MILENG CONTRIBUTION TO MULTI DOMAIN OPERATIONS

2022

DISCLAIMER

The Military Engineering Centre of Excellence (MILENG COE) is established as an international organisation that is affiliated to, but not formally part of, NATO. All statements and comments contained above are that of the MILENG COE and do not represent the official NATO position unless formally stated in the text.

INDEX

1 EXECUTIVE SUMMARY

Just after dawn on September 4, 1943, Australian soldiers of the 9th Division came ashore near Lae, Papua in the Australian Army's first major amphibious operation since Gallipoli. Supporting them were U.S. naval forces from VII Amphibious Force. The next day, the 503rd U.S. Parachute Regiment seized the airfield at Nadzab to the West of Lae, which allowed the follow-on landing of the 7th Australian Division. The Japanese defenders offered some resistance on the land, token resistance in the air, and no resistance at sea. Terrain was the main obstacle to Lae's capture.

From the beginning, the allied plan for Lae was a ***joint one. The allies were able to get their forces across the approaches to the enemy's position, establish secure points of entry, build up strength, and defeat the enemy because they dominated the three domains of war relevant at the time — land, sea, and air****.*

Unfortunately, today's commanders cannot have the same degree of confidence in the joint fight that their predecessors had at Lae. Changes in the character of war threaten to undermine the ability of commanders to wage a joint fight effectively, if at all. The development of anti-access and area-denial (A2/AD) weapons and systems means that the joint force may struggle to close with and defeat some adversaries.

If Lae were to be re-fought today, as the landing ships sailed, their movement would be tracked from space. Enemy cyber-attacks launched to disrupt U.S. electronic systems would commence prior to their departure and continue throughout the voyage. The battle for sea control would rage hundreds of miles from the landing area. Salvoes of missiles would thin out the task force. An airdrop would be too risky to even consider. Footage of the carnage filmed from drones would soon appear on the world's media platforms as the battle for world opinion began.

If commanders are to achieve a similar degree of domain overmatch as the Australians enjoyed in 1943, a response to the challenge of these technologies is needed. ……..

(…) The way forward for land forces in the joint fight is a new concept: the multi-domain battle. This concept promises to restore a commander's ability to maximize the tools at their disposal in and across all domains.

ALBERT PALAZZO AND DAVID P. MCLAIN, III

1.1. Current geo strategic reality has outlined the complexity of the new battlefield that is characterized by the continuous interaction of different actors (military and non-military) in the competition of influencing the physical, cognitive and virtual dimensions.

1.2. NATO is adapting its policy and doctrine to the new operational challenges introducing the concept of Multi Domain Operations (MDO) that captures those complex interactions beyond the Joint Operations concept, **which is still fully valid for planning, coordinating and executing the military instrument of power**.

1.3. Although the NATO defines MILENG as "a function in support of operations to shape the physical operating environment (POE)", MILENG activities could also have some influence in the cognitive and virtual dimensions. Conversely, those dimensions could have impacts on MILENG itself. This paper will investigate

how MILENG produces effects in the different dimensions within the framework of Multi Domain Operations.

1.4. The following topics will be addressed in order to provide the reader an understanding of the overarching topic of MDO:

- the current operational environment
- the NATO proposed definitions related to Multi Domain Operations
- The specifities about MDO within the frame of the NATO Concept of Multi Domain Operations[1]
- the interactions and capabilities necessary for a Cross-Domain manoeuvre (Vignette)
- which MILENG capabilities could be employed in a Cross-Domain manoeuvre and how they influence MDO.

[1] INITIAL ALLIANCE CONCEPT FOR MULTI-DOMAIN OPERATIONS - ACT 5 JUL 22

2. AIM

Doctrine describes how the Army conducts and trains for operations today with the capabilities it already has. Conversely, concepts describe how the Army may operate in the mid- to far-term future based on anticipated future operational environments.

GEN David G. Perkins, U.S. Army, Military Review, July-August 2017

2.1 The aim of this document is to frame the contribution of MILENG capabilities in the context of an operation conducted in a Multi Domain enviroment.

2.2. DOTLMPFI[2] approach will be applied in order to define possible adaption of the current MILENG support to a Cross-Domain Manoeuvre in a Multi Domain Operation.

[2] Doctrine, organization, training, leadership, materiel, personnel, facilities and interoperability

3. CONTEXT

We (the Heads of State and Government of the NATO Allies) will individually and collectively deliver the full range of forces, capabilities, plans, resources, assets and infrastructure needed for deterrence and defence, including for high-intensity, ***multi-domain warfighting*** *against nuclear-armed peer-competitors*

NATO 2022 STRATEGIC CONCEPT -29 JUN 22

3.1. As reported within the NATO STRATEGIC Concept, NATO is operating in an age of constant competition[3] that has changed not only the context for operations but also their conduct. Authoritarian actors are challenging NATO interests, values and democratic way of life. Strategic competitors are heavily investing in sophisticated conventional and nuclear capabilities, and they are interfering in NATO Allies democratic processes via hybrid tactics conducted in all domains. These assertive actions span from disinformation campaigns to malicious cyber activities and use of coercive economic measures (i.e., energy war) or social dynamics like immigration. The physical operating environment and battlespace will be increasingly complex, hyperactive, urbanised and connected with no clear geographical boundaries and where all domains are contested across all levels of command. NATO's MDO Concept assumes that all military activity occurs through the five operational domains of, Land, Maritime, Air, Space and Cyberspace, and that the consequences of these activities, (i.e., the effects), occur in the physical, cognitive and virtual dimensions. Due to this complex context, NATO may re-think its approach to future and current threats; specifically, in terms of time, space and functions[4]:

- Time: the future is now! Near peer competitors and non-state organisations have advanced capabilities and the will to compete with NATO power.
- Space: new technologies and the progressive pervasion of the cognitive and virtual dimensions into the physical dimension, have expanded the battlefield such that the conceptual geographic framework is no longer always suitable for describing and conceptualizing warfighting.
- Functions: the binary concept of action-reaction is no longer valid. The adversary is continually shaping NATO in all dimensions and domains. The shaping, contesting and fighting paradigm is continuously applied, not only after a declared adversary action.

[3] NATO SUMMIT 2022

[4] NATO's Warfighting Capstone Concept: anticipating the changing character of war Rear Admiral John W. Tammen (https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html)

3.2. The NATO Warfighting Capstone Concept (NWCC), which sets the future warfighting context and the priorities for NATO warfare development, recognizes that the NATO Military Instrument of power should be developed under five imperatives (warfare development imperatives):

- *Cognitive superiority*: Truly understanding the operating environment, the adversary and the Alliance's goals entails cohesive and shared political-military understanding of the threats, adversaries and environment NATO operates in, from tech and doctrine, to JISR (Joint intelligence Surveillance and Recce) and big data. Equally, it will focus on providing the right tools for the political-military level to operate effectively (rapidly and dynamically) and safeguard decision-making in the modern information age.
- *Layered resilience*: Underpinning deterrence, the Alliance needs to be able to withstand immediate shocks to supply lines and communications, as well as effects in the cognitive dimension. It must be prepared to persevere in challenging situations over long periods and be ready from day zero.
- *Influence and power projection*: To shape the environment to its strengths, including generating options and imposing dilemmas on adversaries, the Alliance must be proactive in taking initiative through various means to reach its objectives.
- *Integrated multi-domain defence*: The threats that the Alliance faces are no longer in any one domain, so a joint and flexible approach to a fluid environment is essential to protect the Alliance's integrity against all threats, regardless of their origin or nature.
- *Cross-domain command*: Command insight at the blink of an eye, the hallmark of great generals, may be out of reach in a multi-domain and integrated battlespace. Investing in our people, the art of command, critical thinking and audacious action will underpin success.

Clearly, the NWCC underlines the importance of competing in all domains in a simultaneous and coordinated manner, that implies the development (Warfare development Agenda - WDA) of:

- NATO cross-domain concept
- NATO integrated multi domain architecture
- NATO Multi domain defence network
- A cross-domain leadership understanding
- Integrated and realistic training.

3.3. The Threat: NATO is confronted by security challenges coming from different sources, resurgent and assertive state actors, non-state actors and violent extremism. Especially state actors are trying to destroy the Alliance cohesion by an approach in all domains , using Hybrid means, and without distinguishing peace from war but setting a continuous competition in order to erode NATO power and values. The assertive, multi domain strategy is carried out below the threshold of warfighting, at least against any of the Alliance's nations, in order to avoid a direct involvement of the military power of NATO that could be overwhelming, instead focusing on Alliance vulnerabilities inherent to democratic systems and especially present in the information and communication, that are sensitive to manipulation or attacks perpetrated by distance and hidden sources. Systems thinking is the idea which leads the adversaries' strategy that is focusing on exploiting the Alliance systems interdependence vulnerabilities attacking them by kinetic and non-kinetic operations carried out simultaneously in order to obtain strategic effects (i.e., manipulating the perception of the targeted population towards their political power in order to influence decisions on employing military power against a threat carried out by classical military means).

Beside there is not an explicit multidomain reference present in our competitor's military doctrine, they are operating with a multi domain approach by integrating or directly subordinating all the governmental agencies efforts to the military strategy. Using economic sanctions, energy trade, humanitarian aids or technological influence to reach strategic effects is a reality both in China and Russia. They are integrating civilian instruments of power with military instruments in order to compete in all domains and coordinating the actions to reach effects in all dimensions simultaneously. The predominant domain in which the competitors concentrate their efforts is given both by geostrategic considerations and by contingent situation (i.e., Russia is more focused on land domain due to its extension and geography, China is more projected to maritime and air due to its location and trade network), this implies that every adversary employs the multi domain coordination differently, requiring a different approach in contrasting their efforts.

3.4. The technological development: Historically, military ways of fighting have been heavily influenced by the advancement of technology. NATO[5] has identified 9 emerging disruptive technologies (EDTs)[6] that will influence operations in the near future.

- artificial intelligence (AI),
- data,
- autonomy,
- quantum-enabled technologies,
- biotechnology,

[5] Science & Technology Trends 2020-2040, Exploring the S&T Edge - NATO Science & Technology Organization

[6] Ref AC/259-D(2022)0024-REV1 CNAD Implementation Plan for EDTs

- hypersonic technologies,
- space,
- novel materials and manufacturing,
- energy and propulsion.

These technologies will not only be used in new weapon systems but, will also modify the military approach to operations and tactics. (i.e., hypersonic missiles or AI applied to process large amounts of information in order to improve situational awareness). They will also redefine the domain reach of some capabilities, for example sea denial may be carried out by weapons systems deployed in the land domain with long range, hypersonic capabilities; or cyber-attacks may be used to disrupt communication networks used to control unmanned autonomous vehicles. Furthermore, the diffusion of these EDTs will be wider and wider, at low cost, flattening the capabilities superiority, normally detained by state actors.

4. DEFINITIONS

It is apparent that MDO is a chameleon-like concept, adopting various and often inchoate forms, dependent upon both context and the understanding of the person engaged.

Mark O'Neill – Design the Future: Thinking About Joint Operations (AUS Army Research Centre)

4.1. Operational domain: A specified sphere of capabilities and activities that can be applied within an engagement space.

Note: there are five operational domains: maritime, land, air, space and cyberspace, each conditioned by the characteristics of its operating environment

4.2. Engagement space: The engagement space and battlespace are synonyms. The engagement space is part of the operating environment where actions and activities are planned and conducted. The commander's engagement space is often broader than their operations area due to increasing interconnectivity of the effect dimensions. Furthermore, the varying degrees of relevance that geography has in cyberspace and space, the electromagnetic spectrum and the information environment means that a geographically bounded engagement space is not always suitable. (AJP-01)

4.3. Environment: An environment describes the system surrounding an activity. A system is a functionally, physically or behaviourally related group of regularly interacting or interdependent elements. A group of systems is a network. There are multiple types of environments, both physical and non-physical, and commanders use many terms to describe them. Examples include (but are not restricted to): information, maritime, urban, political and human. (AJP-01)

Operating environment: A composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander (NATO Term). We can understand the operating environment as a global set of complex, dynamic and interrelated networks, comprising political, military, economic, social, infrastructure and information systems, each exerting pressure and influence on the others. Understanding the nature and interaction of these systems as part of mission analysis helps the commander define their engagement space and affects how they will integrate actions with in it. (AJP-01)

4.4. Effects dimensions: An analytical construct that translates actions in the engagement space into the physical, virtual and cognitive consequences that these actions may have)

4.5. Physical dimension comprises the audiences, the sub-surface, surface, airspace and space areas where all physical activities take place, and where audiences live, including all physical objects and infrastructure that support them.

4.6. Cognitive dimension comprises the audiences' perceptions, beliefs, interests, aims, decisions and behaviours. It encompasses all forms of interaction between them (such as economic and political).

4.7. Virtual dimension comprises intangible activity in the form of storage transmission of analogue and digital data and information, and all supporting communication and information systems and processes. Besides these, information belongs to the virtual dimension as well.

4.8. Capability: The ability to create an effect through employment of an integrated set of aspects categorized as doctrine, organization, training, materiel, leadership development, personnel, facilities, and interoperability. (NATO Term)

4.9. Operation: Operations are a sequence of coordinated actions with a defined purpose which are military and contribute to a broader approach including non-military actions. Operations are conducted through the art of directing, coordinating, controlling and adjusting the actions of forces to achieve specific objectives. (AJP-3)

4.10. Multi Domain Operations: Orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to deliver converging effects at the speed of relevance. (MCM-0121-2022 (INV) Initial Alliance Concept for Multi-Domain Operations (MDO working definition))

4.11. Cross-domain Manoeuvre: is the employment of mutually supporting lethal and non-lethal capabilities in multiple domains to generate overmatch, present multiple dilemmas, and enable freedom of movement and action. Cross-domain manoeuvre leverages, integrates, and synchronizes multi-domain effects[7]

4.12. Space domain The operational domain that encompasses all activities, functions, and operations undertaken to, in, through and/or from space. (not NATO agreed, under development)

4.13. Cyberspace: The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data,

[7] The U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045 Versatile, Agile, and Lethal

including those which are separated or independent, which process, store or transmit data. (NATO Term)

5. MULTI DOMAIN OPERATIONS characteristics

5.1. This chapter will describe the concept of MDO as it is framed in the current NATO doctrine. This concept is still in its infancy, hence, MDO will be described in general terms, focusing on the differences with the Joint Operations concept and providing details on the space and cyberspace domains. This will provide the reader a comprehensive view of MDO.

5.2. The NATO Concept of multi domain operations is an evolution of joint operations[8] (not replacing them but integrating them, refer to paragraph 5.4). The transition to multidomain operations started when the Alliance recognized the cyberspace and space domains. In the same way that the introduction of air power transformed a single-service focus to a joint approach, the persistence of the space domain and the ubiquitous and pervasiveness of the cyberspace domain is changing how the Alliance operates. Furthermore, the increasing number of multi domain capabilities owned by individual services and civilian partners, means the traditional mindset of 'joint operations' conducted by the services, no longer adequately captures the need to integrate military and civilian capabilities, both horizontally and vertically.

5.3. Multi domain operations[9] (**see fig. 1[10]**) orchestrate military activities from across all domains to create effects synchronizing these actives with non-military activities. This orchestration is achieved by integrating actions (fires, manoeuvre, information and CIMIC). Integration is achieved through coordination, synchronization and prioritization.

- Coordination – coordination brings together different capabilities from across the operational domains into an efficient and effective relationship.
- Synchronization – coordination is enhanced by synchronization, which sequences capabilities and activities, at an appropriate tempo, in time and space.
- Prioritization – coordination and synchronization highlight competing demands for time, space and finite resources; prioritization determines their allocation, in accordance with the commander's plan

[8] AJP 01 (F)

[9] The definition in paragraph 5.3. is taken entirely from AJP 01 (F)

[10] NATO Allied Command Transformation Alliance Concept for Multi-Domain Operations Read Ahead

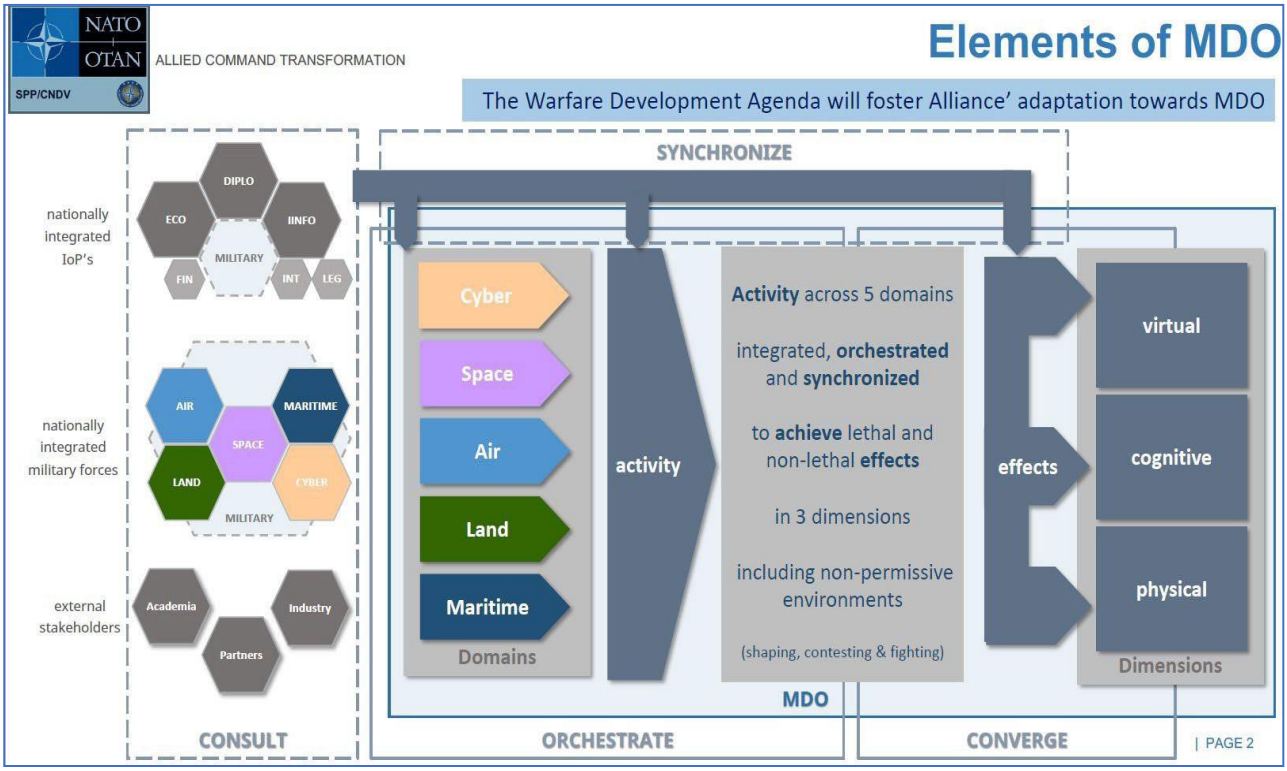


Fig.1

5.4. Joint and MDO:

The first question usually asked when the MDO concept is first introduced is "What is the difference between MDO and Joint Operations?". This is a natural reaction but is not a valid comparison and is in many ways a meaningless question as these two concepts are completely different, based on totally different perspectives, despite both including the word "operations".

The concept of Joint Operations considers operations through the lens of which service (Army, Navy, Air Force) and how many are conducting the operation. It does not consider or specify where the activities are taking place. The concept of MDO on the other hand does not consider which or how many services are involved. Rather, MDO considers operations through the lens of in which domain(s) an operation is conducted, regardless of who is conducting the activities involved. MDO is primarily a mindset that must be developed in order to best exploit all the options and capabilities available in all domains.

Ultimately, the effects that NATO is seeking to achieve have not changed. What is different is the activities that may be conducted to achieve these effects and how they may achieve them.

*Joint operations could be defined as an **integrator of effects** in different domains to achieve Operational and Strategic Objs. MDO could be intended as a complementary concept of Joint because MDO are aimed at **integrating actions** carried out in the different domains **to converge** effects in the 3 dimensions (virtual, cognitive and physical).*

5.5. **Current operational environment is complex, we could assume that all the military operations are inherently or potentially multi domain because all actions carried out in one domain, have interactions or are enabled by capabilities present in other domains. The ubiquitous nature of GPS and computer systems mean that almost or all operations will be multi domain. Most activities will produce effects in at least two and sometimes all three dimensions**.

5.6. According to the ACT, initial MDO concept, the following principles are foundational to the successful implementation of MDO:

Principle	Explanation
UNITY	Allows coordinated action of all capabilities towards a common objective. Provides the basis to orchestrate military activities and synchronise non-military contributions. Requires collaboration, transparency and trust to enable the harmonised planning and execution of MDO. Benefits from willingness to bridge diverse national perspectives.
INTERCONNECTIVITY	Enhances shared understanding and enables interoperability of force elements. It is challenged by differences between legacy and modern-platforms, and by data-classification. Must be resilient and requires standardised data to support user requirements.
CREATIVITY	Stimulates the development of boundless opportunities that can be tailored to offer surprise and multiple dilemmas. Relies on an ability to analyse situations from different viewpoints and turn complexity into simplicity. Enhanced by an ability to visualise context and settings. Supports a commander's aptitude to orchestrate MDO.
AGILITY	Allows the force to take advantage of fleeting opportunities. It requires initiative, relative speed, prioritisation, and flexibility of thought and action.

5.7. MDO are inherently dependent on a strong "digital backbone" for the rapid, resilient and secure transfer of information among all domains. The coordination of actions in all domains is ensured by a reliable and resilient communication infrastructure.

5.8. Focusing on the military instrument of power, MDO could be identified with the following characteristics[11]:

a. **Gain and maintain contact**. Future formations should be proactive in gathering information about the adversary intentions, actions and capabilities in all domains, this implies a proactive and aggressive posture

[11]From: The U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045 Versatile, Agile, and Lethal

in surveillance and reconnaissance.

b. **Persistently compete:** formations should be able to compete in all the domains with the adversary without escalating to open confrontation by:
    i. Operating deception for stimulating adversary systems
    ii. Conducting info ops also using cyber capabilities
    iii. Demonstrating the capability to escalate the competition.

c. **Calibrate force posture for Large-Scale Combat Operations (LSGCO):** Forces employed in MDO should be prepared to operate in a contested environment (in all domains), this leads to a Force which is:
    i. Credible and capable of effectively responding to changes in the operating environment.
    ii. Ready and pre-positioned to maximum extent, completed and sustained by organic enablers.
    iii. Protected by extensive use of Camouflage, Concealment and Deception; positioned in hardened locations and dispersed in the terrain.
    iv. Prepared with an improved situational awareness for responding to changesin the adversary posture and able to rapidly shift to offensive operations.

d. **Converge effects:** Commanders should orchestrate the capabilities they have available in different domains in order to attack the adversary vulnerabilities. The effects obtained by actions in different domains should be coordinated to converge against an identified vulnerability of the adversary (example a coordinated joint fire attack to an adversary critical infrastructure identified by space assets and previously disabled by a cyber-attack with the effects used to build an info campaign against the adversary).

e. **Exploit the initiative.** Shaping activities (in all the domains) must be coordinated in order to allow MDO formations to maintain and exploit initiative. A proactive posture is necessary to shape windows of opportunity against the adversary.

f. **Consolidate gains**: MDO formations should be able to rapidly exploit gains over the adversary by:
    i. Rapidly reducing the adversary force,
    ii. Maintaining and reinforcing taken advantage positions,

5.9. SPACE AND CYBERSPACE

The transition to multi-domain operations started when the Alliance recognized the cyberspace and space domains.In the same way that the introduction of air power transformed a single-service focus to a joint approach, the persistence of the space domain and the ubiquitous and pervasiveness of the cyberspace domain is changing how the Alliance operates….(AJP 01 (F)).

Knowledge of the Space and Cyber domains' activities and capabilities will provide the reader with a better understanding about the interactions that those domains could have with the others, in the context of the MDO.

a. **SPACE DOMAIN**[12]:

i. NATO introduced the Policy for Space support in NATO operations in 2018 and approved the overarching Space Policy (UNCLASS) on 2022. Space was declared an operating domain in Dec 2019 by NATO Head of States. The policy documents set the foundational work for Space Operational Activities along 3 operational functions of:
   - Space Domain Awareness (SDA)
   - Space Domain Coordination (SDC)
   - Operational Space Support (OSS).

i. Space is increasingly important for the Alliance's Allies security and prosperity. Space brings benefits in multiple areas from weather monitoring, environment and agriculture, to transport and science, communications and banking. The use of space has greatly enhanced Allies and NATO's ability to anticipate threats and respond to crises with greater speed, effectiveness and precision.

i. Space is an inherently global environment, and is essential to coherent Alliance Deterrence and Defence.

ii. NATO is not aiming to develop Space capabilities of its own, Allies will undertake to provide, on a voluntary basis, and in accordance with national laws, regulations and policies, the Space Data, Products , Services (DPS) or effects, that could be required for the Alliance 's operations, missions and activities.

iii. Currently the AJP 3.3 Allied Joint Doctrine for Air and Space Operations (version 2016) refers to Space, only through the scope of Space Support operations. This doctrine was written prior to the approval of the MC Space Domain Action plan in 2021 and the declaration of Space as an operational domain. It is not consistent with the MC Space Action plan.

[12] Given the fact the current Space doctrine is embedded in AJP 3.3. and it is not consistent with the recognition of the Space as Operating Domain, all the following information are taken by the Doctrine Proposal for Allied Joint doctrine for Space operations (NSO JOINT 0814 2022 dated 29 July 2022).

iv. The Space Mission Areas which enable all Space capabilities can be described as follows:

1. **ISR** (Intelligence Surveillance Reconnaissance): Space systems contribute to the development of intelligence through surveillance and reconnaissance activities and coordinate the requirements for satellite ISR capabilities in support of operations (G2, G9, Targeting, Battle Damage Assessment (BDA), environmental monitoring) and Joint Personnel Recovery support. Surveillance through space systems can involve multiple satellites and does not have to be continuous monitoring. Most common reconnaissance sensors include Electro-Optical (EO), infrared thermal (IR), and Synthetic Aperture Radar (SAR).
2. **PNT** (Positioning, Navigation and Timing): To determine an object or signal's geographic location, calculation of a route from position A to position B, and accurate location time, for synchronizing clocks and networks to support Precision Guided Munitions and Force tracking
3. **METOC** (Meteorological & Oceanographic): Assess the impact of Space weather events on NATO operations. Space weather could interfere with radio signals and temporarily disrupt SATCOM and PNT satellite ranging from minutes to hours. It can also optimize Search and Rescue operations at sea and determine optimum locations for amphibious landing
4. **SSA** (Space Situational Awareness): Monitoring of Space objects to mitigate the impacts that Space objects have on other satellites through ground-based or space-based sensors. Space surveillance and tracking uses both radar and optical detection, which are important for Space debris tracking and Satellite mapping.
5. **SATCOM** (Satellite Communications): monitoring and analysis in support of J6 and modelling of enemy GPS (Global Positioning System) jammers to assist operational planning, and also to preserve long range communications beyond Line-of-sight (BLOS), provide critical connectivity, keep Command & Control (C2) function, and maintain Remotely Piloted Aircraft (RPA) operations.
6. **SEW** (Shared Early Warning): Provides warning of Ballistic Missile launches. Potential trajectories are calculated and delivered within minutes after a missile launch occurs. Information includes launch point, predicted impact point and estimated flight time. The US is currently the only NATO Nation with Space-based SEW capabilities

b. **CYBERSPACE DOMAIN**[13] : Cyberspace is different from the other domains because it is man-made, partly non-physical and may not conform to geographical boundaries.

i. Cyberspace operations (COs) **apply capabilities in cyberspace to create effects which support operations across the other domains.** Cyberspace impacts many environments, such as the electromagnetic and information environments but it could also produce effects in the physical dimension (i.e. disruption of services in an electric power plant or shut down of electronic control systems in vehicles). Cyberspace exists by virtue of physical components on land, at sea, in the air and in space. Conversely, operations in the physical dimension function effectively by virtue of cyberspace. Consequently, the five domains are dynamically interlinked; a change in one domain may have implications for the situation in the other domains. While some COs may support information operations, other COs will be conducted in support of operations in the physical domains to achieve objectives. Information operations are more specifically concerned with the integrated employment of information-related capabilities during military operations, in concert with the lines of operation, to influence, disrupt, corrupt or usurp the decision-making of adversaries while protecting our own. **Thus, cyberspace is a medium through which some information-related capabilities and techniques, such as psychological operations or deception, may be employed**.

ii. COs are conducted through two types of operations depending on commander's intent and objectives. It is important to note that these types of COs may be executed both by Allies and adversaries:

- defensive cyberspace operations (DCOs); and
- offensive cyberspace operations (OCOs).

COs are always conducted at the logical layer, encompassing direct effects to software, data and protocols. However, indirect effects may be aimed at the other layers of cyberspace, or at creating other higher-order effects in other domains.

Like every other operation, COs are initially considered in the joint targeting process, to identify targeting options where COs could be conducted to create specific effects in support of the commander's mission objectives. During planning, and continuously as part of execution, target nominations are required to implement COs. These are initiated through the joint targeting process into the relevant working groups for development to be fed into relevant boards for inclusion on the joint prioritised target list (JPTL). The cyclic target development process during planning should include input for COs at all relevance.

[13] Ref: AJP-3.20

6. MULTI DOMAIN OPERATION – VIGNETTE

6.1. In this chapter a tactical (Corps size) vignette will help the reader to understand the interactions among different military capabilities in order to carry out a Cross-domain manoeuvre.

6.2. Using the actions described in the vignette, it is possible to frame the MILENG capabilities that could effectively support the force employed in a Multi Domain scenario, at all levels of command.

6.3. The questions to answer are:

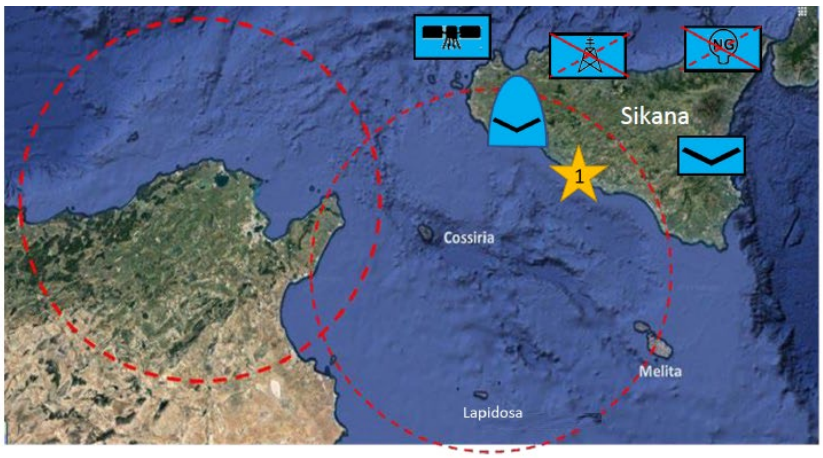
a. What are the key enablers for a cross-domain manoeuvre?
b. How does MILENG support (sustain) a cross-domain maneuver in multi domain ops?
c. Which MILENG capabilities are needed both for forces and staff, in order to support the depicted maneuver?
d. How does MILENG contribute to the coordination, synchronization and prioritization of capabilities and activities across all domains?

6.4. OPERATION LIBERORUM MEDITERRANEI (VIGNETTE)

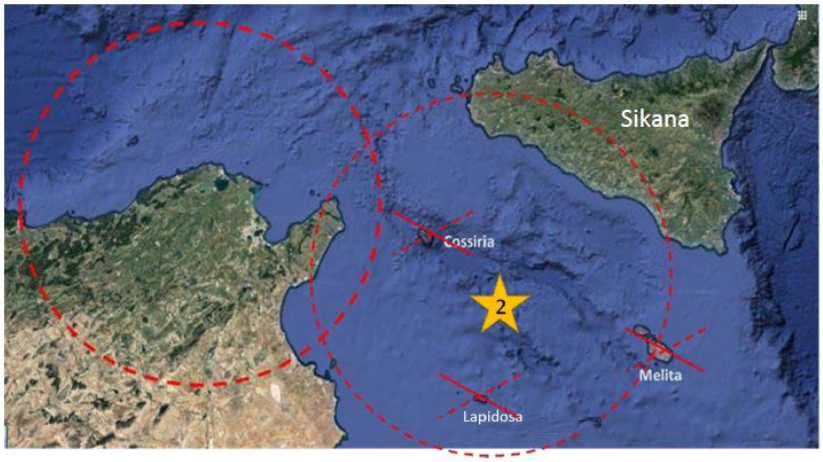
a. **Road to crisis**:
   - Strait of SIKANA is a strategic passage in the MEDITERRANEAN Sea, where an important percentage of world commercial trades and energy transportation pass through and a preferred route for illegal immigration in Europe. Furthermore, critical communication cables are present in the area, connecting 3 continents.
   - An assertive power (SINAE) without direct access on the Mediterranean is gaining increasing power in the south coastline in order to influence and control the strategic passage with the final intent to restrict the free trade and threat or at least control the comms cables.
   - To fulfil its intent, SINAE deploy A2/AD (anti Air/ Area Denial) assets in NORTH AFRICA in order to control the SIKANA strait passage and directly hamper SIKANA (NATO Country). Several ships, both civilian and military are targeted by A2/AD assets by SINAE. Furthermore, robust maritime and amphibious assets are deployed in the ports facing the straight.
   - SIKANA, with NATO backup, reacts militarily in order to prevent the SINAE seizure of the strait and ensure free movement through.
   - **A multi-domain operation** is carried out by SIKANA in order to reach the objective to have a free passage on the SIKANA strait and reduce SINAE threat.

b. Cross domain maneuver:

1 SIKANA receive a full intelligence picture of SINAE assets and movements in the strait area, both by NATO and national ISR (Air,Space, unmanned included) assets. Evidence of a possible attack are provided, moreover, SINAE increase cyber malicious attacks to SIKANA infrastructure in order to deny services.

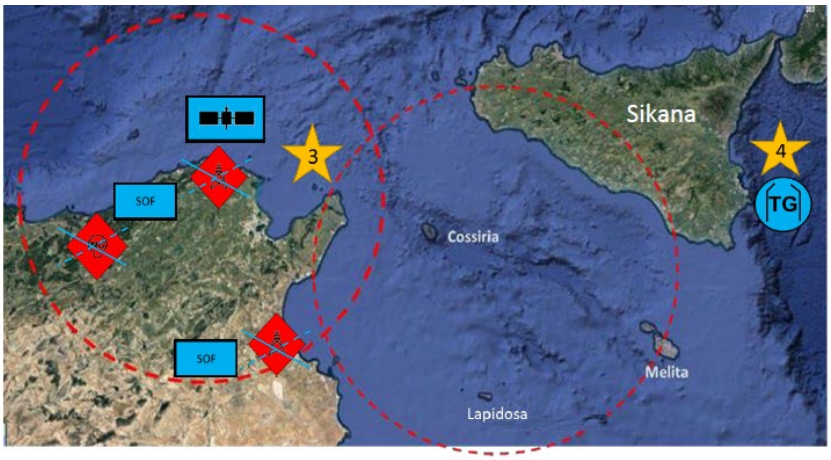


2 SINAE destroy or damage all the airstrips in the minor islands (COSSIRIA, LAPIDOSA and MELITA) in the SIKANA strait by joint fire attacks.

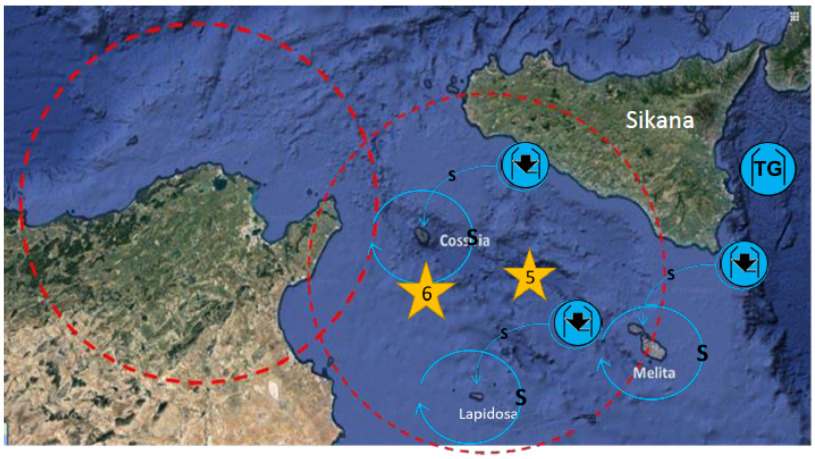


3 SIKANA, backed by Alliance, launch a combined action in space and cyber domains in order to hit energy and comms infra in North Africa and temporarily blind and disrupt the SINAE C2. Special forces are deployed in order to gather information and feed the targeting cycle

4 In the meanwhile, an amphibious force, including heavy engineering and fire assets, is prepared out of the A2/AD bubble. Only fast and armed vessels are moving within the strait. Maritime main force is cruising out of the A2/AD threat ready to backup and support



5 Once ISR grants the information about reduced SINAE capabilities, amphibious landing is concurrently launched to the small islands in the straight (COSSIRIA, LAPIDOSA and MELITA) in order to seize them and prepare austere infrastructure respectively (in priority order) to allow air landing, deploy radars and fire assets

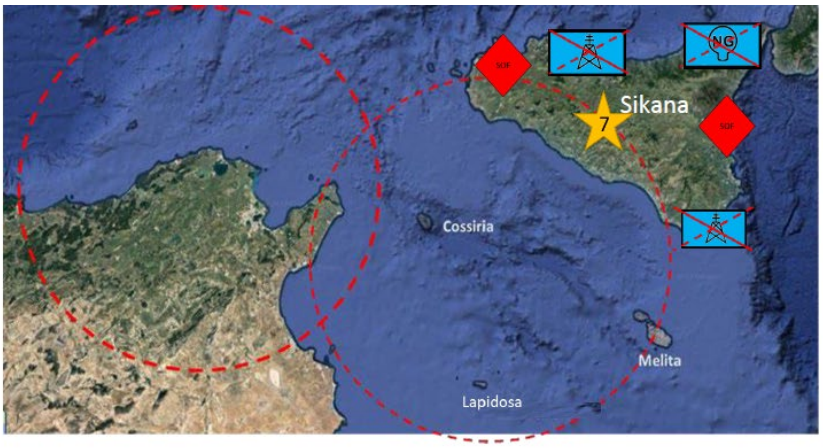


6 Marines ensure beachheads in the islands and engineers will repair airstrip to austere standards and prepare fortifications for defensive positions. Multiple camouflaged positions will be prepared in order to deceive the adversary and offers target dilemmas.
Once austere airstrips are prepared, heavy lift air transportation will bring to islands:

- Radars and EW equipment
- Long fire assets
- Air Defence assets
- Equipment for enabling satellite comms

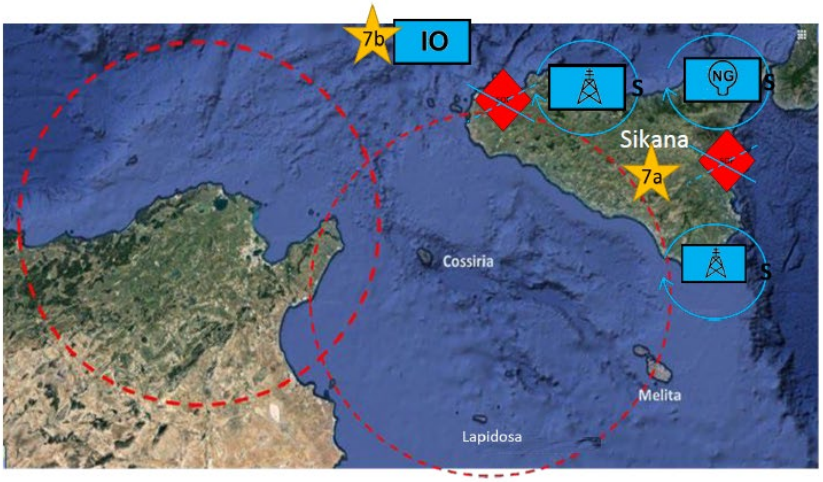
Once deployment of enabling assets is complete, the main amphibious force will land heavy assets like Infantry fighting vehicles that will operate dispersed in small units in order to prevent SINAE landings.
SIKANA force C2 is granted by deployed units HQs and the main force HQ afloat. Mission command is widely applied in order to cope with possible C2 disruptions.
assets are deployed in the minor islands in order to secure them and prepare attacks to SINAE fire assets in NORTH AFRICA.

7 SINAE special forces are operating in the SIKANA mainland trying to carry out sabotage in the SIKANA critical infra especially comms landing stations, transportation and energy.



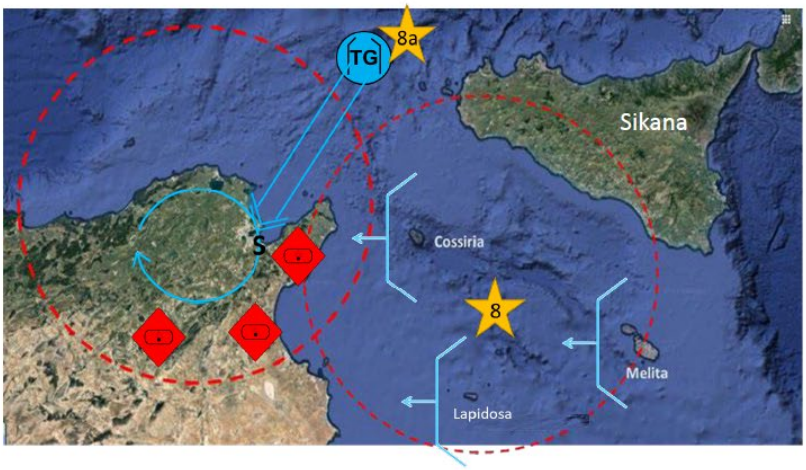
7a SIKANA will secure the rear contrasting SINAE SOF operations and securing energy and comms infra.

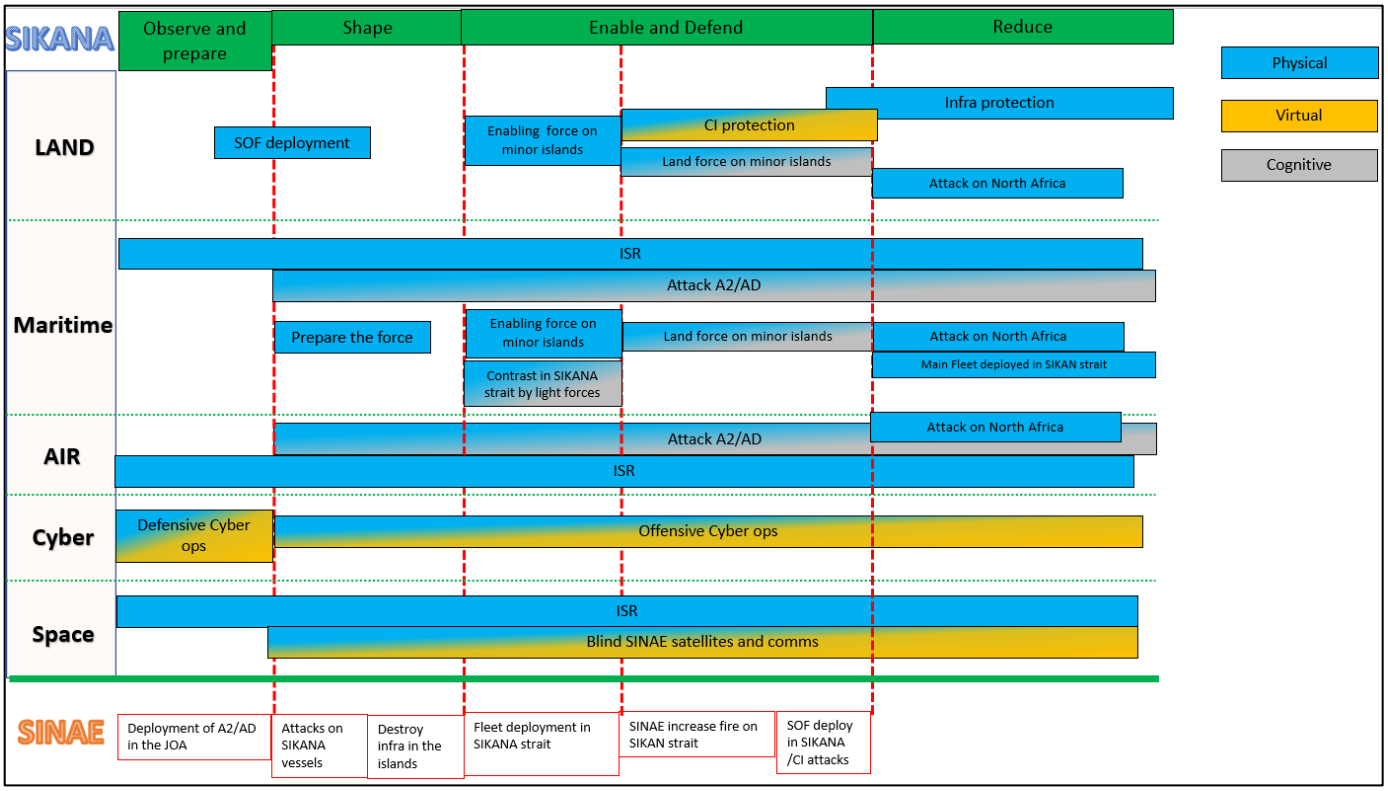
7b Concurrently an info ops campaign is launched in order to strengthen fight willing and reduce SINAE strategic obj to influence SIKANA population.



8 SIKANA forces will target SINAE A2/AD assets from minor islands acquired positions and…

8a ..once the threat is reduced, main maritime force launches a decisive attack on the NORTH AFRICA coast in order to seize and secure the area granting free passage on the SIKANA strait





7. MILENG CAPABILITIES IN MDO

7.1. This chapter will list the enabling capabilities for MDO and then how MILENG is nested within those enablers, in supporting the cross-domain manouvre.

7.2. Given the assumption that MILENG capabilities[15] should be integrated in the effective orchestration of the multidomain actions, the following is a list of possible MILENG related tasks and resources that could be considered enabling an MDO.

a. What are the key enablers for a cross-domain maneuver?

i. The cross-domain maneuver is enabled by an effective intelligence, dispersed forces connected by reliable communications and self-sustainable to the maximum extent possible.

ii. Effective ISR for granting situational awareness consistent with high tempo.

iii. Rapid deployable, long range joint fire assets are thedecisive tool for the delivery of lethal effects and for reducing the adversary capabilities.

iv. SOF employed both as enabler (for intelligence) and effectors for the DEEP area.

v. Space assets are enablers for maneuver in terms of comms and delivery of fire

vi. Cyber operations are the main effectors for the virtual and cognitive dimensions.

vi. Reliable communications are the link among the different domains for delivering coordinated actions.

vii. Real time data sharing is crucial for proper C2 in MDO environment.

ix. Use of Electronic Warfare assets (harmonized with Cyber operations) can restrict significantly adversary maneuver, fire and communication capabilities.

x. Air missile defense system – through the survivability of friendly forces - can support maneuver and fire.

b. How MILENG to support (sustain) a cross-domain maneuver in MDO?

i. Intelligence capacity is supported by MILENG in providing MILENG related information to the cycle, this means all the information concerning the terrain and the physical environment. Special focus should be dedicated to infrastructure assessment, which means the determination of mission- critical infrastructure, a risk analysis including the effects on the multi domain actions in case of disruption and protective measures, finally how the infrastructure are affected by or how they affect the manouvre

ii. Dispersed forces should be independent in term of support, including MILENG support capabilities. Mob/CMob and general support to

[15] Both in terms of staff and units

maneuver should be ensured by detaching required MILENG assets, mission tailored, at the right time. This requires accurate planning and timely deliverance of MILENG capabilities to avoid slowing maneuver.

ii. Logistics must be able to support the line of communication maintenance and improvement. Furthermore, the REAR area should be always enabled by MILENG support to maintain the infrastructure needed for stocks and distribution.

iv. Sustainment of forces supported by planning and use of sufficient MILENG capabilities for developing, maintaining and improving infrastructure, supporting the survivability and sustainability of forces and enabling manoeuvre or mobility of suppliers / enablers.

v. Joint Fires must be supported both by staff and capabilities respectively in the targeting cycle (infra assessment, battle damage…) and by concealment, camouflage and deception (CCD) and prepared protected positions.

vi. Space is indirectly supported by the protection or enablement of the land-based infrastructure.

vi. Cyber could be supported by MILENG staff both in assessing the impact of Cyber operations on the infrastructure and, vice versa, how the Cyber domain is influenced or enabled by existing infrastructure in the battlefield area.

vii. Land based cyber, space or any other critical infrastructure protection is supported by defensive Military Search / EOD.

c. Which MILENG capabilities are needed both for forces and staff, in order to support the depicted manoeuvre?

i. Engineer assets detached to manoeuvre units with a high degree of independence and a range of Mission – tailored capabilities.

ii. General support assets focused on the provision of support to Sustainment and Fires.

ii. General support assets in support of the AIR domain for enabling the air related land based infrastructure. Airfield Damage Repair (ADR)/ Air Force engineer units with assets and materials to designate the MOS and restore the runway, parking area. As required, aviation related markings, lightning, arresting systems, etc. to beestablished

iv. General support assets in support of the Maritime domain for enabling the maritime related land based infrastructure.

v. MILENG staff at every level of command able to be effective in providing specialized advice (i.e. targeting cycle, planning, intelligence cycle).

vi. Engineer intelligence capabilities to the recce units for early MILENG related information collection. Extensive use of unmanned equipment in support of the recce units , as a capability multiplier.

vi. MILENG staff, able to carry out infrastructure assessment, must be properly integrated into the targeting cycle and intelligence cycle. This will allow early MILENG advising in both areas.
vii. EOD units to clear the UXOs from the airfield/airstrip.
ix. Engineer assets to prepare fortifications, defensive positions and CCD.

d. How does MILENG contribute to the coordination, synchronization and prioritization of capabilities and activities across all domains?

i. Infrastructure assessment: the MILENG expertise is useful in planning properly the use of different domains' capabilities in order to have converging effects (i.e.: the interconnections between infrastructure, in a given operating environment, will help to defend or attack critical nodes).
ii. Mobility of dispersed units will allow them to rapidly concentrate capabilities where and when needed.
ii. Effective infrastructure support will help to sustain operations across domains (i.e.: APOD/SPOD maintenance and development, protection of mission and critical infrastructure) and prioritize capabilities.

7.3. MILENG DOTMLPFI Analysis on MDO: the table below provides possible DOTMLPF adaptations for addressing the MILENG support in MDO. This table should be considered speculative based upon the previously mentioned MILENG tasks and the characteristics of the MDO described above.

MILENG Support to Multi Domain Operations – DOTMLPF-I matrix.

	STAFF Echelons Above Divisions	MILENG BDE	MILENG BN	MILENG COY
DOCTRINE	The current doctrine appears to fit the purpose because it advocates the presence of the MILENG staff in all the decision-making process and planning. Furthermore, the MILENG advisor is required at all level of command. More emphasis is needed in the Cyber and Space domains doctrine in order to integrate the MILENG staff contribution respectively to targeting cycle and ISR and METOC supported missions	Dedicated doctrine for MILENG Bde should be developed in coping with MDO. Especially the role as "force provider" must be emphasized.	-	-
ORGANIZATION	The MILENG staff should be robust especially on the Planning and Intelligence sections.	• The task organization should cover all those specialized, resource demanding capabilities that cannot be included at the Bn level (i.e. INFRA, Bridging, Intelligence) • The MILENG Bde should be intented also a "capability" provider for the tactical level (Bn and lower) in order to fulfill specialized tasks. • Strong C2 capabilities must be ensured to enable the Bde as "capability provider" • The MILENG bde staff should be robust enough to cope with the rapid tempo of the MDO and the information management (planning and intelligence) • Robust INFRA section both for protection works and infra related spt	• MILENG Bn primary focus must be the support of the manouvre but it should be ready to receive specialized capabilities from the MILENG Bde and/or detach them to the subordinate units. • The unit should be organized on the modularity based upon the assigned mission or contingent task given to spt the main effort or windows of opportunity.	
TRAINING	• The staff must be trained in coping with the complexity of the MDO. Preparation must be focused on the cross effects of the activities in the different domains. • More INT and Targeting related training	• Prepare the staff to complex operating environment • Prepare the staff to high tempo of the MDO • Refine the C2 procedures • Train the staff on the INT and Targeting cycles • Train with supported Corps	• Train the staff to C2 procedures for supporting capabilities received from the MILENG Bde. • Rapid deployment capabilities related training • Integration with Recce assets • Support of Fire assets • More CCD related training • Staff trained in intelligence	• Train the MILENG recce units to feed the INT and targeting cycle • Train the use of UAVs and UGVs
MATERIEL	Info-fusion system to be established.	• Robust C2 systems • Pre positioned stocks	Robust C2 systems	Satellite Comms Recce equipment (UAV, UGV)
LEADERSHIP	The MILENG advisor should be of a suitable rank in order to effectively and timely coordinate all MILENG resources and capabilities	C2 over the MILENG assets organic to Corps.	Role of the MILENG Advisor to supported units	Role of the MILENG Advisor to supported units
PERSONNEL	• Preparation in the INT and Targeting • MDO Mindset			
FACILITIES	From this level down to the level of the Eng Bn it is imperative to have facilities which allow realistic training (one of the pillars of the NWCC). Therefore, a truly reliable and capable "digital backbone" is needed to support the training and thereby the capabilities. So not only training areas but the required IT to really operate in a MDO mode.	-	-	-
INTEROPERABILITY	Info-fusion data sharing system within all domains to be established (in CZE Army it is in preparational phase and called "Extended Reality" however it covers just Land, Air and Intel/Cyber sources so far).	Connectivity to Info-fusion system.	Connectivity to Info-fusion system.	Connectivity to Info-fusion system.

7.4. CONCLUSIONS

The MDO concept does not constitute a revolutionary change in MILENG support but it is rather a modification in the mindset of the MILENG staff, primarily in understanding the complexity and interactions inherent to MDO and, secondly in accepting and coordinating the role of MILENG capabilities as "enabler of cross domain maneuver enablers". In this context, the decisive role of the MILENG staff is advising the maneuver commanders in the best employment of the MILENG capabilities and expertise. The unique knowledge and expertise of terrain and infrastructure provided by MILENG advisors is especially important in enabling the intelligence and targeting cycles, vital for the superiority in MDO. MILENG staff should be oriented, at all levels, at understanding the terrain and the interactions of the present infrastructure (considering also the space and cyberspace, this, an area that needs further development) and properly feed the information to obtain up to date and effective situational awareness.

To obtain effective MILENG support from the staff, it is vital to invest in focused training and new equipment (comms and robotics). that respond to the increased MDO tempo and inherent information complexity.

Edited by Policy Concept and Doctrine branch of the Military Engineering Centre of Excellence.

For any remark or request please write to:

- ***forceprotectch@milengcoe.org***
- ***pcdbc@milengcoe.org***

All the information are internal speculations or comes from National and NATO doctrine.

Military Engineering Center of Exellence

Manchinger Strasse 1

85053, Ingolstadt (Germany)