ALL DOMAIN ACCESS” IN THE LITTORALS A JOINT CONCEPT TO HYBRID WARFARE

OSMAN GUL
Turkish Naval War Colleges Istanbul, Turkey

Abstract- Since the end of Cold War, conventional warfare has yielded to hybrid warfare in the littorals. This type of war is not new, but what makes today’s hybrid warfare unique is, state and non-state actors in the littorals can easily acquire Anti-Access and Area Denial (A2/AD) capabilities to counter conventional forces. Today, contrary to common belief, intervention from the sea to the hybrid warfare needs a new operational function “All Domain Access”, defined in “U.S. A Cooperative Strategy for the 21th Century Sea Power-2015” document, as “The ability to project military force in contested areas with sufficient freedom of action to operate effectively”, can play a critical role for NATO’s current and future maritime operations.

Index Terms- Hybrid Warfare, A2/AD Threats, All Domain Access, Crimean Crisis, NATO Maritime Command.

I. INTRODUCTION

From the very beginning of recorded history, peoples and nations have sought to be powerful at sea. “Dominance of the seas has generally been essential for the command of the land. In 480 BC, for example, the ancient Greeks used an Anti-Access/Area Denial (A2/AD) strategy at Salamis, denying the invading Persians the ability to land a huge army on the Peloponnesse.”[1] Although this form of warfare was inherently conventional, technological advances in A2/AD capabilities such as missile defense systems, weapon of mass destruction, mines, torpedoes, and submarines have changed the nature of this warfare.

As Milan Vego has stated that “after the collapse of the Soviet Union and Warsaw Pact, the political, military, demographic, and economic importance of the littorals has steadily increased over the past two decades.”[2] Especially, the Crimean Crisis illustrates that NATO faces a “hybrid”[3] warfare which involves multilayered efforts designed to destabilize a functioning state and polarize its society. Unlike conventional warfare, hybrid warfare is population-centric. The adversary tries to operate inside civilian areas to influence policy-makers and key decision makers by combining A2/AD capabilities with subversive efforts. In order to address new threats, “NATO has adopted a new maritime strategy to help resolve critical security challenges and implemented four core tasks: deterrence and collective defense, crisis management, cooperative security and maritime security in 2011.”[4] But, the illegal annexation of Crimea and ongoing military aggression in Ukraine has suggested that as difficult as hybrid warfare has been, the operational fusion of irregular and conventional A2/AD capabilities embedded in population may be even more complicated.

In hybrid warfare “any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the battle space to obtain their political objectives.”[5] Hybrid type of war approaches are not new, but what makes today’s hybrid war unique is, with the technological advances, state and non-state actors in the littorals can easily acquire A2/AD capabilities to counter conventional forces. In other words, “The ability to adapt systems, and in particular information systems and structures, and strategies often allow hybrid forces to outmaneuver conventional forces.”[6] In order to deal with hybrid warfare and to ensure long-term security and stability in the littorals, NATO Maritime Command should develop a new joint concept based on “All Domain Access”[7] against A2/AD threats in the hybrid warfare.

II. OPERATIONAL LEVEL OF WAR: CONVENTIONAL WARFARE VERSUS HYBRID WARFARE

In war at sea, the main operational objective is commonly for the stronger side is to obtain sea control, while the weaker side tries to obtain sea denial. According to Milan Vego, “the operational level of war at sea emerged during the Crimean War (1854-1856) when several British and French steam-powered ship squadrons operated in the Baltic Sea, the Black Sea, and Far East.”[8] The main objective of these maritime operations was to obtain Sea Control or Sea Denial. With the new technological advances, namely, A2/AD threats have limited the ability of the stronger side’s fleet to operate effectively in the littorals. This conventional character of the operational level of war continued to the end of the Cold War in 1991. This in turn had a major impact on the international political and security environment. Since the end of the Cold War, conventional warfare has yielded to hybrid warfare in the littorals. Crimean Peninsula has become a new area of hybrid warfare. Today, “the rise of hybrid warfare in the littorals has not represented the end of traditional or conventional warfare, but it does present a complicating factor for defense planning in the 21st century.”[9]
Contrary to common belief, intervention from the sea to hybrid warfare needs a new operational function other than sea control or sea denial. Because, conventional forces in the littorals are more vulnerable to A2/AD threats in hybrid warfare. The term “All Domain Access”, as a new operational function, defined in “U.S. A Cooperative Strategy for 21th Century Seapower-2015” document, as “the ability to project military force in contested areas with sufficient freedom of action to operate effectively”[10], can play a critical role for NATO’s current and future maritime operations.

Given the nature of both conventional warfare and hybrid warfare, principal objectives and center of gravities of these type of wars differentiate. The following figure depicts the differences between conventional warfare and hybrid warfare. Unlike conventional warfare, in hybrid warfare for the stronger side principal objective is to obtain “All Domain Access” and enemy center of gravity is A2/AD Threats.

![Figure-1: Conventional Warfare versus Hybrid Warfare.][11]

III. FORWARD NAVAL PRESENCE IN THE LITTORALS: A2/AD THREATS IN HYBRID WARFARE

Forward naval presence is a manageable component, described as “a key enabler of regional stability which enables familiarity with the operational environment, as well as contributing to an understanding of the capabilities, culture, and behavior patterns of regional actors, and it enables influence.”[12]

According to Geoffrey Till, forward naval presence is “the exercise of naval diplomacy in a general way involving deployments, port visits, exercising and routine operating in areas of interest to declare interest, reassure friends and deter.”[13] In this respect, forward naval presence matters in terms of factor time. It can be routine and continuous to demonstrate a permanent interest or it can be periodic to demonstrate a temporary interest. Although NATO Maritime Command has four Standing Naval Forces as a response force that provides the Alliance with a naval presence, it lacks persistent situational awareness in the littorals which involves integrating capabilities and synchronizing efforts in a manner that applies force from different domains to shock, disrupt, and defeat opponents.

In current Crimean Crisis, after non-state actors seized Sevastopol Naval Base in 2014, Russian Black Sea Fleet took control of the Crimean Peninsula littorals. In addition, the essence of A2/AD threats in this hybrid warfare constrained the forward presence of NATO naval forces. Due to the lack of situational awareness and the high level of risk, NATO decision makers hesitated to task naval forces to conduct sea control or sea denial operations in the Black Sea. This conventional approach would be risky in that enclosed sea. Besides, this hybrid warfare illustrates that enclosed sea such as Black Sea is susceptible to influence from the land and sea Anti-Access (A2) and Area Denial (AD) threats.

In the light of the challenging security environment to the east of the Alliance’s borders, NATO Defense Ministers decided on 5 February 2015 to enhance NATO Response Force (NRF).[14] In this context, it was agreed that four “Standing NATO Maritime Groups (SNMG)”[15] would be enhanced to support maritime situational awareness and to conduct full spectrum conventional maritime operations.

In March 2015, NATO Standing Maritime Group-2 (SNMG-2) was deployed to the Black Sea to reassure Allies in the region of the Alliance’s collective defense and resolve. NATO ships assigned to SNMG-2 completed their participation in joint NATO training exercises and maritime situational awareness operations in the Black Sea. SNMG-2 forces trained on anti-air and anti-submarine warfare procedures and also responded to simulated small boat attacks and maneuvers with the ships in close proximity to one another. In this sense, NATO Maritime Forces focused on more conventional maritime operations.

IV. ALL DOMAIN ACCESS IN LITTORALS

Today, as the hybrid warfare in Crimean Peninsula littorals, demonstrates that state or non-state actors can limit friendly freedom of action or put naval forces at risk with their A2/AD threats. Since the nature of hybrid warfare is a mixture of asymmetric, irregular, conventional, and population-centric, the lack of situational awareness in the operational environment results in collateral damage. Because state or non-state actors can exploit non-combatants as a fake target.

In May 2015, at the end of meeting NATO Foreign Ministers in Antalya, Turkey, the NATO Secretary General expressed that “NATO is concerned by Russia’s efforts to further build up its presence in the Black Sea region, warning that this could have further implications on regional stability.”[16] As seen in this Crimean case, the complexity of hybrid warfare has showed that NATO Maritime Command needs “All Domain Access” in the littorals to deter conflict, respond to crisis and defeat aggression.

“All Domain Access” is a new operational function consists of five operational elements: “Battlespace Awareness, Assured Command and Control,
Cyberspace Operations, Electromagnetic Maneuver Warfare and Integrated Fires.”[17]
Employed in coordination with naval forces and capabilities, All Domain Access can allow the NATO Maritime Command to provide cross-domain capability to the operational commander of Combined Joint Task Force through the All Domain Access operational elements.

V. DEVELOPING A NEW JOINT CONCEPT FOR HYBRID WARFARE

“The current NATO deterrence policy for hybrid warfare is based on a rapid military response.”[18] But, in times of crisis, this approach has potential weaknesses to counter A2/AD threats in the littorals. Regardless of how rapid a response maybe, projecting naval forces to a contested area swept by A2/AD threats. To effectively deal with A2/AD threats in the littorals, NATO Maritime Command should develop a new joint concept for hybrid warfare. This concept must be proactive rather than reactive to synchronize its efforts from the peacetime to crisis with the All Domain Access operational elements: “Battlespace Awareness, Assured Command and Control, Cyberspace Operations, Electromagnetic Maneuver Warfare and Integrated Fires”[19] in sea, air, land, space and cyberspace domains. Therefore, the cumulative effect of all domains that permits the conduct of joint maritime operations without effective opposition or prohibitive interference is essential to Combined Joint Task Force mission success. In this respect, it is critical to achieving cross-domain synergy. Seeking combinations of actions to fulfill concentration or synergy in conventional and non-conventional domains can enable the projection of focused capabilities in the operational environment.

VI. CROSS-DOMAIN SYNERGY

“Cross-domain synergy has clear utility at the operational level of war for operating at the speed of the problem.”[20] In military application, “cross-domain synergy is the use of two or more domains to achieve a military advantage. This frequently involves application of capabilities from one domain to another, with the principal aims of improving operational performance and reducing unnecessary joint force redundancies.[21] Achieving cross-domain synergy requires approaching A2/AD threats in hybrid warfare from a multi-domain perspective. Understanding of the capabilities of the adversary in operational environment entails high reliance on friendly ISR systems. On the other hand, in hybrid warfare, non-state and state actors intentionally attempt to reduce the effective use of friendly ISR systems. Friendly ISR systems will be the decisive point of any adversary’s strategies, requiring a higher degree of protection. In order to shock, deter and defeat the A2/AD threats, cross-domain synergy must be created among the All Domain Access operational elements. This synergy should focus on the adversary’s kinetic and non-kinetic systems rather than its weapons. As an example, Combined Joint Task Force can promptly shock the adversary’s counter ISR and defense systems by establishing superior information dominance to synchronize ISR, C2, cyber and electromagnetic capabilities. This approach suppresses the A2/AD threats before they have even been launched.

CONCLUSION

This paper aims to advocate the borderless nature of the sea and naval diplomacy make sea power one of the best platforms to contribute to the regional security and stability. Today, lesson learned from Crimean Crisis, the operational fusion of irregular and conventional A2/AD capabilities embedded in population has made the littorals even more complicated. In this hybrid warfare, especially the possible use of lethal weapons such as missile defense systems, explosive laden small boats, mines, torpedoes and weapon of mass destruction (nuclear, radiological, chemical, biological) has challenged the freedom of action of NATO naval forces and put them at risk. Considering that current forward presence of NATO naval forces has potential weaknesses to counter A2/AD threats, lack of persistent situational awareness in the littorals favors the adversary. Intervention from the sea to the hybrid warfare requires a new operational function beyond sea control or sea denial. As a new operational function, All Domain Access, can play a critical role for NATO’s current and future maritime operations in hybrid warfare. Because, this function is key for the success of dealing with hybrid warfare in the littorals. Employed in coordination with naval forces and capabilities, All Domain Access can allow the NATO Maritime Command to provide cross-domain synergy to the operational commander of Combined Joint Task Force through its operational elements. Given the potential dangers and adverse consequences of the ongoing Crimean crisis, NATO should develop a new joint concept based on “All Domain Access” for hybrid warfare in the littorals. Otherwise, regional security and stability can be contested by state and non-state actors’ A2/AD strategies. NATO Maritime Command requires a cooperative approach to implement this new operational function to counter A2/AD threats in hybrid warfare. As described in Figure-2, developing a joint concept for hybrid warfare will be more cost-effective and feasible. In general, this concept consists of three core components: Maritime Capability Building (MCB), Maritime Situational Awareness (MSA) and Maritime Security&Stability Operation (MSSO).
In this concept, operational function, “All Domain Access”, needs to have comprehensive Maritime Capability Building (MCB) under ISR systems, Defense systems and Platforms subheadings to counter Anti-Access (A2) and Area Denial (AD) threats. It also aims to establish persistent Maritime Situational Awareness (MSA) with the assistance of ISR systems in order to obtain freedom of action in the littorals. On the other hand, the protection of friendly ISR systems is the critical vulnerability. This must be protected by Defense systems from peacetime to crisis. The synchronization of All Domain Access operational elements: Battlespace Awareness, Assured Command and Control, Cyber Operations, Electromagnetic Maneuver Warfare and Integrated Fires in Maritime Security and Stability Operations (MSSO) will provide dominance to the NATO Maritime Command in hybrid warfare.

In addition, there might be some takeaways for the NATO Maritime Command in the Baltic Sea and East Mediterranean littorals. These littorals have some potential challenges for the regional security. In order to keep the stability in these littorals, NATO Maritime Command should implement this joint concept to overcome possible hybrid type of war in the near future.

REFERENCES

[3]. [3] The term “hybrid” have recently been used to express the seeming increased complexity of war, the multiplicity of actors involved, and the blurring between simple categories of conflict. (Richard M. Crowell, Analyzing Hybrid Warfare, 2014, p.2.)
[7]. [7] “All Domain Access” is defined as the ability to project military force in contested areas with sufficient freedom of action to operate effectively. (A Cooperative Strategy for the 21st Century Seapower,
[15]. [15] The Standing NATO Naval Maritime Groups (SNMGs) composed of the SNMG1 and the SNMG2; and the Standing NATO Mine Countermeasures Groups (SNMCMG1 and SNMCMG2).

★★★