reduced access and management costs, more and more users can take advantage of space services. The proliferation of dual-use applications, both civil and military, has definitely expanded the military uses of space. Born out of resource optimisation needs, such applications have proved to be a winning strategy to gain greater public and private support for the space industry and have blurred the boundary between military and civil use. To counterbalance this, there is a dark side to the space domain, as it is increasingly exposed to new risks and systemic vulnerabilities such as espionage, sabotage and space junk multiplication. Therefore, the full achievement of the capability to operate in any condition, including one in which space-based services may be limited or even denied, is highly desirable.

In the competition continuum, space architecture and, more specifically, its individual segments will increasingly represent an area of confrontation. In particular, space technologies will be a strategic sector and will play a decisive role in all of a country's activities, both public and private. For instance, they will help connect to networks globally, provide essential data in the event of natural disasters, and support the conduct of military operations.

With reference to the conduct of military operations, the international treaties in force merely identify aggressive conduct, rather than military uses in general, as a violation of the norm prescribing peaceful uses and purposes in Space. In fact, we accept all military uses not expressly prohibited by the letter of Article IV of the Space Treaty and consistent with the principles contained in the Charter of the United Nations. This is an original approach, based on the idea that there is a continuum between peace and aggression, and that the critical question concerns the amount of force that can be employed without crossing the ideal line separating peaceful from openly aggressive conduct and, therefore, unacceptable under international law.

Finally, a clear distinction must be made between the militarisation and weaponisation of Space. The 'militarisation of space' refers to the use of space-based devices in order to increase the military effectiveness of conventional forces and identifies legitimate military uses. The weaponisation of space, on the other hand, refers specifically to the placement of space-based weaponry in orbit. Ultimately, the currently permitted military uses of space are of a 'passive' nature, while weaponisation would imply a qualitative leap towards 'active' military uses of space, intrinsically endowed with a disruptive nature.

1.4.3 The Information Domain and the Cognitive Dimension



The information environment and the cognitive dimension, although not officially defined as domains of operations, have their own significance, which will probably tend to increase in the conduct of operations, especially in a geostrategic framework whose trend is to avoid kinetic confrontation while increasingly resorting to indirect forms of warfare.

In multi-domain operations, the aim is to achieve a position of advantage that is not only physical, but also psychological, by moving from a situation of military dominance (strongly enabled by technology) to a situation of potential equality or, possibly, subjugation in the virtual field. Among the different ways to achieve this, an indirect approach has been chosen: one defeats the opponent by gaining positions of psychological advantage without necessarily destroying it. Within this framework, information and communication have always historically played a fundamental role, with obvious social repercussions due to their effect in orienting public opinion. The evolution over time of the print media, radio and television has profoundly changed the world of information and communication, thanks to their growing capacity to transmit instant messages to ever larger audiences. However, the use of communication tools for propaganda and counter-propaganda purposes was, at least in part, limited by the forms of control exercised over communication tools and the limited number of people working as information professionals. The digital revolution and the advent of social media and all other digital communication channels have profoundly revolutionised the world of information. They have effectively supplanted all previous tools and opened up the world of communication to a new array of actors who convey their messages and contribute, sometimes decisively, to shaping public opinion and fuelling political debate. It is evident that the opponents will focus their efforts on affecting the way people think, both in real and virtual terms. It is no longer about 'programming minds', but making people choose one behaviour over another spontaneously through a clear and precise information and cognitive strategy.

The pervasiveness of the information environment, with particular reference to its digital dimension, therefore requires an in-depth study to understand the core issues affecting its complex management. These are:

- the sheer amount of information, which has made and will make it increasingly difficult for individual users to have their own informed opinion. Indeed, the quantity and timeliness, to the detriment of the credibility of verified and/or scientifically validated information, have undermined the very authority of information and its professional figures;
- fake news that discredit people, institutions and political positions will be difficult to distinguish from the truth. The cases concerning the COVID-19 pandemic show how the dissemination of news, whether or not they are verified, not only provokes reactions in public opinion, but also becomes central in the political debate;

The manipulation of information could be a strategic factor in the hands of those who know how to exploit it. On the one hand, it could be used to provoke divisions and rifts in those states with a weak national identity or strong internal instability, paving the way for economic and/or military penetration initiatives. On the other, it could increase friction between states to favour other powers that would benefit from the clash that have been triggered, or facilitate the break-up of multinational organisations. This trust becomes the target of the opponent's offensive information and/or cognitive capabilities.

It is therefore evident how the ability to understand the information environment and its dynamics will increasingly become an element of high strategic value. A system that guarantees democratic control and maximum transparency must have a constant and permanent monitoring capacity, in order to prevent, especially in moments of special international tension, manipulated information from weakening the national structure and open the door to initiatives of a financial and economic, if not military, nature that could affect the national system's important and strategic assets.

The pervasiveness of the information environment and technological developments in the field of neuroscience are significantly expanding the scope of competition in the cognitive dimension. The $PSYOPS^{13}$ and $INFO-OPS^{14}$ functions – i.e. key elements in countering the threat described above – could evolve toward a more integrated and all-encompassing stage.

This would translate into the concept of cognitive warfare, that is, a new mode of permanent confrontation where the beliefs and opinions of a population are attacked to destabilise the cohesion, security and prosperity of a nation.



In particular, cognitive warfare employs disinformation campaigns and immense flows of fake news potentially supported by Artificial Intelligence (AI) systems to disarticulate decision-making processes, weaken internal cohesion, erode trust in democratic institutions, and sow doubt and indecision to pursue an ideological agenda by emptying elements of the population's identity of meaning.

The rapid advances in neuroscience and its technologies are generating increasing interest in

the potential use of these tools and methods to exert influence and power on the global stage – so-called neuroscience weaponisation.

By using AI-based systems developed in simulated environments to test the ability of a target to respond to a crisis, or to validate the effectiveness of strategic decisions and military operations in a global context, an aggressor could conceal his identity and act directly against a specific target, thus destabilising the opponent and preventing his response through, among others, popular protest or self-determination movements.

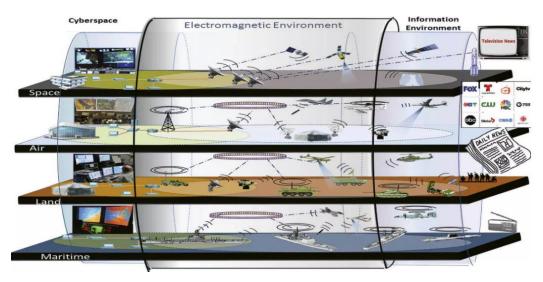
Western democracies are more exposed to this type of risk than authoritarian systems and, therefore, require a whole-of-government approach that, through close collaboration between departments and agencies, can achieve common goals and mitigate the risk arising from this new frontier of competition.

1.4.4 The Electromagnetic Environment

The military use of the electromagnetic spectrum is normally traced back to electronic warfare (EW). The latter includes any action that uses the electromagnetic spectrum, or directed energy to control the radio emission spectrum and alter it. EW is used to attack enemy forces by incapacitating some of their systems, or to gain a tactical and strategic advantage through the electromagnetic spectrum by neutralising adversary mechanical and/or robotic systems.

¹³ Planned activities using communication methods and other direct means to influence perceptions, attitudes and behaviour of an authorised audience (target audience) in order to achieve political and military objectives.

¹⁴ A staff function with the purpose of analysing, planning, evaluating and integrating information activities to create the desired effects on the will, understanding and capacity of adversaries and the public, in support of mission objectives.



Its cross-cutting nature across the physical domains makes the electromagnetic spectrum, together with the cyber domain and the information environment, particularly relevant. It is therefore necessary to be able to monitor, disrupt and interdict the electromagnetic environment to possible competitors.

Among the capabilities required to operate across the electromagnetic spectrum to acquire temporary superiority and exploit any windows of opportunity, the following non-comprehensive list of macro-types is worth mentioning:

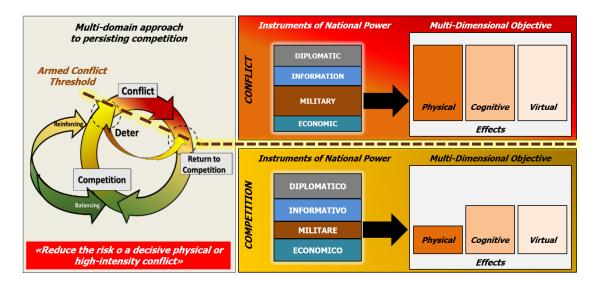
- *signal detection* means the detection, in a congested, chaotic and contested electromagnetic environment, of one or more signals;
- *signal classification* means the classification of a signal, having recognised its main technical characteristics;
- *spectrum monitoring* means the surveillance of the electromagnetic spectrum in theatres of operation to retrieve information on the position of the opponent and the occurrence of possible threats (also called 'spectrum awareness').

Acquiring the skills to operate effectively represents a significant added value as one manages the delicate phase of competition. Indeed, the activities carried out in the electromagnetic spectrum may not be identifiable as an explicit and intentional act of war. Moreover, the electromagnetic spectrum is characterised by extreme mutability in time and space. Therefore, one must develop (1) skills regarding the propagation of electromagnetic waves in air, surface, land or underwater space, the interaction between several electromagnetic waves and the different modulation criteria of a carrier; (2) specific sensors and tools to guarantee situational awareness in the electromagnetic spectrum and, at the same time; (3) dedicated skills to develop actions and generate effects, whether physical or non-physical, lasting or temporary.

2.1 DEFINING A MILITARY PROBLEM

Modern threats become particularly critical and complex when perpetrated, combined and controlled by a single entity capable of grasping and managing the overall effectiveness of the actions implemented as part of a grand strategy. In such a circumstance, the attack on the country's vital interests can in fact be carried out through a variety of means – which are not necessarily weapon systems – and combatant and non-combatant actors, while still keeping the clash below the threshold of open aggression. The ambiguity and pervasiveness of this form of aggression, together with the difficulty of identifying the aggressor itself, hampers the clear and timely recognition of the attack, especially if it is carried out against apparently unconnected targets. This exposes the attacked party to the risk of a delayed or ineffective response. In such a scenario, it is therefore necessary to analyse how national military forces can effectively contribute to the defence of the country and its national interests, as well as to international security within the International Organisations to which Italy belongs. Such a contribution would entail an integrated and synchronised action with the other instruments of national power, namely the diplomatic, informational, military and economic ones.

The competition continuum requires a variable degree of synergy between the aforementioned instruments and a shared and balanced effort to reduce the risk of a kinetic clash, to be used as a last resort. The military must act at all times, in proportion to the circumstances and even below the threshold. This is already the case, for instance, with NATO's Enhanced Forward Presence, where the military helps to generate effects not only in the physical dimension, but also in the cognitive and virtual ones.



2.2 THE RISK FACTORS

An analysis of the major trends and potential adversaries identifies a number of major risk factors that contribute to increasing the threat in a multi-domain context. They are:
 Strategic asymmetry, i.e. the development of new technologies and the multiplication of those of a disruptive nature, the access to which by state and non-state actors is increasingly easy. They generate a direct impact with long-term effects on every dimension of competition, triggering unexpected and unpredictable

- accelerations that are complex to manage, control and predict. Unscrupulousness in the choice of means, methods and strategies to achieve one's own strategic interests unchallenged can be an element of significant strategic advantage for a number of international actors, whose values may be competing with ours as they are less constrained by respect for rules.
- Lawfare indicates the use of advanced technological innovations that can increase vulnerability to possible asymmetric law enforcement (wars on law/wars through law), in the broader context of a multidimensional threat. The lack of standards, or their inadequacy in some areas, could expose some countries, mainly Western democracies, to a regulatory framework that is not conducive to technological innovation itself, promoting a substantial manipulation of international law, and a distortion in customary justice in different countries. To prevent such regulatory gaps, which can be exploited as hybrid threats, anticipation in the form of regulations on the use of technological innovations for operational purposes is key. This evidence of lawfare is even clearer when one addresses the new cyber and space domains, whose character is markedly technological and where developments in artificial intelligence may bring disruptive effects.
- Centralised forms of power, i.e. the ability of certain international actors to employ all the instruments of their national power within a single grand strategy design can be a significant risk factor. The ability to take even unpopular decisions very quickly allows such forms of power to respond promptly to the onset of crisis situations that require a whole-of-government approach. The aforementioned evolution of cognitive warfare opens up new ethical-legal frontiers in competition that require, from the outset, common and shared solutions within an integrated national approach.

2.3 CONFLICT FACTORS

The combined effect of the development of new technologies, the interdependence of modern systems, and the innovative use of new modes of aggression and conflict creates scenarios in which the ability to manage international competition and possible forms of aggression transcends traditional boundaries and takes on an all-embracing dimension that requires complex responses. It follows that it is the continuity of action between security and defence that secures a country. Defence has taken on a broader significance; it extends from the military field alone to all other vital interests and needs of citizens. It is embedded in a synergetic system that envisages the participation of all the actors in the system, each in their own field of competence.

In this general context, a number of factors are recognised as useful in countering the emergence of crises in order to mitigate the potential risks and effects of an escalation of competition. These are:

Understanding complexity. The complexity of the entire system and the strong interdependence of its elements call for detecting individual variations in the system itself. Specific indicators must therefore be defined and correlated with the possible effects generated on the other variables. In this regard, one must first understand the need to overcome the binary model of peace and war and consider how modern threats come from the prevalent use of non-military means.

There is a need to act in an integrated manner and at all levels to develop the ability to understand the complexity of the system rather than simply the sum of its elements. The ability to observe and understand connections through the use of military and non-military means becomes crucial over time to recognise how hostile activities threaten national interests.

Multidimensional deterrence means the ability to deter possible competitors from initiating or continuing their aggression. Deterrence is crucial to ensure the mitigation of possible risks arising from the complexity of the global scenario. Capability and credibility are the main factors that make deterrence fully effective.

Capability is linked to the availability of appropriate tools and procedures to disrupt an aggressive action and respond to the aggression itself, including in the cyber and space domains and the information environment. Credibility, on the other hand, is linked to the actual capacity and willingness to respond to an aggression and to develop a coherent and effective strategic narrative through the use of the different instruments of national power. In this perspective, actions to maintain the capacity to act independently through collaborative resilience¹⁵ as the first line of defence can also contribute to deterrence.

Decision-making agility. The complexity and volatility of threats and the very rapid evolution of the situation mean that decision-making time is significantly compressed. Tools and procedures will be needed to ensure decision-making agility at all levels in order to take quick decisions adapted to the continuously evolving situation within an overall strategy.

¹⁵ Resilience of international organisations to be assessed by recognising and quantifying the dependence of military forces on critical national services and infrastructures and how any critical issues and/or inefficiencies may affect the conduct of military operations.

2.4 THE NATIONAL SECURITY STRATEGY AND THE ROLE OF DEFENCE

The evolution of the threat requires a new reference model where the military is one of the elements of the National Security Strategy, which indicates the strategic priorities for the country.

All instruments of national power – notably diplomatic, informational, military and economic – will contribute to create the model, with the further participation of all those who are indispensable to define its essential elements and any descendant action. Such priorities must reflect the definition and categorisation of national interests (hierarchisation and geographical anchoring). This is how objectives can be identified and the military instrument correctly characterised.

This exercise will guide the transformation of the security and defence system and provide the right evolutionary cue to adapt to the changed context. "*The national military instrument can, in this sense, represent both a significant amplifier of power and a lever among those of national power (Diplomatic, Information, Military and Economic). It can be decisive in opening up spaces of manoeuvre useful for the achievement of specific national interests within the broader country system*"¹⁶.

The definition of a National Security Strategy is also indispensable to identify those sectors of emerging and disruptive technologies in which the Ministry of Defence should invest and commit resources, especially if no other state institutions have invested in them. There is no doubt, however, that the military instrument must be characterised by technological superiority and must be multidomain in nature. This means having the military capability to achieve windows of superiority in every domain, including space and cyber. Superiority should not be all-encompassing, but appropriate to defend vital, strategic, or even contingent national interests that the National Security Strategy will have identified.

¹⁶ The Chief of Defence's Strategic Concept – 2020 ed., page 15.

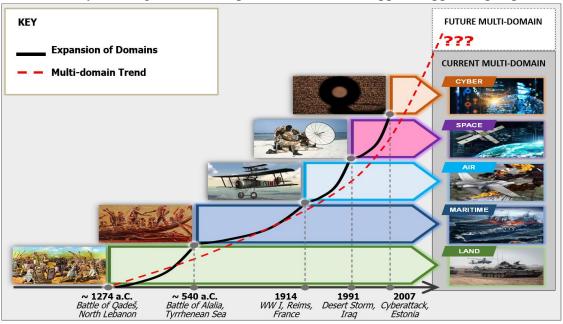
3.1 DEFENCE ORGANISATION ACROSS DOMAINS

The need to synchronise military activities in all domains requires first and foremost an assessment of the current defence organisation and the definition of possible adaptations to best meet future challenges in multi-domain operations.

The traditional land, maritime and air domains have consolidated independently of each other on the basis of the historical physical opposition between opponents, as it is typical in classic warfare. They predominantly hinge on the centrality of the components operating in the target environment, i.e. Army and Carabinieri for the land environment, Navy for the maritime environment and Air Force in the air. However, the technological evolution in military operations over time, together with the increasing expansion of classical environments, have also influenced the configuration of the individual components. With a view to agility and operational autonomy, they have developed capabilities that enable them to operate beyond the 'classical' domains.

Military confrontation in such domains is characterised by physical opposition with a clear manifestation of widespread violence and regulated by the law of war (*ius ad bello* and *ius in bello*). These are universally recognised and accepted principles, to which are added certain general principles within customary law applicable to everyone.

For the conduct of military operations in the classical domains, Defence had set up the Joint Operations Headquarters (JOHQ) under the Chief of Defence. It performed the functions of planning and directing operations, as well as joint and multinational exercises. In addition, it ensured the necessary liaison with the Services' Component Commands by defining tasks and responsibilities from a support-supported perspective.



On the other hand, the recognition of the new domains - first Cyber and then Space - has occurred much more recently. They are characterised by a high rate of technological development, by the pervasiveness and transversal nature of their effects, and by the presence of a growing number of state and non-state public and private actors that can achieve strategic effects without any obvious manifestation of violence or without being identified.

The absence, to date, of a recognised international legal framework and the different stances taken by the competitors in the international arena in the new domains have highlighted the need to rethink the way of addressing confrontation in the military dimension and to develop new capabilities and methodologies to respond to the new challenges.

In this perspective, and it light of the trends that have marked the historical and technological evolution of the domains, we may assume that the introduction of further technological innovations, even disruptive ones, and the innovative use of consolidated capabilities will contribute to the identification and definition of new domains of operations.

In order to adapt to this new context, Defence has decided to adapt its structure by creating inter-force organisational units and maintaining responsibility for the two new domains at a central level. In particular:

- <u>for the cyber domain</u>, the Joint Cyber Operations Command (CIOC) was initially set up and later merged into the Network Operations Command (*Italian: Comando per le Operazioni in Rete*, COR). The COR is responsible for carrying out operations in cyberspace. Furthermore, it opposes and neutralises any possible cyber threat and/or enemy action brought to Defence networks, systems, and services - both classified and unclassified - as well as to Defence critical infrastructures.
- for the Space domain: in line with the evolution of this domain in NATO¹⁷ and national¹⁸ frameworks, the Space Operations Command (Italian: Comando per le Operazioni Spaziali, COS) was established in June 2020 to enhance the national capability to operate in space, and to protect and defend the national space infrastructure while effectively integrating space into joint operations.

The COS is the interface for space operations, both within Defence and in the interministerial and international frameworks, without prejudice to technical-military intelligence tasks performed by Information and Security Division (*Italian: Reparto Informazioni e Sicurezza*, RIS) of the Defence General Staff.

However, while we have acquired specific knowledge and skills thanks to the establishment of specific Commands for operations in the new domains, the real ability

^{17 &}quot;Overarching NATO Space Policy", 2019 ed. And recognition of space as fifth operational domain.

¹⁸ In Italy, pursuant to Law 7/2018 (Measures for the coordination of space and aerospace policy and provisions concerning the organisation and functioning of the Italian Space Agency), the Italian governance of space was reorganised under the high direction of the President of the Council of Ministers. The Inter-ministerial Committee for Space Policies and Aerospace Research (Italian: Comitato Interministeriale per le politiche relative allo spazio e alla ricerca aerospaziale, COMINT) was assigned a guidance and policy-making role. Within this framework, the "Government's guidelines on space and aerospace", the "National Security Strategy for Space" and the "National Space Policy Strategy Paper" were approved in 2019.

to operate in cyberspace and space requires further action, as the capabilities reside in the individual Armed Forces.

The need to operate in the multi-domain context implies the need to fully integrate the new domains in the conduct of military operations by synchronising the actions and effects that can be generated.

Therefore, on the basis of the powers of the Chief of Defence Staff and given the evolution of the current geo-strategic scenario, Defence requires an increasingly joint and multi-domain transformation. This translates into the evolution of the JOHQ into a structure that, while maintaining the same name in English, is intended to conduct complex joint and/or multinational and multi-domain military campaigns across the entire spectrum of operations, while guaranteeing unity of command.

3.2 MULTI-DOMAIN OPERATIONS (MDO)

Framing MDOs and understanding their true scope in terms of transformation needs requires first of all understanding the paradigm shift from traditional joint operations. The latter are based on the need to achieve superiority in the respective domains of competence through the capabilities of the individual components to operate in a coordinated manner. Thus, while aiming at a certain degree of interoperability, individual components are entrusted with the conduct of activities in their own environment, with a clear demarcation between domains that are generally considered to be contiguous.

Instead, MDOs are based on the awareness that it is not possible to maintain supremacy in all domains over a peer competitor. Therefore, their goal is to maintain freedom of action in all domains in order to exploit any windows of opportunity through the convergence of effects to be achieved by synchronising cross-domain actions. In particular, MDOs envisage, if necessary, the development of autonomous actions limited in time and space by a single component to create a window of opportunity for the benefit of the other components.

The multi-domain approach thus reworks operations in multiple domains in an innovative way. It seeks to create effects by combining different capabilities and starting from the assumption that the context of reference must be understood as a single entity. This is on the grounds that:

- The unique characteristics of each domain influence the forces, capabilities, personnel and weapon systems operating in it. In particular, the three classical domains i.e. land, sea and air are de facto associated with the individual components. This has led, over time, to the consolidation of a conceptual separation that in fact risks not facilitating the conduct of MDOs;
- there is a transversal relationship between cyber, space and the other domains/environments, in that
 - space represents a domain in which discrete activities are developed that have a constant relationship with the other physical domains. Among these is space control, which has strategic value and involves high stakes in terms of deterrence;

- activities in/through the cyber domain and the electromagnetic environment are intended to ensure an operational advantage by inhibiting and/or degrading the adversary's use of the electromagnetic spectrum and cyberspace. They are enabling and transversal to the other domains due to the spread of digital technology and the difficulty of threat detection;
- the information environment i.e. the place where information is received, transformed, processed and transmitted - is characterised by great complexity and dynamism. It extends beyond the physical boundaries of the crisis/conflict area and involves all the national and transnational elements capable of producing effects in the PMESII spectrum.
- there is a stronger engagement in increasingly contested areas, such as, for example, densely urbanised areas. In perspective, this also involves so-called coastal megacities, where military actions must be able to influence¹⁹ the operational environment and actors therein. In such contexts, all factors that contribute to the complexity of the operational environment are compressed into a limited geographical area with a very high density of civilians. Therefore, effects in the physical dimension such as the destruction caused by classical combat can have exponential effects on the cognitive dimension.

We have outlined the essential elements of MDOs; we can now frame them on a conceptual level and define their main characteristics and novel elements.

3.2.1 Conceptual Framework

Within NATO, there is no agreed definition of Multi-Domain Operations to date, although the Allied Command for Transformation (ACT) has been tasked with developing the topic within the Warfare Development Imperatives descending from the NATO Warfighting Capstone Concept. An initial MDO Concept should be ready by 2022. The current draft definition²⁰ briefly describes MDOs as:

Orchestrate and synchronize military and non-military activities across all domains and environment that enable Commanders to deliver converging effects

From an Italian perspective, this definition can be expanded as follows:

Military activities conducted across multiple domains to perceive, understand and act on converging effects aimed at generating multiple dilemmas at such a speed as to overcome the adversary's decisionmaking capacity. Activities are conducted by synchronising military actions with other instruments of national power and/or with allies and

¹⁹ Influence is to be understood as the ability to directly influence the will of the adversary (or potential adversary), in order to change its 'behaviour' in the desired manner, at every level of operations management (tactical, operational and strategic), i.e. mutually supporting each other, in relation to the desired effects.

²⁰ From the outcomes of the Alliance Warfare Development Conference (AWDC) 2021 (7-9 December 2021), an annual event organised by NATO's Allied Command Transformation (ACT), which brings together the Flag Officer General Officers (FOGOs) and Decision Makers responsible for the transformation of NATO and Partner countries. The conference directs future efforts and discusses topics of particular interest related to innovation and transformation of the armed forces of NATO and Partner Countries.

partners, under a synchronised command and control structure (socalled Multi-Domain Command & Control, MDC2).

Therefore, in keeping with the strategic/political national and NATO guidelines and decisions, multi-domain operations can be conducted across the entire competition continuum and in all phases of the campaign. The multi-domain approach must be constantly maintained in the consideration that the competition continuum is a constant and fluid alternation of phases. To different degrees and at different times, it moves from confrontation to conflict through crises. In this context, since the threshold concept itself is intangible outside the classical physical dimension, it will be necessary to promote an international regulation of the new domains and at the same time develop capacities, procedures and methodologies suitable to exploit the potential of the new domains.

3.2.2 Perceive, Understand, and Orchestrate

In MDOs, the decision-making cycle of military operations known as Observe, Orient, Decide and Act (OODA loop) is complemented by 'Sense', 'Understand' and 'Orchestrate'. It extends beyond the military context to include predominantly nonmilitary aspects through the involvement of other national and international, public and private actors. The scope of change necessarily requires a revision of the balance of functions in the consideration that superiority over a potential competitor can be achieved by perceiving and understanding the opponent better to maintain a certain freedom of manoeuvre. In fact, through greater understanding one can orchestrate effects and create multiple dilemmas to the opponent at a higher rate than the adversary will be able to cope with and solve. In more detail:

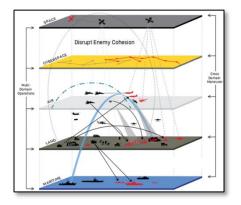
Sense is the preparatory function for understanding. In MDOs, it is extended beyond military surveillance systems alone; it also takes into account national or multinational civil and commercial capabilities, so that through surveillance, discovery, classification, recognition, tracking and identification activities, data useful for the intelligence cycle can be collected and help generate understanding. This requires the availability of a wide range of sensors in all domains, physical and virtual, covering both the electromagnetic spectrum and the information environment in order to understand the behaviour and attitude of all actors involved.

In addition, depending on the evolving situation and the course of the competition, through proactive sensors capable of fulfilling the actuator function (every sensor is a shooter, every shooter is a sensor), one can probe and, at the same time, promptly and actively stimulate an appropriate response. In particular, this could be achieved through the use of automated and/or autonomous systems and platforms.

Understand is the function performed by interpreting the information gathered through the Sense phase. It aims at framing the situation in its context and making *assessments* (why something has happened or is happening) and *predictions* (identifying and anticipating what might happen). Both are useful to support quick and effective decision-making. In MDOs, understanding must focus on the operational environment in order to understand its characteristics, actors, relationships and predict how it may evolve as a result of different interactions. The effort should focus on potential adversaries, how they operate in the domains and the electromagnetic spectrum, and how they exploit the information environment to influence the actors present. In this perspective, knowledge-sharing between the different levels and actors of the international community is imperative in order to increase the degree of synergy and orchestrate appropriate responses by assessing risks, benefits, vulnerabilities and strengths to achieve objectives. Assessments will reveal possible windows of opportunity to compete successfully in a domain deemed significant and to integrate available capabilities by reshaping the deployed assets.

Orchestrate is the function that encompasses the integrated planning and execution of actions and activities to achieve set goals. It is based on the continuous effectiveness of the perceive and understand functions and allows multi-domain operations to be conducted flexibly, while taking into account the actual effects achieved, rather than the assumed or desired effects. In this context, the orchestrate function must be ensured by a resilient structure that is able to guarantee its efficiency and effectiveness even when the environment becomes contested and/or degraded. In this situation, it may prove particularly challenging to obtain a clear picture of the operational situation.

3.2.3 Cross-Domain Actions and Synchronisation of Effects



Cross-Domain actions represent the integrated combination of military and non-military capabilities in different domains aimed at exploiting a limited window of superiority and engaging the opponent in the physical, cognitive and/or virtual dimensions.

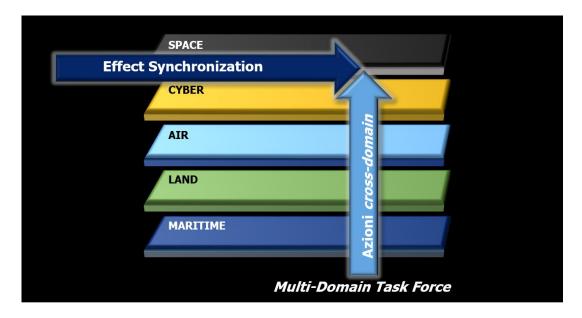
To ensure the achievement of strategic objectives, cross-domain actions necessarily presuppose the synchronisation of effects at different levels (strategic, operational and

tactical) and the synergetic deployment of capabilities (kinetic and non-kinetic) across domains and electromagnetic and information environments. Therefore, the purpose of cross-domain actions is to create integrated effects in the physical, virtual and cognitive dimensions and saturate the opponent.

Effect synchronisation, on the other hand, concerns the integration of activities/events over time to achieve a favourable operational tempo²¹ with respect to what a potential opponent has developed. Therefore, synchronisation refers not only to the coordination of military activities at the tactical, operational and strategic levels, but

²¹ The speed and intensity of a party's actions in relation to the speed and intensity of other events occurring in the operational environment.

also to the necessary integration with the activities underlying the other instruments of national power in a given time interval.



In this framework, cross-domain actions must therefore be developed at all levels (strategic, operational and tactical) and within a single strategic design by multidomain military formations to operate in the competition continuum, shape the operational environment, deter adversaries and - as the competition intensifies - fight and/or neutralise the threat and return to a situation of strategic advantage.

Instead, the synchronisation of effects goes back to the strategic-military level, which through greater integration at the national and international governmental level can configure and, if necessary, adapt the strategic design of the campaign in which the cross-domain operations of the individual Services are developed.

Therefore, the force generation process²² of a Multi-Domain Task Force will necessarily take into account the need to provide individual multi-domain formations with all the capabilities required to operate in multiple domains and generate effects in all dimensions. Special attention will have to be paid to capabilities for the cyber and space domains. Given their cross-domain nature, and with respect to the specific Service competences, they will have to be carefully proportioned in order to

- decentralise capability packages to the individual multi-domain formations to guarantee their operational autonomy and possible cross-domain actions;
- centralise strategic capabilities under the direction of the Network Operations Command and Space Operations Command, which will dispose of and deploy them in line with the strategic design and synchronisation requirements.

²² A process of establishing a military contingent by defining the capabilities and assets for the conduct of a military operation. At the multinational level, this process takes place through the conduct of Force Generation Conferences during which nations offer capabilities and assets that they pledge to make available within the coalition.

The national chain of command and control for Multi-Domain Command & Control (MDC2) operations must be defined a priori. In this chain, the necessary command and control relationships and delegations for the decentralised conduct of cross-domain actions and synchronisation of effects must be identified.

3.2.4 Multi-Domain Command & Control (MDC2)

Operational situations can evolve in an extremely dynamic and complex manner. This requires the most up-to-date situational data possible and the ability to speed up decision-making processes in order to make decisions in an agile and timely manner. Therefore, the enhancement of the existing JOHQ by means of a 'joint direction' becomes particularly important: this is the case with the **Joint Operations Centre** (**JOC**)²³. It would operate within a whole-of-government approach and exploit up-to-date technologies, connectivity and processes for situational awareness and the streamlining of planning and conduct processes. The JOC can be

- the point of convergence of all information of strategic, operational and tactical value coming from the areas of operations where Italian military contingents are deployed;
- the linking element with the other ministries and actors involved.

The need to transform the JOHQ organisation into the current one arose precisely from the need to strengthen, in terms of uniqueness and speed, the operational Command and Control (C2) function and to provide the Chief of Defence Staff²⁴ with a much better tool to plan and conduct operations from a joint, interagency and/or multi-domain perspective in cooperation with the Civil Authorities. This is thanks to increased situational awareness related to the five domains (land, maritime, air, cyber and space²⁵) and to the information environment (so-called Multi-Domain Common Picture).

In this respect, the JOC Project is the pivot for the functional review of the JOHQ and the introduction of new technological solutions concerning

- situational awareness, with the Joint Common Operational Picture (JCOP²⁶) serving as an example;
- the streamlining of planning and conduct processes²⁷;
- new technologies for deliverables and document management and the monitoring of typical operational level functions²⁸.

²³ It is part of the organic-functional review and transformation of the JOHQ, the so-called Functional Review.

²⁴ As well as the JOHQ Commander in the functions of Joint Force Commander (JFORCOM) or Multinational Operation Commander (MNOCOM).

²⁵ In the awareness that cyber and space are domains that necessarily require new capabilities to be developed and acquired.

²⁶ An integrated and current representation of ongoing operations for all components/domains (Ground, Maritime, Air, Cyber, Space) and each of the functional areas from J1 to J9 for use by the Operations Commander and the various decision-making levels. This information is associated with information layers called Domain Pictures (DPs).

²⁷ For example: FAS (Functional Area Service) tools, Core Services, augmented connectivity, tools enabling assessment and evaluation (Campaign-Operational-Tactical) and the execution of the Joint Operations Planning Process (JOPP).

²⁸ Such as: Information Knowledge Management (IKM) and the info cloud dashboard.

In particular, the evolution of the JOC will have to take place through the implementation of products that are already available in the national and NATO. Through a step-by-step adaptation process, an info-structure will be created characterised by flexibility and multi-domain and a multi-level information collection point meeting the most advanced security standards and that can interact with NATO, EU and Coalition networks. Therefore, standardisation requirements will have to ensure

- interoperability with the systems of the different Defence and Allied components, as well as with other national ministries. The latter include those for crisis management in national and extra-national contexts (among others and primarily, the Ministry of the Interior and the Ministry of Foreign Affairs and International Cooperation);
- interchangeability of newly acquired or modernised systems with those already available at the Services.

Moreover, depending on the evolution of the situation and the emergence of any crisis or conflict situations, the JOC may be re-configured based on the operational situation.

3.3 NATIONAL INTEGRATION IN MANAGING NEW DOMAINS

The desire for integration and interoperability of the military and civil components is not supported by a shared international legal framework. As a result, there is a risk that some competitors may continue to maintain an aggressive attitude in the new cyber and space domains, i.e. in the information environment. By keeping their actions below the threshold of open aggression, these competitors could thus acquire a position of strategic advantage (strategic asymmetry) over Western democracies and, in particular, our country.

The ability to promptly 'sense' the variations occurring in the system and 'understand' how these can be incorporated into a single Grand Strategy requires a common approach and robust information sharing, both nationally and internationally, with the involvement of all the institutional, governmental, public and private actors. This would allow a careful assessment of the vulnerabilities of the national system as a whole and the possibility of taking the necessary mitigation measures.

The growing relevance of competition in the new cyber and space domains and in the information and electromagnetic environments highlight disruptive potentials, which open spaces of opportunity, but also significant risks.

Therefore, in view of their rapid and growing evolution, also due to their intrinsic capacity to generate strategic effects, one must first of all understand that cyber and space will increasingly take on a decisive role in the management of competition, including military competition, to the point of equalling and, on some occasions, even exceeding the relevance of the classical domains.

The recent approval of Decree Law no. 82 of 14 June 2021, by which the National Cybersecurity Agency (NCA) was established, represents a significant growth opportunity for the country system in the cyber domain. Within this, however, the needs of Defence and the contribution of the military instrument to protect national interests must necessarily be grafted. Therefore, it becomes of paramount importance to

revisit/integrate the national regulatory framework to move away from the current reactive cyberdefence-centric approach and create an effective proactive response capability focused on sovereign cyber effects effectiveness (*Sovereign Cyber Effects Provided Voluntarily by Allies*, or SCEPVA²⁹) and the conduct of cyber defence operations (CDO) within a broader multi-domain framework.

Likewise, the establishment of the Inter-Ministerial Committee for Space and Aerospace Research Policies (Italian: *Comitato Interministeriale per le politiche relative allo Spazio e alla ricerca aerospaziale*, COMINT) represents an important step forward for the growth of the country system in this domain. The role of the COMINT must in fact be understood both as an inter-ministerial board where the security and defence aspects of national assets can be addressed, and as a policy and investment tool in the sector. Also in this context, the needs and the contribution that Defence can guarantee to protect national interests will have to be appropriately conveyed and enhanced.

Therefore, in order to ensure its primary Defence function and full interoperability within the relevant international organisations, Italy will have to adopt a common and shared national approach that will allow investments and the definition of wide-ranging innovative policies, regulations and procedures. All of the above will enable Defence to develop capabilities to operate effectively in the new forms of confrontation and contribute to an active role in the competition continuum.

²⁹ Sovereign Cyber Effects Provided Voluntarily by Allies: an Atlantic Alliance mechanism that allows NATO to conduct offensive and defensive operations and produce effects in and across the cyber domain using Alliance networks and systems and/or authorised others. – NATO AJP-3.20 "Allied Joint Doctrine for Cyberspace Operations".

CONCLUSIONS GUIDELINES

MULTI-DOMAIN: A NEW PARADIGM

Preparing to face the future challenges posed by the evolution of the international multidomain scenario requires a profound conceptual, cultural and management paradigm shift capable of developing a distinctly multi-dimensional response. It is a reality perceived by many, but understood by few, especially in terms of the potential to strike at the heart of the country system without us being able to clearly identify the origin of the threat. The full integration of different civilian and military actors (so-called wholeof-government and whole-of-society approach) at the international, national, intergovernmental and interagency levels must therefore be achieved.



The starting point of a **new paradigm for multi-domain operations** is a **unified and shared national strategic vision** to unequivocally delimit the political, economic and legal perimeter within which such operations can be conducted and clearly identify the areas of national interest to be safeguarded.

Furthermore, there is a strong need for **a body at the central government level that defines the National Security Strategy** and coordinates, integrates and synchronises the instruments of national power (diplomatic, informative, military and economic) for crisis management and international competition in a multi-domain context. At the operational level, on the other hand, we need to define the optimal configuration of a **Command and Control model** that goes beyond the logic of sectorial competence, gives coherence to the information provided by peripheral sensors, and integrates the different situations on the ground into a single, coherent and updated general picture - also known as Multi-Domain Common Picture – which decision makers can use as a basis.

A further cornerstone of multi-domain operations will be the **continuous search for integration and interoperability** between systems, processes and actors involved in the domains at the national, international and supranational levels.

Finally, it will be crucial to define the new role of the **human dimension** given the evolution of its relationship with emerging technologies, especially artificial intelligence. Renewing the process of selecting, training and improving human capital will be crucial. This process will have to be geared towards both the development of technical and specialised skills and the education of leaders to deal with different realities and to employ new tools.

Within this framework, the Italian Ministry of Defence intends to promote a collective debate on possible general guidelines for a national approach to multi-domain operations, as well as Defence guidelines to define the main needs for transformation and innovation of the military instrument.

GENERAL GUIDELINES

Defining the elements that will be decisive for the development of a **national approach to multi-domain operations** requires the initiation of an intra-governmental dialogue to analyse potential vulnerabilities, identify the best solutions, adopt the necessary organisational adjustments and define competencies. The following general, though not exhaustive, guidelines have been drafted, aimed at developing awareness of new threats, capacity for analysis and synthesis, and proactive rather than reactive decision-making speed:

Promoting the National Security Culture

The starting point lies in the promotion of a National Security Culture that educates and informs society - from leaders to individual citizens - on the possible threats to the country's interests and, at the same time, on the plans and actions defined within a single National Security Strategy. In a complex system, in which the new forms of threat can strike at the intimate and private sphere of individuals, companies, society and institutions, the weakness of a single link in this complex chain between public and private actors can lead to a breach in the broader national security perimeter.

The distance between government and civil society in Italy could make the information environment a vulnerable element of the Italian defence strategy, especially in light of the level of sophistication achieved in this area by competitors. Controlling the information environment may, in fact, be particularly problematic for Western democracies. It will be necessary to be able to rely on the entire population to recognise threats in the information environment. In this sense, reinvigorating a national society that is mistrustful and not very cohesive while revitalising the social contract through the development of ad hoc strategies is crucial to ensure a resilient country system.

It is therefore important to structurally intervene in <u>information and training courses</u> at every level that deal with national security and defence. They should be enhanced as a specific subject area by developing a common language between institutions and

citizens. The soft power approach will be aimed at strengthening the sense of belonging and national identity.

Specific attention in this process of cultural growth must then be paid to the training of strategic leadership to adapt the speed, comprehensiveness and effectiveness of decision-making to the new context of multidimensional confrontation.

This new approach to security must then spur an in-depth and courageous debate to redefine the current ethical-political-legal framework in order to adequately address the new scenarios, especially the technological one. This will create the capacity to respond rapidly to crisis situations and implement tools and methodologies suited to the needs of the new challenges.

> Developing Integrated Multi-Domain Security

Extending international competition to the new cyber and space domains also means extending the concept of battle space and highlighting the need to evolve the concept of security and defence beyond the physical and/or geographical dimension alone. All of the above is necessary to protect tangible and intangible, physical and virtual national interests wherever they may be, including through a proactive and preventive posture. It follows that the defence of space assets and networks requires additional critical functions beyond the traditional ones to ensure the continuity of essential strategic services and the protection of national interests. The rapid evolution of the new domains and the possibility of an escalation of competition, including military competition, require innovative policies to avoid inefficiencies and delays both in terms of fragmentation of competences and deployment of resources, which are a significant element in economic terms that must be taken into account. It is necessary to develop an integrated multi-domain security in which to review, particularly for the new domains, the competences assigned to the various ministries, as well as to ensure unity of direction and continuity of funding through additional resources to develop credible capabilities. Likewise, depending on the choices to be made, it is necessary to identify national and international thresholds beyond which the corresponding national reaction is authorised through a system of predefined delegations. This would create incremental response options in all domains and instruments of national power (so-called Multi-Domain Escalation Management Options).

> Developing a Multi-Dimensional National Deterrence Approach

According to the current concept of deterrence, a potential aggressor is convinced that the consequences of coercion or armed conflict would outweigh the potential gains. This is done by maintaining a credible military capability and a strategy with a clear political will to act. Applying this concept to the evolving international geopolitical scenario with a multi-domain approach, the need to develop a <u>national deterrence approach</u> based on credible military capabilities in all domains to complement current conventional capabilities, which are still crucial, is evident. The reference is to new military capabilities to operate in the new cyber and space domains, as well as in the information and electromagnetic environment. Furthermore, through the definition of national interests and the overcoming of the threshold concept to authorise a military intervention, it will also be possible to

develop a <u>communication strategy geared towards supporting a preventive</u> <u>intervention</u> with all the instruments of national power, including military power. The effectiveness of the above cannot be separated from an <u>appropriate mindset of the</u> <u>leadership</u>, which must be trained and educated to use all the capabilities at its disposal so that the national approach and posture can be coherent.

> Building a Digital Backbone

The perception of what is happening in the physical and virtual domains depends on the availability of a vast network of sensors that also cover the electromagnetic and information environments. The sensor network allows for an understanding of the behaviour and attitude of all actors involved. The ability to collect, analyse, transmit, merge and distribute large amounts of data requires a distributed, scalable and redundant communication platform. It will have to be originally designed and developed to ensure protection from potential attacks or possible data manipulation; to allow for the continuity of essential services such as PNT satellite radio navigation; and to enable the dissemination of information according to multi-level security. Furthermore, the platform will have to exploit advanced technological solutions to achieve real information and cognitive superiority and use standardised protocols in the incremental deployment of new sensors and actuators - or their immediate replacement with state-of-the-art solutions - and the extension of the network to an increasing number of actors.

The creation of this digital backbone, extended and integrated among all the instruments of the National Power, will allow the full sharing of information, the development of common processes and procedures and the support of national decision-making to ensure the synchronisation of effects. Specifically, this structure is crucial for Defence in ensuring the "sense" function and generating a full and shared Multi-Domain Common Picture.

Accelerating the Innovation Process

The development and implementation of new technological solutions are enabling elements for the conduct of multi-domain activities. The ruthlessness with which some actors adopt new technological solutions to achieve their own particular interests by exploiting the regulatory gaps in international law contributes to exacerbating the possible technology gap to the detriment of Western countries. In order to reverse this trend, we must initiate a process of strong acceleration of technological innovation, including at home. We will have to develop new models to enable more streamlined forms of collaboration between the public and private sectors. From this collaboration, we will be able to develop and implement new technological solutions on which basis we can also model the evolution of the regulatory framework, if necessary. More generally, it is necessary to promote a culture of innovation to enable all organisational and decision-making levels to fully grasp the challenges, but above all the opportunities offered by emerging and disruptive technologies.

DEFENCE GUIDELINES

Success in multi-domain operations depends on the integration of all factors, namely instruments of power, constant technological development and available capabilities, and the ability to intercept national security threats. The concept of multi-domain operations therefore expands upon the current military doctrine of joint operations. It is based on the synergy of a coordinated development of operations conducted in the conventional domains, the cyber and space domains, the information and electromagnetic environments, and the ability to generate effects in the physical, virtual and cognitive dimensions. It is quite obvious that the seamless integration of all the elements in the field is almost impossible to achieve due to the various political, economic, and operational constraints, the timing of resource utilisation, and so on. It follows that simultaneous utilisation of all available resources is impossible, but multi-domain synchronisation is necessary to maintain the strategic advantage and initiative over the opponent.

Hence, there is a need for the current concept of joint and combined operations to evolve into a new, non-linear, non-compartmentalised cross-domain paradigm, due in part to the extraordinary evolution of technologies applied to decision-making processes, sensors and weapon systems.

The first objective will be to **train and educate current and future military leadership** and create a sound mindset for understanding and managing all domains. We will have to create the vision and will to act on the basis of an objective, open and creative approach and achieve the required result at an acceptable cost. Leaders will have to be able to manage a situation full of dynamic interactions and anticipations that pose fundamental problems for any strategic doctrine or theory.

Equally crucial is the development of **new force preparation models** to meet the challenges imposed by MDOs. The integration and interoperability between systems and actors (not only military) necessary to prepare the military to operate effectively in the multi-domain environment will be achieved by training individuals and units of all Services at every level in a multi-dimensional perspective. At the same time, simulated training scenarios and targeted exercises in a joint environment will be prepared.

The **way we plan**, achieve and measure the effects will have to be adjusted, as will the definition of the objectives that contribute to them. Therefore, conceptual and executive design (Operation Design and Plans, respectively) will change.

A **new national regulatory framework** will have to be developed that can give greater impetus to the activities described above by implementing integration at inter-force level to a greater extent than now. It will enable the military to operate synchronously in different physical and virtual contexts and with short notice. Within the alliances to which our country belongs, it is also important to play a leading role in the evolution of organisations, to achieve regulatory and, consequently, doctrinal unity and to ensure consistency of terminology and unity of purpose in countering threats in the competition continuum.

An effective response to threats in a multi-domain environment requires strong integration to synchronise effects and define a synchronised chain of command and

control for the purpose of unity of command. Where necessary, delegation and extensive decision-making autonomy of lower levels can be used. For Defence, the evolution of the Joint Operations Headquarters and the implementation of the JOC project will bring the necessary synthesising capability to develop a **Multi-Domain Common Picture** based on the sharing of concepts and the integration of the systems of the Component Commands and their respective Operations Centres. The Multi-Domain Common Picture alone is, however, of little significance if not contextualised and integrated into the Command and Control processes and battlespace management. It will therefore be necessary to create a synchronisation matrix that, through new technologies, can relate the domains, capabilities, vulnerabilities and opportunities to be exploited with cost-effectiveness.

The need to prevent and manage the escalation of competition, and to influence the environment and the actors operating in it, requires a national approach for an integrated and, where necessary, preventive use of all capabilities that can contribute to generating lasting effects in the cognitive dimension. The trend in multi-domain operations is one of increasing and decreasing competition, which differs substantially from the linear escalation model. Therefore, Defence will have to develop an approach to employ all **its kinetic and non-kinetic capabilities** in an integrated manner so as to contribute to the national strategy by enhancing its non-kinetic capabilities to generate effects in the cognitive dimension and the information environment.

The capabilities acquired by Defence to date are those of the individual Services. They have been developed with a bottom-up approach, in which the individual components have progressively adopted new tools to guarantee their operational autonomy, generated redundancies and a real internal competition for the acquisition of further capabilities with consequent funding programmes aimed at extending their range. However, the specificity of the new domains and the amount of resources, including financial resources, needed to develop new capabilities **require a top-down approach**. Such an approach would make it possible to rationalise capacities, overcome the current service-specific stovepiping, and define objectives and, consequently, distribute the necessary means. This will not entail, at least in the short term, the establishment of new dedicated forces, but rather the exploitation of existing excellence to overcome single-service logic and develop strategic capabilities to be integrated from the outset at the joint force level.

In the area of **technological development**, Defence must also develop its own innovation accelerator/incubator. Through a close public-private partnership, it will be able to launch, right from the embryonic and conceptual phase, a forward-looking innovation process that can intercept and direct new and unprecedented technological trajectories even before the subsequent research and development phase. One only has to think of the increasing need for distributed sensors/actuators in all domains. This will require large-scale Robotic Autonomous Systems (RAS) to be deployed through swarm intelligence logics and processes, or the need to operate effectively in the electromagnetic environment following the development of offensive capabilities (so-called Directed energy weapons) capable of generating temporary and/or permanent effects and preventing the adversary's use of this environment to access the domains.

The pervasiveness of technology will not, however, replace the predominant position of human beings, who will retain their central role, albeit within new management paradigms. The ever-increasing relevance of the new cyber and space domains and the evolution of competition in both the information and electromagnetic environments will require greater investment in resources, including human resources who, through dedicated training courses and employment profiles that enhance competence, will acquire different and diversified skills. The same people will leave room for autonomous systems and platforms in conventional sectors, thus reducing their presence.

GENERAL

Multi-domain, and more specifically Multi-Domain Operations, are the subject of lively international debate. The initial conceptualisation of the US army-centric model envisaged MDOs as the sole military response to penetrate enemy Anti Access - Area Denial (A2/AD) strategies and defeat a peer opponent/near-peer competitor. In that context, MDOs are understood as an evolution of joint operations to ensure convergence of capabilities in all domains. Other visions have been juxtaposed to this, namely those that seek the integration of military Instruments of Power (MIoP) with other Instruments of Power (IoP). An example is the British approach, with its Joint Concept entitled 'Multi-Domain Integration'. It emphasises the need for integration from the government level and across the entire spectrum of competition at all levels of military operations (strategic, operational and tactical).

THE NATO PERSPECTIVE

The Atlantic Alliance's multi-domain approach goes far beyond simply adding the space and cyber domains to the joint approach, and envisages an integration to gain and maintain the initiative.

This new approach combines actions in all five domains of operations, orchestrates and amplifies the capabilities available to exploit surprise, convergence

and success to generate freedom of manoeuvre in a battlespace that creates effects in the physical, virtual and cognitive dimensions.

The Alliance's multi-domain approach optimises the full range of political, military and civil capabilities and integrates them across the five domains for maximum advantage³⁰. It should also be noted in this regard that the Allied Command for Transformation (ACT) supports different concept development initiatives within the Multinational Capability Development Campaign (MCDC) through the project entitled 'Multi-Domain - a multinational understanding', as well as through the support of the Joint Air Power Competence Centre (NATO Centre of Excellence - CoE) for the development of a project on 'Joint All Domains Operation - JADO'.

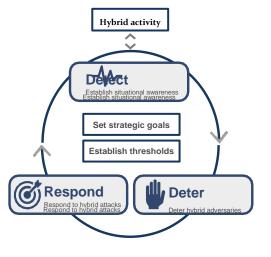


³⁰ AJP-01 Ed. F "Allied Joint Doctrine" (draft).

Moreover, ACT has recently included its multi-domain project in the Lines of Deliveries and, even more so, in the Warfare Development Imperatives of the NATO Warfighting Capstone Concept (NWCC³¹) as a priority requirement and enabler. In doing so, it confirmed the centrality of the need to operate in all domains across the entire spectrum of operations.

EUROPEAN UNION – COUNTER HYBRID

Although not strictly related to the concept of multidomain in the strict sense, the European Union is also addressing the issue of the relationship between the military instrument and other Instruments of Power in the management of international competition against hybrid threats. In particular, through the drafting of its own document entitled 'EU Guidance on countering hybrid threats during the planning phase of EU-led





CSDP military operations and missions' and starting from the conceptual model elaborated by the EU Hybrid CoE³², the EU intends to provide guidance on countering hybrid threats during the planning phase of military operations under the Common Security and Defence Policy - CSDP.

According to European guidance, the first step in countering hybrid threats is to identify the threat and then decide on the most appropriate course of action to take, knowing that the level of ambition cannot be the same for all actors. The forms of response will have to conform to political choices and be adapted to the intensity of the threat, political decisions and the possibility of response, from simple absorption of attacks, to aggressive deterrence and the adoption of more assertive or retaliatory measures to stop the aggression and prevent further attacks.

The model proposed by the EU is based on the definition of common strategic objectives and response thresholds and a framework on a cycle of three different functions: Detect, Deter and Respond, where the first function is permanently active and the other two are activated in accordance with the response thresholds.

³¹ ACT-led concept to identify capability areas from which to develop the military tool of the next 20 years on criteria of multi-domain, interoperability and use of technologically advanced resources.

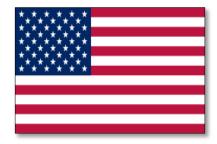
³² Centre of Excellence for Countering Hybrid Threats (Hybrid CoE): established in 2017 in Helsinki by nine founding nations – namely Finland, France, Germany, Latvia, Lithuania, Poland, Sweden, the UK and the US – with the aim of establishing a forum for discussion and cooperation between the EU and NATO to counter hybrid forms of threat. A further 19 countries subsequently joined.

Finally, the EU approach takes into account escalation between instruments of power, where an opponent may escalate its action vertically, by increasing the intensity of one or more instruments of power, or horizontally, by synchronising several instruments of power to create greater effects than vertical escalation alone.

US – JOINT ALL DOMAIN OPERATIONS

The origin of the US conceptual construct is related to the identification of an effective

solution to successfully compete in the strategic operating environment with peer/near-peer competitors (e.g. Russia, China, Iran and North Korea), below and above the threshold. Below the threshold, the centrality of general or tailored deterrence emerges in all its forms, from capacity modernisation to capacity building and pre-positioning of forces.



In above-threshold situations, however, special emphasis is placed on the ability to penetrate and disarticulate enemy A2/AD systems.

In particular, the US Air Force recently published the Air Doctrine Publication entitled 'Department of The Air Force Role in Joint All-Domain Operations (JADO)'. In it, the implications for the use of air power in multi-domain operations are explained, and the US Army has initiated a project in three macro areas summarised as follows:

- conceptual and doctrinal awareness, with the development of a series of conceptual, capability-related and doctrinal documents, primarily for Brigade Combat Team employment;
- creation of dedicated units namely multi-domain task forces (MDTFs) that bring together existing lethal and nonlethal capabilities under one command and integrate and synchronise them across multiple domains to overwhelm a specific target. One MDTF with kinetic and non-kinetic capabilities is already deployed in the Pacific theatre (INDOPAC) and another will be deployed in Stuttgart within EUCOM/AFRICOM.
- testing the ability of a Brigade Combat Team level formation to conceive and conduct an operation in an MDO environment based on the basic assumption expressed above that all formations must be able to fight cross-domain.

Although unchanged in its essence, the idea has been repurposed into a vision called Joint All-Domain Operation (JADO), a model that will guide the capability modernisation process in the medium to long term perspective (beyond 2035).

UK – MULTI-DOMAIN INTEGRATION

Unlike the US approach, which focuses on solving a military problem with military

means, the UK approach extends the scope of Multi-Domain Operations to include inter-ministerial, interagency and multinational environments. This increases the level of 'integration' of military and civil capabilities, the 'synergy' of actions and thus ensures the 'synchronisation' of effects on the opponent's multi-dimensional critical nodes.



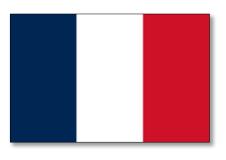
At the moment, the UK, similarly to the US, is also

working on federating capabilities pertaining to the cognitive and virtual dimensions.

FRANCE – MULTIMILIEUX ET MULTICHAMPS (M2MC)

The French approach is based on an awareness of the complexity of the operational environment, which in turn is centred on the recognition of the five NATO domains

(*milieux*) to which are added two further fields of action (*champs*), electromagnetic and informational, which allow one to operate to generate effects. Such complexity requires a profound paradigm shift in the management of operations through enhanced cooperation between components. In particular, the French approach is based on a well-established national strategy in which the contribution of the



military instrument is ensured through the pre-positioning of forces in areas of strategic interest, as part of a national strategy of advanced presence.

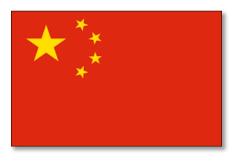
RUSSIAN FEDERATION - REFLEXIVE CONTROL

The vision of the Russian Federation can generally be traced back to the concept of 'reflexive control'. Developed historically through different periods of the 20th century, reaction control is a product of a Marxist-Leninist paradigm. According to this paradigm "cognition results from the reflection of the material world in the human mind, which determines social consciousness. Man's intelligence and cognitive processes depend on his sensory awareness of the outside world, which in turn determines the content and dimensions of his consciousness'.³³

The strategy of 'reflexive control', applicable against human decision-makers as well as computer systems, is defined as a means of inducing a collaborator or an adversary to voluntarily take a decision desired by the initiator of the action, by conveying ad hoc packaged information to him. In this context, the techniques used in reflexive control

³³ Nicola CRISTADORO (2018) "La dottrina Gerasimov e la filosofia della guerra non convenzionale nella strategia russa contemporanea", Libellula Editions.

can be intimidation, flattery, misinformation, deception, dissimulation that aim at disrupting the adversary's decision-making process and reducing the time available for the adoption of effective corrective measures. It follows that in order to achieve its effectiveness, the strategy requires an indepth study of the most 'intimate' nature of the adversary and his thinking and a set of concepts, knowledge, ideas and experience.



Against this backdrop is the Gerasimov doctrine, which envisages attacking the adversary economically, cognitively and physically by making extensive use of unconventional procedures, through a correlation of non-military and military instruments in the ratio of 4 to 1. The non-military tools that the doctrine identifies include efforts to condition adversary political, economic and social components through subversion, espionage and propaganda, combined with cyberattacks that, with their capabilities and increasingly sophisticated tools at their disposal, represent the vanguard of information warfare. Belonging to the cyber domain is the tool of 'white', 'black' or 'grey' propaganda. It can devastatingly affect the nerve centres of a state's economy, society, and politics through the compromise or neutralisation of computer networks. With such an approach, the role of non-military means to achieve political and strategic ends grows. They also exceed the power of force of arms in effectiveness. The key to practical conflict methods has shifted in the direction of a broad use of political, economic, media, humanitarian - and other non-military - measures implemented in coordination with potential popular discontent. The overt use of force is reserved only for the achievement of ultimate success in the conflict.

CHINA – THE DOCTRINE OF THE THREE WARFARES

The goal of the People's Republic of China's (PRC) grand strategy is far-reaching and often looks several decades into the future. China aspires to become a 'modern socialist country' by 2049³⁴. To do so, the Chinese establishment believes it must transform the People's Liberation Army (PLA) into a 'world-class' armed force by the middle of the 21st century. Over the previous decade, Chinese doctrine has produced some important concepts in this respect. They offer a clear idea of the vision of the conflict, but also of the realistic Chinese military ambitions and capabilities. The concept of 'advanced defence', for instance, refers not only to the need to move the first line of defence away from home territory, but also to 'support an omni-directional expansion of national

³⁴ Xi Jinping, 2017. 'Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era'. Political report presented at the 19th National Congress of the Communist Party of China, 18 October. http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf

interests'.³⁵ With the expression 'strategic space', the military doctrine identifies areas that it 'would like to influence with the military, but not through combat operations'.

Of particular relevance is the concept of 'effective control', an expression that reveals China's awareness of how its 'capabilities' for military action abroad are still limited. This concept complements the better known 'active defence', which refers to adherence to the principles of '*defence, self-defence, reactive attack*', and '*we will not attack unless we are attacked, but we will certainly counter-attack if we are attacked*'³⁶. In addition, the Chinese government believes that 'strategies centred on kinetic confrontation' can lead to 'unwinnable wars'.³⁷

These doctrinal elements make sense in the context of Chinese interests growing at great speed compared to the PLA's backwardness in some areas. Therefore, on the one hand "threats must also be pre-empted in the minds of elites in rival countries that may decide to compete, contain, or attack China"³⁸. On the other, China sees multi-domain emerging from the 'convergence of different capabilities across different domains on all levels of warfare in order to compensate for relative weaknesses in individual domains and create windows of superiority'³⁹. Within this doctrinal context is the doctrine of the 'Three Wars', which is also based on the principles of ancient Chinese 'perception warfare' strategies⁴⁰. This doctrine aims to influence 'international public narratives, weaken the will of the enemy, shape diplomatic and political narratives and promote PRC interests in all phases of conflict'⁴¹. The US Pentagon offers the following examples for each of the three components:

- *Psychological warfare*, uses propaganda, deception, threats and coercion to influence the opponent's decision-making process, while also countering the opponent's psychological operations;
- *Public opinion warfare*, disseminates information for public consumption to drive and influence public opinion and obtain the support of the national and international public;
- Legal warfare, or Lawfare, uses national and international laws to gain international support, manage political repercussions and influence the target audience.

³⁵ Taylor Fravel, China's Changing Approach to Military Strategy: The Science of Military Strategy from 2001 and 2013. *MIT Political Science Department Research Paper*.

³⁶ State Council 2015. China's Military Strategy.

³⁷ Stefan Halper, 2013. China: The Three Warfares. Office of the Secretary of Defense. Washington, D.C. May.

³⁸ Peter Mattis, 2018. China's 'Three Warfares' in perspective. War on the Rocks. January 30.

³⁹ Derek Solen, 2020. Chinese views of all-domain operations. China Aerospace Studies Institute. Agosto.

⁴⁰ J. Garnaur, 2014. 'US unsettled by China's "three warfares" strategy: Pentagon report'. The Sydney Morning Herald. April 11.

⁴¹ Office of the Secretary of Defense, 2020. Military and Security Developments Involving the People's Republic of China 2020. August 21.

ENVIRONMENT

The surroundings in which forces operate, including air, water, land, space, cyberspace, natural resources, flora, fauna, human beings, and their interrelation. The environments where military operations take place are: maritime, land, air, space, cyber, plus the information and the electromagnetic environments.

ANTI-ACCESS (A2) & AREA-DENIAL (AD)

Anti-Access (A2) and Area-Denial (AD) operations include a variety of military activities that can be conducted in all domains of operations (land, maritime, air, space and cyber) aimed at denying the opponent's ability to enter a given area and manoeuvre freely in the battle space. In particular:

- <u>Anti-Access</u> traditionally refers to the ability to delimit an area and control access to it, effectively denying an opponent entry into the contested area;
- <u>Area-Denial</u> refers to the ability to diminish, degrade or neutralise an opponent's freedom of action within a contested area.

CROSS-DOMAIN ACTION

The integrated combination of military and non-military capabilities in different domains aimed at exploiting a limited window of superiority and engaging the opponent in the physical, cognitive and/or virtual dimensions.

COGNITIVE WARFARE

A new mode of permanent confrontation that attacks the beliefs and opinions of a population with the aim of destabilising the cohesion, security and prosperity of a nation.

UNDERSTAND

One of the functions of multi-domain operations is to interpret the information gathered during the 'perceive' phase. Its purpose is to place the situation in context and make useful evaluations and predictions to support rapid and effective decision-making.

DIMENSION of effects

The conceptual scheme for assessing the effects that military operations must achieve in the three dimensions of the battle space, i.e. physical, virtual and cognitive.

DOMAIN of operations

A set of capabilities and activities applied to the battlefield in a target environment (maritime, land, air, cyber, or space).

EFFECT

The result, outcome or consequence of one or more actions that will influence the physical or behavioural state of a system (or system elements), thereby contributing towards the realisation of one or more decisive points or conditions⁴².

JOINT FUNCTIONS

Homogeneous military activities that, when combined, enable the effective development of a military operation.

MULTI-DOMAIN ESCALATION MANAGEMENT OPTIONS

Construction of incremental response options through the use of all domains and instruments of national power.

MULTI-DOMAIN OPERATIONS

Simultaneous and sequenced actions to generate effects in multiple domains. (NATO definition, draft)

Military activities conducted across multiple domains to perceive, understand and orchestrate converging effects aimed at generating multiple dilemmas at such a speed as to overcome the adversary's decision-making capacity. Activities are conducted by synchronising military actions with other instruments of national power and/or with allies and partners, under a synchronised *Command* and *Control* structure (so-called Multi-Domain Command & Control, MDC2). (Italian definition, draft)

ORCHESTRATE

One of the functions of multi-domain operations including all planning and execution activities augmented by the actions and activities necessary to achieve stated goals. This function is based on the continuous effectiveness of the 'perceive' and 'understand' functions and allows multi-domain operations to be conducted flexibly, taking into account the actual effects achieved, rather than assumed data or desired effects.

SENSE

One of the functions of multi-domain operations including surveillance, discovery, classification, recognition, tracking and identification, collecting data useful for the intelligence cycle and to help generate understanding.

⁴² AJP-01 (D), Allied Joint Doctrine.

RULES BASED INTERNATIONAL ORDER (RBIO)

Shared commitment of countries to conduct activities according to shared rules that evolve over time. They may include: international law, regional security agreements, trade agreements, immigration protocols and cultural agreements, etc.

EFFECT SYNCHRONISATION

The integration of activities/events over time to achieve a favourable operational tempo with respect to what a potential opponent has developed. Effect synchronisation refers not only to the coordination of military activities at the tactical, operational and strategic levels, but also to the necessary integration with the activities underlying the other instruments of national power in a given time interval.

SYSTEM

Set of elements that, neatly linked together, contribute to a given object. A system tends to be a collection of interconnected and interdependent parts, forming an identifiable, organised, complex and dynamic whole. It may comprise elements, activities, people or ideas.

SYSTEM OF SYSTEMS

A set of oriented or dedicated systems that combine their resources and capabilities to create a new, more complex system.

Annex C RESEARCH METHODS AND REFERENCES

This conceptual document was drafted by the 'Project Group for the Innovators Team' known as Committee for Defence Innovation (Italian: *Comitato per l'Innovazione della Difesa*, COMIND). The Group was formed to project the military into the near future by developing and integrating the Strategic Concept of the Chief of Defence Staff in an innovative manner.

A network of experts from academia, industry and research located at the Office for Defence Innovation (INNOV@DIFESA) embraced the Open Innovation paradigm. They analysed the multi-domain issue through multiple ideas and varied perspectives from different backgrounds. The weekly meeting and discussion sessions were interspersed with regular moments of summarisation and sharing with the Services.

From a methodological point of view, the specific contributions of the experts were collected and made available by applying the Concept Development & Experimentation (CD&E) method; international sources were consulted and the outcomes of participation in international NATO and EU activities were shared.

Below is the list of experts who have provided continuous and extensive support to the development of the Concept, to whom goes the Defence General Staff's recognition, followed by the references.

EXPERTS

Industries

- > Mr. Daniele FRISONI LEONARDO, Project Engineering Manager
- > Mr. Alessandro FIDENZI RAIT 88, Chief Global Strategist
- Mr. Massimo AMOROSI RAIT 88 CBRN e *Biothreats specialist*, former advisor to the Ministry of Foreign Affairs for CBRN and to the Senate for defence-related issues.

Academia

- Prof. Andrea UNGARI, Full Professor of Contemporary History at Guglielmo Marconi University and Luiss Guido-Carli University
- Mr. Zeno LEONI, lecturer in International Security at King's College London and Defence Academy of the UK
- Ms. Cristina FONTANELLI, PhD student in Security and Strategic Studies at the University of Genoa and Fellow at LAPS - Laboratorio Analisi Politiche e Sociali

Researchers

- Mr. Alessandro ZACCHEI member of the Technical Scientific Committee of CESMA (Giulio Douhet Military Centre for Aeronautical Studies) for the study of dual-use artificial intelligence applications; Ce.Mi.S.S. researcher
- Mr. Pierluigi BARBERINI, CeSI Centro Studi Internazionali, Defence & Security Desk Analyst
- Mr. Master's student "Peace, War and Security" University of Roma Tre; collaborator Geopolitica.info and IARI - Institute for Analysis of International Relations
- Ms. Michela DI FRANCESCANTONIO, expert in economic security, geopolitics, and intelligence.

REFERENCES

National Publications

- STATO MAGGIORE DIFESA, The Chief of Defence's Strategic Concept "Systemic Efficiency, Overall Relevance" (2020)
- STATO MAGGIORE DIFESA, Future Scenarios Concept (2021)
- STATO MAGGIORE ESERCITO, "Multi-Domain Operations, Approccio Concettuale" (2020)
- STATO MAGGIORE ESERCITO, Nota Dottrinale "Le Operazioni multi-dominio" (2021)
- Ce.Mi.S.S., Ricerca AP-SMA-03 "Prospettive del ruolo del Potere Aereo e Spaziale sulle sfide poste dalle future operazioni multi-dominio", Alessandro ZACCHEI (2018)
- "La dottrina Gerasimov e la filosofia della guerra non convenzionale nella strategia russa contemporanea", Libellula Edizioni - Nicola CRISTADORO, (2018).

NATO Publications

- > NATO Warfighting Capstone Concept (NWCC), (2020)
- > NATO Allied Joint Publication (AJP-01-F) "Allied Joint Doctrine" (draft).
- > NATO INNOVATION HUB "Cognitive Warfare" (2020).
- NATO Cooperative cyber Defence Centre of Excellence (CCDCOE), "cyber Threats to NATO from a Multi-Domain Perspective" (2020)
- NATO Joint Air Power Copetence Centr (JAPCC) "Shaping NATO for Multi-Domain Operations of the future" (2019)
- NATO Combined Joint Operations form the Sea Centre of Excellence (CJOSCOE "Study on Multi-Domain Operations in the Maritime Domain" (2021)

EU publications

- ➢ UE Hybrid Centre of Excellence (CoE), "The Landscape of Hybrid Threats: a concpetual model public version" (2021)
- ➢ UE European External Action Service (EEAS), " EU Guidance on countering Hybrid threats during the planning phase of EU-led CSDP military operations and missions" (draft)

Foreign Publications

- Multinational Capability Development Campaign (MCDC) "Countering Hybrid Warfare" (2019)
- US Army Training and Doctrine Command (TRADOC), Pamphlet 525-3-1 "The U.S. Army in Multi-Domain Operations 2028" (2018)
- UK MoD, Development, Concepts and Doctrine Centre(DCDC) Joint Concept Note 1/20 "Multi-Domain Integration" (2020)
- UK MoD, Development, Concepts and Doctrine Centre (DCDC), Joint Concept Note 2/17 "Future of Command and Control" (2017)
- French Joint Centre for Concepts, Doctrine and Experimentations (CICDE), Joint Concept 0.1.1 "Multimilieux et multichamps (M2MC), la vision française interarmées" (2021)

Academic Articles and Websites

- http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_ National_Congress.pdf
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2774761
- http://english.www.gov.cn/archive/white_paper/2015/05/27/content_28147511561 0833.htm
- https://cryptome.org/2014/06/prc-three-wars.pdf
- https://warontherocks.com/2018/01/chinas-three-warfares-perspective/
- https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/CASI%20 Articles/2020-06-30%20Chinese%20Views%20of%20All-Domain%20Operations.pdf?ver=0gVa73tTs6oxBmMIQnTYxg%3D%3D
- https://www.smh.com.au/politics/federal/us-unsettled-by-chinas-three-warfaresstrategy-pentagon-report-20140410-36g45.html
- https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF



