"OLD?" C-IED FOR A "NEW?" ALLIED CONCEPT: THE C-IED APPROACH IN THE LIGHT OF NATO WARFARE DEVELOPMENT IMPERATIVES

By Lieutenant Colonel Jose M Rufas, Chief of Attack the Networks Branch, C-IED Centre of Excellence

"You realize that our mistrust of the future makes it hard to give up the past."
(Chuck Palahniuk in his book "Survivor", first published in 1999)

If you, dear reader, have been reading about the North Atlantic Treaty Organization (NATO), most probably you would be familiar with hearing (and even harder to effectively understand…) terminology such as "*comprehensive approach*", "*countering improvised explosive devices*", "*enhanced forward presence*", "*integrating gender perspective as a force multiplier*", "*attack the networks*", "*innovation continuum*" or "*grey zone*"..

So lately, under the umbrella of "*countering hybrid threats*" approach and in the context of the NATO "*Warfighting Capstone Concept*", the NATO "*Warfare Development Agenda*" (WDA) framework emerges…

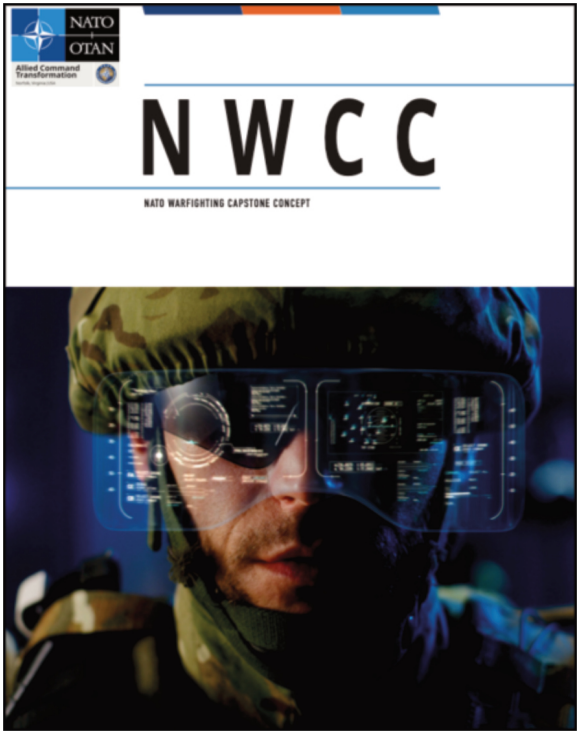

Figure 1: Cover of "NATO Warfighting Capstone Concept" document, as published in 2021 *(Source – www.act.nato.int)*

D'où venons-nous? Que sommes-nous?...[1]

Despite the strong focus of the Alliance on the Russian threat at the Eastern Front, the NATO Strategic Concept 2022 was still considering terrorism as one of the main threats for the Alliance.

> 34. Countering terrorism is essential to our collective defence. NATO's role in the fight against terrorism contributes to all three core tasks and is integral to the Alliance's 360-degree approach to deterrence and defence. Terrorist organisations threaten the security of our populations, forces and territory. We will continue to counter, deter, defend and respond to threats and challenges posed by terrorist groups, based on a combination of prevention, protection and denial measures. We will enhance cooperation with the international community, including the United Nations and the European Union, to tackle the conditions conducive to the spread of terrorism.

Figure 2: Capture from "NATO Strategic Concept" page 8, as published in 2022 *(Source – www.nato.int)*

Additionally, the last Annual Report from the NATO Secretary General (as published some days before the publication of this article) is making direct reference not only to terrorism but also directly to C-IED and Technical Exploitation…

In other words: do you know about any terrorist group which has been/is not employing or willing to employ improvised explosive devices as a weapon of choice?

Between the lines, we could read and understand how the Countering Improvised Explosive Devices (C-IED) approach could persist as absolutely necessary even without any casualty as directly caused by the detonation of any IED over allied troops. In fact, C-IED is based on the integration, synchronization and coordination of actions seeking for anticipation in benefit of the reduction of capabilities of adversary human networks in the aim of denying them the potential manufacture and use of those devices.

Terrorism: Remaining Vigilant

Terrorism remains the most significant asymmetric threat to the security of the citizens of NATO and to international peace and stability. Terrorists and terrorist groups have continued to demonstrate their ability to cross international borders, expand their networks, enhance their capabilities and invest in new technologies to increase their reach and lethality against both NATO Allies and partners.

Delivering innovative capabilities to defeat the terrorist threat is a core pillar of NATO's efforts. Spanning technical exploitation, countering unmanned aircraft systems, biometrics, battlefield evidence and countering improvised explosive devices, NATO's work continues to address capability gaps and strengthen Allies' interoperability. It is also focused on incorporating new technologies into counter-terrorism capabilities, and ensuring through exercises that existing capabilities are fit for purpose.

Figure 3: Captured from "NATO Secretary General 2024 Report" page 15, as published in April 2025 *(Source – www.nato.int)*

1 Taken from the title of Paul Gauguin´s oil on canvas "D*'où venons-nous? Que sommes-nous? Où allons-nous?*" (Where Do We Come From? What Are We? Where Are We Going?) as painted in 1897.

... Où allons-nous ?[2]

The NATO Warfighting Capstone Concept provides five warfare development imperatives to focus and synchronize efforts to develop the Alliance military instrument of power (MIoP).

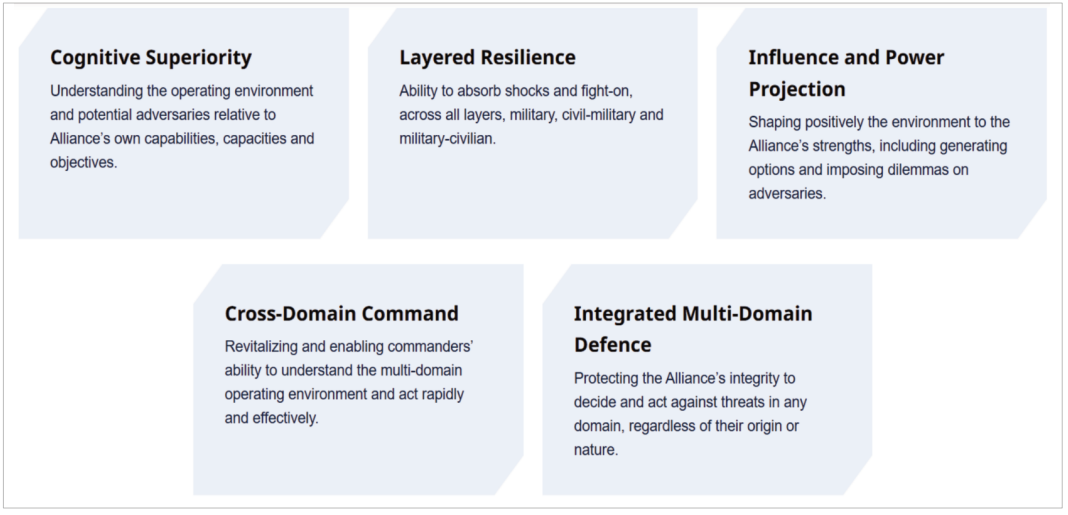

Figure 4: NATO warfare development imperatives *(Source – www.nato.int)*

One of those imperatives is **"Cognitive Superiority"** (aka COGSUP), which is described as the degree of dominance through possessing and applying faster, deeper and broader understanding and more effective decision-making than adversaries.

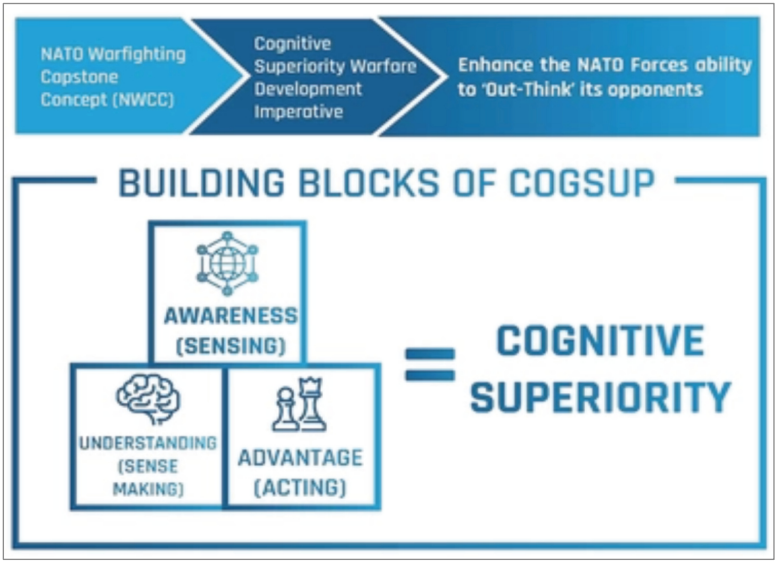

Figure 5: NATO description of Cognitive Superiority *(Source – www.nato.int)*

2 Taken from the title of Paul Gauguin´s oil on canvas "D'où venons-nous ? Que sommes-nous ? Où allons-nous ?" (Where Do We Come From? What Are We? Where Are We Going?) as painted in 1897.

From a C-IED perspective, the blocks derived from the concept for Cognitive Superiority have always been considered from the Attack the Networks approach:

- Awareness (sensing) is essential for deep knowledge about the threat, our own capabilities, and the Human Terrain through analyzing the cognitive environment.
- Understanding (sense making) poses a must for Human Network Analysis and Support to Targeting/Engagement.
- Advantage (acting) fully implies Human Network Engagement and Assessment steps.

Nonetheless, the main problems for an effective and anticipatory application of the C-IED approach (So Attack the Networks) remain active for achieving the Cognitive Superiority. Information collection and intelligence processing capabilities need to be reinforced, enhanced, and refined… which, in general terms, has never happened even during the Allied involvement in Afghanistan, Iraq and so on. The emerging threat scenarios unavoidably require an increase in intelligence capabilities and an evolution of the processes associated with those intelligence capabilities!

On the other hand, the development of allied initiatives in the field of Cognitive Warfare (COGWAR) is directly associated with Cognitive Superiority imperative. From an Attack the Networks point of view, the current approach to Cognitive Warfare has been considered inside the essential-to-success non-lethal actions.

COGWAR integrates cyber, information, psychological, and social engineering capabilities. These activities, conducted in synchronization with other instruments of power (so not only the Military Instruments of Power (MIoP)), can affect attitudes and behaviour by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary. In fact, there is a huge umbrella of different emerging and disruptive technologies (EDTs) which could potentially support COGWAR development.

With regards to **"Layered Resilience"**, so a sort of comprehensive and holistic approach to collective defence resilience, it would refer to the ability of a single nation and all allied nations to withstand and recover from a broad spectrum of threats and challenges. Accordingly, NATO emphasizes that the resilience of each member country contributes to the overall strength and preparedness of the Alliance, but also the common cohesion and unity of effort is essential for that.

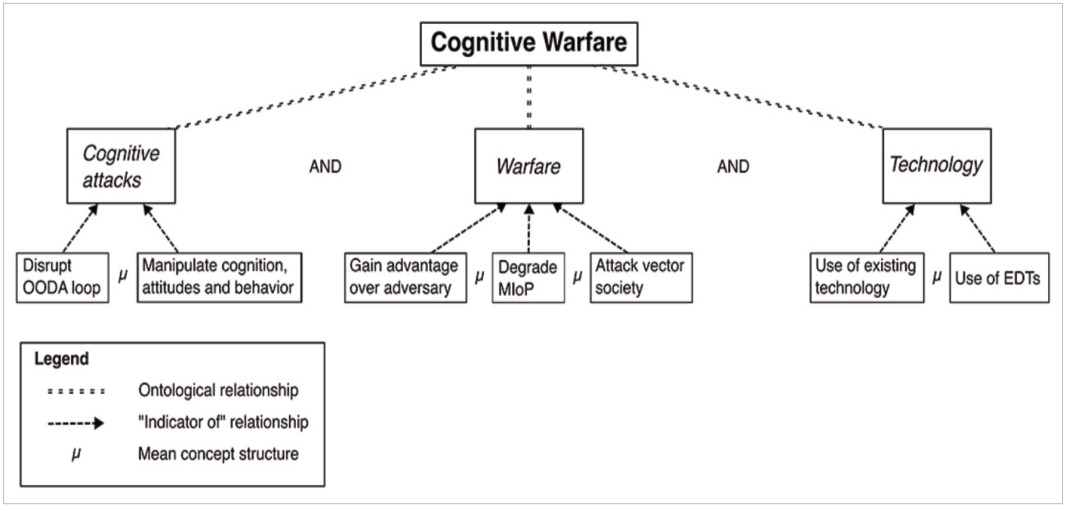

Figure 6: Visualization of NATO cognitive warfare working definition. *(Source - https://doi.org/10.3389/fdata.2024.1452129)*

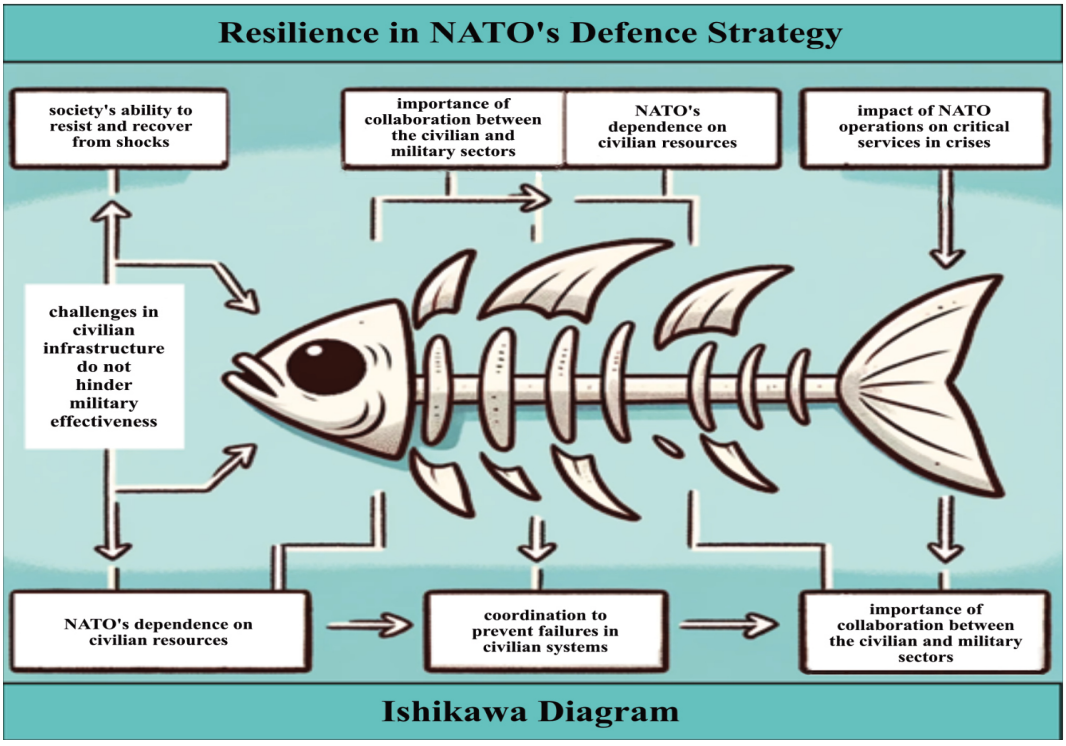

Figure 7: Structured visualization of the factors influencing resilience in the context of allied defence *(Source - www.e-arc.ro)*

Although a layered resilience is not directly related to a generic C-IED approach, it is partially applicable from Attack the Networks perspective when referring to both:

- The preparation of friendly human networks against the potential negative effects from adversary actions.
- The effectiveness of own actions developed in support of the achievement of positive effects over friendly human networks in benefit of strengthening own capabilities in the aim of undermining the potential development of adversary capabilities.

From the combination of the other three imperatives (**"Influence and Power Projection"**, **"Cross-Domain Command"** and **"Integrated Multi-Domain Defence"**) we arrive at the allied implementation of the concept for Multi-Domain Operations.

Multi-Domain Operations (MDO) are currently defined by NATO as "*the orchestration of military activities, across all domains and environments, synchronized with nonmilitary activities, to enable the Alliance to deliver converging effects at the speed of relevance*".

After an initial review, MDO concept is mostly based on:

- Military and nonmilitary activities synchronization, which is another way of considering the essential "Interagency" flavor of C-IED/Attack the Networks.
- Actions over all domains and environments, which have been a must for C-IED/Attack the Networks from its conceptual creation.
- Integration of effects at the speed of relevance, which is the root of the application of C-IED/Attack the Networks approach in the aim of achieving effects over the capabilities of human networks.

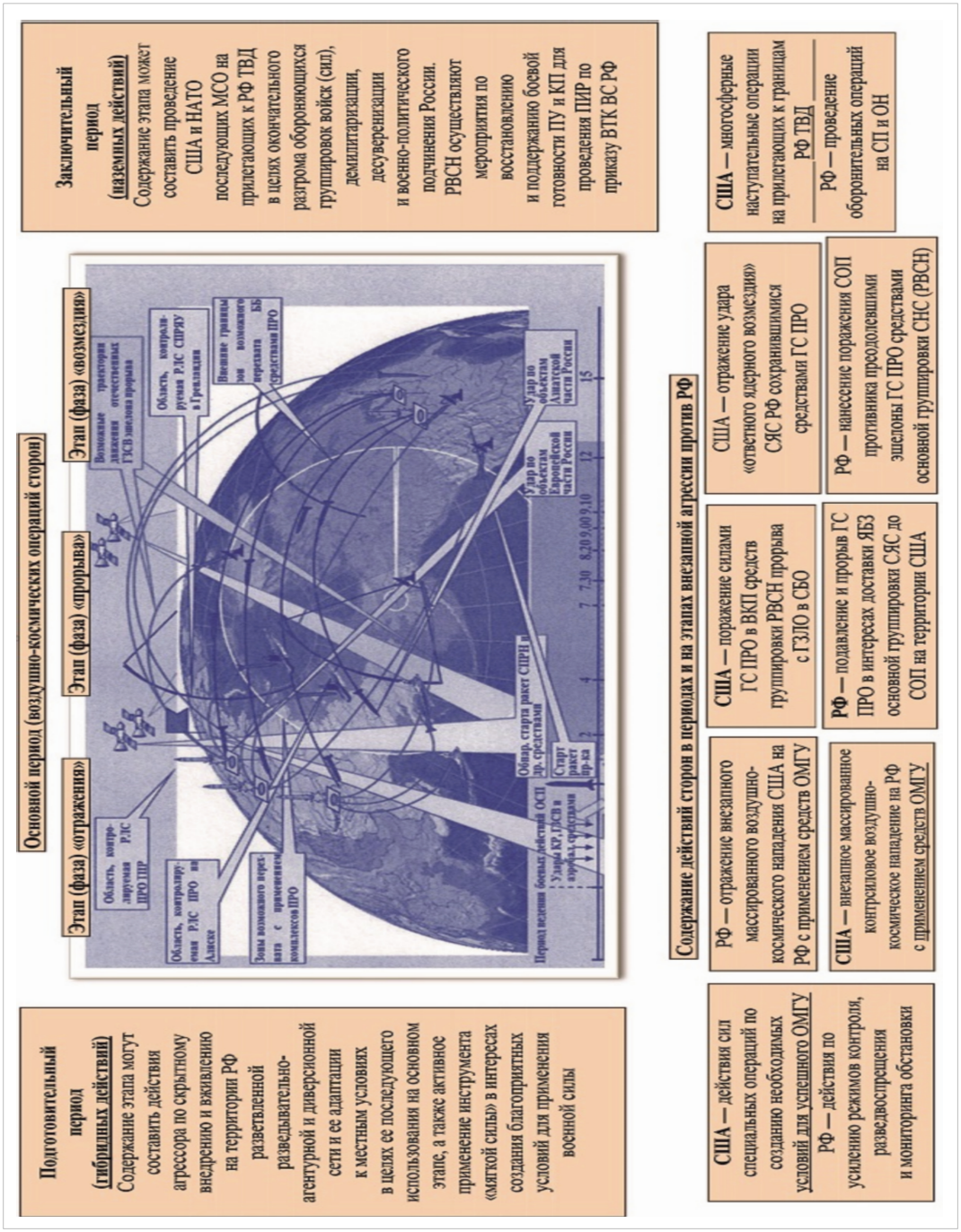

Figure 8: Russian conceptual model of bilateral interactions based on USA strategic MDO aggression *(Source - www.vm.ric.mil.ru)*

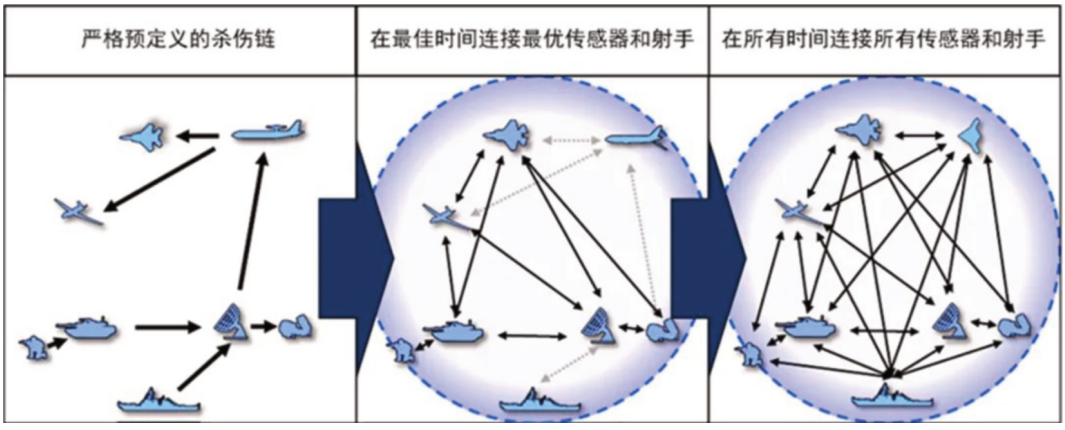

Figure 9: Joint Command & Control evolution in the sight of All-Domain Operations *(Source - www.secrss.com)*

Multi-Domain Operations is a new NATO concept... Are you really sure?

In fact, NATO Allied Command Transformation (ACT) has merely adopted concepts (Multi-Domain Extended Battlefield and Multi-Domain Operations) which were developed by the United States of America (USA) Army and Marines Corps during last decade (although finally published by the Army).

On the other hand, Russia has imitated the USA approach to MDO through their "многосферной операции, multi-sphere operations" concept.

In parallel, China adopted the equivalent to MDO "全域作战 all-domain operations" approach.

MDO finally moves around two essential elements: network-centric warfare, and deep strike capabilities as integrated at the five domains (air, land, sea, space & cyber).

If there be nothing new, but that which is! [3]

Firstly, it looks like the whole spectrum of NATO Warfare Development Agenda (WDA) is not too revolutionary in 2025.

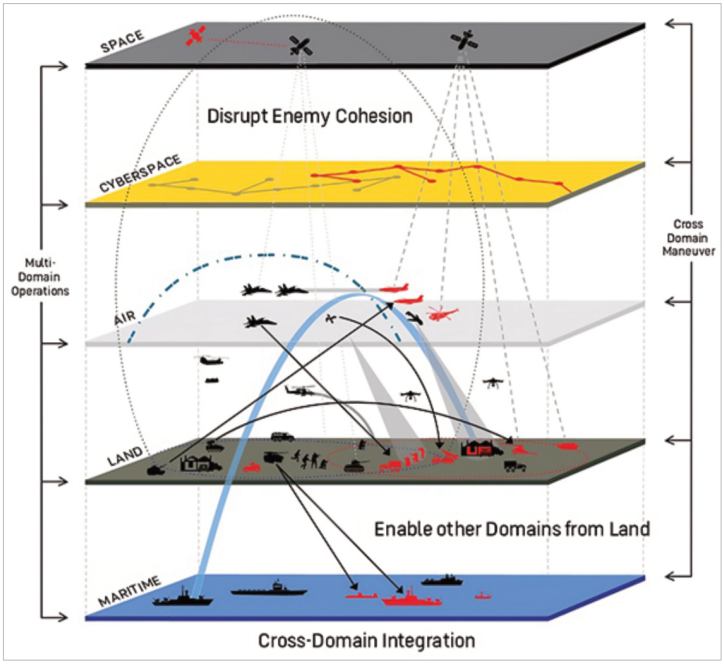

Figure 10: Cross-domain integration for Multi-Domain Operations *(Source – www.immmedia.in)*

3 From the Sonnet 59 as written by Willian Shakespeare

Secondly, it looks like the Alliance (but mostly its member nations) could currently not be ready for effectively implementing Multi-Domain Operations, due to both the NATO lack of accuracy in defining the concept and the huge effort in the development of intelligence and operations that MDO would require.

Thirdly, it seems that the MDO approach is already implemented (so fully applicable to C-IED) into the Attack the Networks approach from its very beginning of existence in 2008. Along with the evolution of the emerging threats and the persistence of IED as a future weapon of choice, that makes C-IED still valid and of course necessary. ■

"Extinction is the rule. Survival is the exception."

(Carl Sagan in his book "The Varieties of Scientific Experience: A Personal View of the Search for God", 2006)

REFERENCES

- (NATO) 2019 NATO Military Strategy
- (NATO) 2020 Concept for Deterrence and Defence of the Euro-Atlantic Area (DDA)
- (NATO) 2021 NATO Warfighting Capstone Concept (NWCC)
- (NATO) 2022 NATO Warfare Development Agenda (WDA)´
- (NATO) 2022 NATO Strategic Concept
- (NATO) 2024 Secretary General's Annual Report
- www.e-arc.ro
- www.irsem.fr
- www.japcc.org
- www.tandfonline.com/journals/ucst20
- www.c2coe.org
- www.act.nato.int
- www.finabel.org
- R. McDermott, "*Russian Armed Forces Test Multi-Domain Operations*", Jamestown Foundation, 9 September 2020.
- D. Solen, "*Chinese Views of All-Domain Operations*", China Aerospace Studies Institute, August 2020
- www.cssas.unap.ro
- www.secrss.com
- UK MoD Joint Concept Note 1/20 "Multi-Domain Integration" (archived)
- Ionita, Craisor *"THE CONCEPT OF MULTI-DOMAIN OPERATIONS AND ITS MULTINATIONAL UNDER-STANDING"* (STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment, 186-193) 2022

Disclaimer

This article does not represent the opinion of any national or multinational organisation; its whole content should only be considered as the opinion of the author. As all information has been obtained from open sources, potential mistakes could have been made during the research process. Please feel free to send your comments, corrections and inputs to the author; they will be highly appreciated.

ABOUT THE AUTHOR

Lieutenant Colonel Jose M Rufas graduated from the Spanish Army Military Academy in 1993. He was commissioned into the C-IED Centre of Excellence as Head of the Defeat the Device Branch in August 2016 and currently holds the post of Chief of Attack the Networks Branch. As a Military Engineer Officer, his background has been mainly based on Explosive Ordnance Disposal activities in the Spanish Army and C-IED staff issues at the multinational headquarters. In addition to his EOD Operator / EOD Officer education, he attended some other military courses regarding Parachuting, Army Staff, Information Operations, War College General/ Joint Staff, Military Search, Technical Exploitation Operations, Weapons Intelligence Team, Exploitation Laboratories, Homemade Explosives and other C-IED courses. His operational assignments include Bosnia and Herzegovina (3), Afghanistan (3), the Republic of Ecuador, Iraq and Uganda.

E-mail: jrufas@ciedcoe.org