SYNCHRONISING MULTI DOMAIN OPERATIONS USING THE BREACH MINDSET

Lieutenant Colonel Paul Pembroke
3rd Combat Engineer Regiment

"A good plan violently executed now is better than a perfect plan executed next week."

George S. Patton

Abstract

1. The US Army developed the Multi Domain Operations concept to address the shift in focus of national security as articulated in the 2018 US National Defense Strategy from countering violent extremists to long term strategic competition with revisionist powers. The Multi Domain Operations concept has operationalised Joint Warfare doctrine for the specific problem set that requires competing with a US near peer adversary along the competition spectrum up to and including armed conflict in areas controlled by adversary anti access area denial capabilities. Multi Domain Operations seek to converge effects at the strategic, operational and tactical levels across the domains of land, air, maritime, space and cyber to obtain an advantage for friendly forces. The Australian Defence Force as part of a US led Multi-National Task Force will benefit from understanding how the Multi Domain Operations concept seeks to converge multi domain effects to create a window of local advantage. If each tactical objective is considered a multi domain obstacle to be breached, the breach mindset or SOSRA can be used as a tool to synchronise multi domain effects and create or capitalise on opportunities.

Introduction

2. The 2018 US National Defense Strategy shifted the focus of US national security from countering violent extremists worldwide to long term strategic competition with revisionist powers. The US Army developed the Multi Domain Operations concept to articulate how the land component will contribute to a joint force in competition with a near peer adversary across the domains of land, air, maritime, space and cyber. The Multi Domain Operations concept has operationalised joint warfare doctrine for the US Army specific to the problem of competing with a US near peer ally across a competition spectrum up to and including armed conflict at the strategic, operational and tactical levels. As the Multi Domain Operations concept becomes further developed, it is likely to influence future US joint warfare doctrine. The Australian Defence Force will benefit from an understanding of the Multi Domain Operations concept and how this can be used to synchronise multi domain effects to achieve advantage on the future battlefield.

MULTI DOMAIN OPERATIONS CONCEPT

3. The US Army describes Multi Domain Operations as the land components contribution as part of a joint force to counter and defeat a near peer adversary

capable of contesting in all domains[1]. The concept is focussed in the 2025 to 2050 time frame and considers the requirement to integrate multi national and joint forces to deter and defeat near peer strategic competitors in both competition and armed conflict. Multi Domain Operations is a US Army concept, not doctrine and is deliberately focussed on how the US Army is structured and equipped for the future battlefield. The series of war games and exercises conducted by the US Army in 2019 are intended to inform an updated concept that may become a joint multi-service one rather than an Army focused concept[2]. The principal author of the Multi Domain Operations concept, General Mark Milley has been nominated as the next Chairman of the US Joint Chiefs of Staff and US investment in the Multi Domain Operations concept will continue.

IS MULTI DOMAIN OPERATIONS JUST ANOTHER NAME FOR JOINT WARFARE?

4. The Multi Domain Operations concept sounds very similar to Joint Warfare doctrine. The Australian approach to joint that has evolved over the last 50 years integrates service combat capabilities as a joint force to provide the best coordinated effects into the land, air and maritime domains and more recently into those of space and cyberspace[3]. The US Army has operationalised Joint Warfare to meet the specific problem set that is competition with China and Russia in areas controlled by adversary anti access area denial capabilities. There are three key differences between Joint Warfare doctrine and the Multi Domain Operations concept that are important for the Australian tactical planner to understand when working with the US Army. The first of these is the concept of a near peer adversary, the second is the competition spectrum and the third is the synchronisation of effects at echelons above Brigade to achieve areas of local advantage.

5. The phrase near peer is a US concept that has limited applicability to Australian doctrine. What determines whether or not a country can be considered a near peer to the US involves the country's capability to compete across all domains. Hostile intent alone is insufficient to be a near peer, without adequate capability the hostile country is relatively benign as a threat[4]. The US 2018 National Defense Strategy specifically lists China and Russia as revisionist states in competition with the US[5]. The ANZUS Treaty between Australia, New Zealand and the US specifies if there is an armed attack in the Pacific Region against one of the parties, the others must take action[6] while recent history has seen Australian involvement in US led wars across the globe. It is likely Australia

---

[1] TRADOC Pamphlet 525-3-1 *The US Army in Multi Domain Operations 2028*, 6 December 2018, pvii

[2] Andrew Feickert, *The US Army and Multi-Domain Operations*, 17 January 2019

[3] Tim McKenna & Tim McKay, *Australia's Joint Approach: Past, Present and Future*, Joint Studies Paper Series No. 1, Commonwealth of Australia 2017, p73

[4] J. Robert Kane, *Russia is not America's near peer threat*, published on the Small Wars Journal website

[5] US Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, 2018

[6] Alison Pert, *North Korea, Australia and the ANZUS Treaty*, Australian Strategic Policy Institute The Strategist, 4 April 2018

will be part of a multi-national coalition, led by the US, should competition lead to armed conflict against a US near peer.

6. The Multi Domain Operations concept considers a competition continuum ranging from competition below armed conflict, armed conflict and a return to competition below armed conflict[7]. During the armed conflict phase, the Army as part of the joint force will be required to:

a. Penetrate enemy anti access and area denial systems to enable strategic and operational manoeuvre.

b. Dis-integrate enemy anti access and area denial systems to enable operational and tactical manoeuvre.

c. Exploit the resulting freedom of manoeuvre to achieve operational and strategic objectives by defeating enemy forces in all domains.

d. Re-compete by consolidating gains across all domains to force a return to competition on favourable terms to the US and allies.

7. The US are investing heavily in experimentation and war gaming to develop the concept of employment, releasing the US Army Concept: Multi Domain Operations at Echelons above Brigade in December 2018[8]. In the US Army context, echelons above Brigade will be employing effects in all domains at the strategic and operational level to achieve areas of local advantage. The Australian Army considers the Combat Brigade as the unit of action being the basic tactical fighting element that is enabled with sufficient scale of force and range of capabilities to apply the full suite of tactics[9]. On the future battlefield, the Australian Army may employ forces at Brigade level and below as part of a Multi-National Division to exploit areas of local advantage created by multi domain effects.

MULTI DOMAIN OPERATIONS AND ACCELERATED WARFARE

8. The Australian Army futures concept of Accelerated Warfare has similarities to the US Army Multi Domain Operations concept as both seek to prepare the Army to be future ready. Accelerated warfare recognises that we are living in an era of increasing competition while the threat landscape is subject to rapid change. The proliferation of anti access area denial capabilities will limit or deny manoeuvre while systems are becoming more distributed and harder to target. Accelerated Warfare drives consideration of how we create access, persistence and lethality in the joint force while capitalising on the opportunities available in the Space and Cyber domains[10]. The Multi Domain Operations concept complements Accelerated Warfare and provides a means to consider how the Australian

[7] TRADOC Pamphlet 525-3-8 *US Army Concept: Multi Domain Combined Arms Operations at Echelons above Brigade 2025-2045* 6 December 2018, p14

[8] Ibid

[9] Land Warfare Doctrine 3-0-3 *Formation Tactics 2016* Interim Publication, p31

[10] Lieutenant General Rick Burr, *Accelerated Warfare – Futures Statement for an Army in Motion*, 2018

Defence Force will integrate as part of a US led multi-national task force across the competition spectrum.

APPLICABILITY OF MULTI DOMAIN OPERATIONS FOR BRIGADE MANOEUVRE

9. The Multi Domain Operations concept is still under development within the US Army and is being focussed at echelons above Brigade. The Joint Task Force Commander may employ the Land Component Command as part of a synchronised Multi Domain Operation to create multiple dilemmas for the enemy. In 2028 an Australian Combat Brigade as part of a Multi-National Division may be conducting manoeuvre operations synchronised with multi domain effects on the battlefield however may not be the priority of support for the Joint Task Force. For this reason it is important that the Combat Brigade understands the Multi Domain effects being applied and synchronises manoeuvre operations to capitalise on these effects. Tactical manoeuvre will only be occurring in the armed conflict phase and will be enabled by multi domain shaping operations conducted in the earlier phase. Convergence of Multi Domain effects seeks to dis-integrate the enemies networks by targeting nodes to sequentially degrade parts of the integrated system and creating additional vulnerabilities[11]. Tactical manoeuvre will seek to exploit vulnerabilities from degradation of the enemy network while seeking to create local windows of synchronisation that support tactical defeat of the enemy at a specified time and place.

THE FIVE DOMAINS

10. Multi Domain Operations seek to converge effects in the domains of land, air, maritime, space and cyber in order to create multiple dilemmas for the enemy commander. It is important that the manoeuvre commander understands the effect that can be produced within each domain rather than the specific capability that will achieve this.

11. The traditional domains of land, air and maritime are the most well known and the effects available in each domain can be articulated using the combat functions of Know, Shape, Strike, Shield and Sustain[12]. Each domain applies available capabilities through Joint planning to know the operating environment and the enemy, shape the environment to support friendly operations, strike enemy forces, shield friendly forces from enemy actions and sustain friendly forces to continue the fight. The domains of Space and Cyber are relatively new to Joint considerations and need further explanation to create a common understanding of effects.

12. Space based capabilities are typically focussed on Intelligence Surveillance and Reconnaissance (ISR), communications and Precision Navigation and Timing (PNT). Satellite networks enable application of these three capabilities and satellites are vulnerable to a wide array of threats. When competing against a

[11] Ibid, p15

[12] Land Warfare Doctrine 3-0-3 *Formation Tactics 2016* Interim Publication, p10

near peer enemy, adversary capabilities in the space domain will match or even exceed friendly capabilities. Counter space weapons used to target satellite networks can be considered in four categories[13]:

a. Kinetic physical weapons attempt to strike directly or detonate a warhead near a satellite or ground station. The two primary types of kinetic physical weapons are direct ascent anti-satellite weapons that are ground launched and use their trajectory to close with the target or co-orbital anti-satellite weapons which are first placed in orbit then manoeuvred to strike the target.

b. Non-kinetic physical weapons such as lasers, high powered microwaves and electromagnetic pulse weapons can have physical effects on satellites and ground stations without making physical contact.

c. Electronic attacks target the method space systems transmit and receive data by jamming or spoofing radio frequency signals.

d. Cyber attacks target the data obtained from satellites and the systems that use this data. A cyber attack on a space system crosses the boundary between the space domain and the cyber domain.

13. The most misunderstood and overestimated of the five Domains is cyber. Cyber capabilities are largely the realm of the strategic level of engagement however the tactical level may experience the effects of cyber activities. Operations in the cyber domain can broadly be considered as offensive cyber operations or defensive cyber operations. Offensive cyber operations are those that target the enemies network while defensive cyber operations aim to protect friendly networks. The authorities to employ offensive cyber operations are usually held well above the manoeuvre commander.

14. The practical application of cyber effects at the tactical level is better articulated under the umbrella of Cyber and Electromagnetic Activities (CEMA)[14]. CEMA includes all activities that operate within the electromagnetic environment and includes the traditional Electronic Warfare effects employed at the Combat Brigade level and below[15]. Tactical advantage can be achieved by flexibly using or denying the enemy the use of the electromagnetic environment.

15. The effects available in both the space and cyber domains are best articulated as Deception, Disruption, Denial, Degradation and Destruction[16]. Deception aims

---

[13] Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, *Space Threat Assessment 2019*, Center for Strategic and International Studies, April 2019

[14] Joint Doctrine Note 1/18 *Cyber and Electromagnetic Activities*, UK Ministry of Defence, Development, Concepts and Doctrine Center, piii

[15] Major David M. Rodriguez, *The influence of electronic warfare on Operations Manoeuvre*, published in *Lethal and Non-Lethal Fires: Historical Case Studies of Converging Cross-Domain Fires in Large Scale Combat Operations*, Edited by Thomas G. Bradbeer, Army University Press, Fort Leavenworth, Kansas, 2018, p49

[16] JP3-14 *Space Operations*, Curtis E. Lemay Center for Doctrine Development and Education, 19 June 2012 pA1

to provide multiple dilemmas to the adversary and draw attention from the friendly main effort. Disruption reduces the effectiveness of the enemy network while denial will prevent enemy access to their networks for a period of time. Degradation seeks to target nodes within the enemy network leading to destruction where the network will collapse. A near peer enemy will be capable of employing space and cyber effects against friendly forces and a mitigation method is essential to support manoeuvre operations.

PRACTICAL APPLICATION OF MULTI DOMAIN OPERATIONS

16. The US is not the only military with an interest in the application of Multi Domain Operations. On 1 August 2008 Georgian separatists from the border provinces of South Ossetia and Abkhazia, formally a part of Georgia but dense with ethnic Russians, shelled the Georgian village of Tskhinvali. Georgian soldiers rapidly mobilized to recapture the village however on 9 August, Russian troops supported by air strikes and a naval blockade on the coast entered the provinces to conduct peace enforcement operations. At the same time Russian forces crossed the border, Georgian websites were hacked and the nations entire internet service rerouted to Russian servers, which shut them down. Georgian citizens couldn't gain information on what was happening, military commanders couldn't pass orders and Russia owned the narrative on what was occurring[17]. Including the use of space based reconnaissance and PNT assets to support the operation makes this a text book example of Multi Domain Operations applied with speed and skill to dis-integrate an adversary network and support decisive action. It could be argued that Georgia is not a near peer to Russia however multi domain effects were effectively applied across the competition spectrum at the strategic and operational levels to achieve decisive advantage at the tactical level.

THE BREACH MINDSET IN MULTI DOMAIN OPERATIONS

17. The fundamentals of the breach are Suppress, Obscure, Secure, Reduce and Assault or the acronym SOSRA[18]. The breach mindset is an operational framework to achieve isolation of an objective and determine the minimum force ratio to achieve conditions favourable to the attack[19]. The breach mindset allows the tactical commander to prioritise and control those effects essential to achieve the objective and begins an iterative process for planning subsequent operations.

18. Multi Domain Operations seeks the convergence of multi domain effects at a specific point and time to enable friendly force freedom of action. Considering each tactical objective as a multi domain obstacle to be reduced allows the use of

---

[17] Fred Kaplan, *Dark Territory: The Secret History of Cyber War*, Simon and Schuster, 2017

[18] Land Warfare Doctrine 3-0-3 *Formation Tactics 2016* Interim Publication, p98

[19] Ryan Orsini, *Surrounded yet Unaware: Achieving Isolation in Future Urban Terrain*, published on the Small Wars Journal website, 2018

the breach mindset or SOSRA as a means to phase and synchronise multi domain effects at a time and place of our choosing. All tactical manoeuvre must be enabled by ISR and this Know function is a precursor before any Multi Domain Operation commences. The fundamentals of the breach mindset to synchronise Multi Domain Operations can be expanded as follows:

a. **Suppress** the enemy's ability to observe or interfere with our actions. Suppression focusses on the enemy and their capabilities that can directly observe friendly activities. The objective of the suppression phase is to attrite the enemies ability to perceive the friendly main effort.

b. **Obscure** what we are doing from the enemy. Obscuration focusses on friendly actions that cause uncertainty for the enemy commander in determining the friendly main effort. If synchronised across multiple domains, the enemy commander will be presented with multiple dilemmas and their decision making process will be impeded.

c. **Secure** friendly actions from being interdicted by the enemy. Security focusses on friendly efforts to protect the decisive action from being deliberately targeted by the enemy and is broader than just the key terrain. In Multi Domain Operations command and control is essential to synchronise cross domain effects and protection of friendly networks in all domains will be necessary. An important component of this phase is the ability to operate in a communications degraded environment.

d. **Reduce** the enemy and their ability to influence our actions at the specified time and place. Reducing the enemy considers kinetic and non-kinetic effects across all domains to deliberately target the enemy at the time and place of our choosing. The reduction phase will be decisive to seize the initiative from the enemy and set the stage for subsequent offensive operations.

e. **Assault** in order to seize the initiative following dis-integration of the enemy and exploit opportunity. The Assault phase comes with considerable risk as the enemy will likewise be seeking to deceive us into believing weakness exists. If friendly forces become desynchronised across the multiple domains, they will be vulnerable to isolation from support and interdiction by enemy cross domain effects. An understanding of risk and how to mitigate friendly weakness in order to exploit opportunity using multi domain effects is essential to the tactical commander following dis-integration of the enemy.

THE PRACTICAL CONSIDERATION OF RISK

19. The 11 July 2014 Russian Strike on Ukrainian forces at Zelenopillya highlights the risk to force from becoming isolated from support[20]. The attack was a pre-emptive undertaking against Ukrainian brigades, postured in assembly areas, which were preparing to conduct offensive action against Russian and partisan forces. The buzzing of tactical drones and cyber-attacks targeting Ukrainian communications preceded the strike. An onslaught of rockets and artillery fell on the Ukrainian position shortly after the drones arrived, leaving thirty Ukrainian soldiers dead, hundreds more wounded, and over two battalions worth of combat

[20] Amos Fox, *The Russian Ukrainian War: Understanding the Dust Clouds on the Battlefield*, 17 January 2017, Modern War Institute Website

vehicles destroyed. Ukrainian forces became isolated from support, bunched up due to degradation of their command and control networks and vulnerable to destruction by offensive fires. Prior to the strike, the Ukrainian forces had been successfully on the offensive and this is an example of the need to mitigate risk when exploiting opportunity.

20. Risk is a concept that is often misunderstood and the difference between seizing an opportunity or taking a gamble poorly perceived. Tactical risks are those opportunities that if taken win a battle at hand[21]. But how does the tactical commander differentiate between a gamble and seizing the opportunity? Speculative Risk is a category of risk that when undertaken results in an uncertain degree of gain or loss[22]. Speculative risks are made as conscious choices, not just as a result of uncontrollable circumstances and come with a chance of either a gain or a loss. A speculative risk without any mitigations is a gamble. Speculative risk when appropriate mitigation measures are in place is an opportunity. Contingency planning, use of a reserve and economy of force operations are examples of mitigations to speculative risk[23] for the tactical commander. The decision to take risk must be made in consideration of the advantage for the commander in doing so.

JOINT WARFARE ACTIVITY 2019 – 3 ANZAC BRIGADE CROSSING OF THE COLUMBIA RIVER

21. The Joint Warfare Activity 2019 saw 3rd Combat Brigade reinforced with a NZ Battle Group, join Multi National Division Bayonet with formations from Canada, the UK and US, as the Coalition Force Land Component Command for combat operations to liberate the nation of Movari from invading Katari forces in 2028. The first deliberate operation of the Multi National Division's advance involved 3 ANZAC Brigade manoeuvring to conduct an opposed crossing of the Columbia River then breaking out to pursue defeated enemy forces. Commander 3 ANZAC Brigade[24] planned the operation using the breach mindset:

a. **Know**. Space, Air and Land capabilities were used to Know the Battlespace during the weeks prior to the commencement of ground combat operations. CEMA capabilities were used to Know and Shape the electromagnetic environment immediately surrounding the objective.

b. **Suppress**. Air, Land and Maritime assets conducted Strike actions against enemy capabilities. The commencement of ground manoeuvre was synchronised with a Joint Task Force CEMA action to degrade adversary command and control networks across the battlespace and isolate local ground commanders from higher echelon. Air and Land CEMA assets were used to Deny ground forces use of their local command and control networks.

---

[21] Kevin Benson, *Tactical Risk in Multi-Domain Operations,* 25 April 2019 published on the Modern War institute website.

[22] Ibid

[23] Ibid.

[24] Brigadier Scott Winter verbal orders to 3 ANZAC Brigade 28 April 2019

c. **Obscure**. Land and Air CEMA assets were used to Deceive the enemy commander regarding the Main Effort for the attack. Multi-National Division Bayonet conducted synchronised Land actions to create multiple dilemmas for the enemy commander and draw adversary ISR assets away from the decisive action to cross the Columbia River.

d. **Secure**. Land and Air manoeuvre were used to strike the objective and secure the crossing site. Maritime, Air and Land capabilities provided a defensive bubble to Shield 3 ANZAC Brigade activities. Adversary disruption to friendly electromagnetic environment actions was mitigated through Shielding the network.

e. **Reduce**. Land capabilities reduced the obstacle while Air, Land and Maritime assets Shielded friendly actions from enemy interdiction as combat power was built up on the opposite bank.

f. **Assault**. 3 ANZAC Brigade broke out of the bridgehead line in an advance to contact. Air and Land assets were used to Strike enemy defensive positions while Air, Land and Maritime capabilities Shielded the force during manoeuvre and in the CEMA domain.

22. The risk to 3 ANZAC Brigade of being separated from support and destroyed by enemy offensive fires was mitigated through the use of a reserve, the application of higher echelon fires to support manoeuvre and an integrated fires plan. Successful crossing of the Columbia River presented an opportunity to the Land Component Command however the enemy was a long way from dis-integration and remained a potent threat if the force became isolated.

Conclusion

23. The Multi Domain Operations concept has operationalised Joint Warfare doctrine as the US Army prepares for competition below and including armed conflict against a US near peer adversary. The concept seeks to synchronise effects within the domains of land, air, maritime, space and cyber at the strategic, operational and tactical levels to create multiple dilemmas for an enemy commander leading to dis-integration of adversary networks and a return to competition below armed conflict. The Australian Combat Brigade as part of a Multi-National Land Component Command needs to understand and synchronise Multi Domain effects to achieve decisive action on the future battlefield. The breach mindset or SOSRA provides a method for the manoeuvre commander to synchronise multi domain effects in support of decisive action to **Suppress** the enemy's ability to observe or interfere with our actions; **Obscure** what we are doing from the enemy; **Secure** friendly actions from being interdicted by the enemy; **Reduce** the enemy and their ability to influence our actions at the specified time and place; and **Assault** in order to seize the initiative following dis-integration of the enemy and exploit opportunity. A US near peer adversary will contest friendly actions at all stages of the conflict and the risk of isolation must be mitigated when exploiting the opportunity presented through successful synchronisation of Multi Domain Operations.