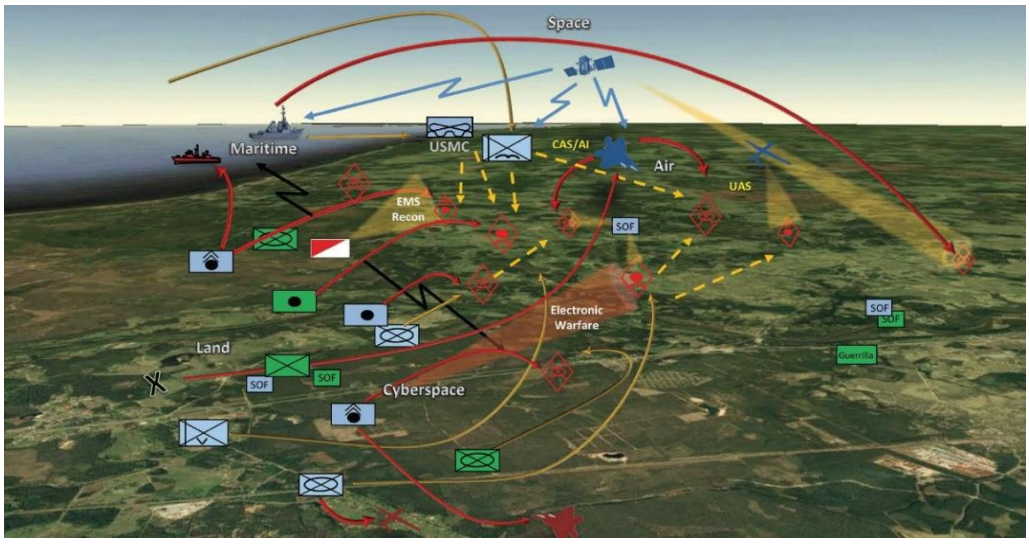
BIPSS Commentary
www.bipss.org.bd October - 2024
BIPSS Towards a Secure World

Multi-Domain Defense Force for the Future Battlespace

Mohosina Mostofa[1]

Introduction

Warfare today is changing quickly due to new technologies and the rise of different types of threats. In the past, wars were fought mainly on land, at sea, or in the air. However, modern conflicts now take place across many different areas, or "domains"—including not just land, sea, and air, but also space and cyberspace. To handle these complex challenges, militaries around the world are shifting toward what is called a "multi-domain defense force."



Source: Modern War Institute

A multi-domain defense force means that the military is prepared to fight across all these areas at the same time. Instead of just focusing on one type of attack—like a land battle or an air strike—modern defense strategies involve coordinating efforts in every domain. For example, if a country

[1]Mohosina Mostofa is a Research Assistant at the Bangladesh Institute of Peace and Security Studies (BIPSS). She completed her BSS & MSS in International Relations from the Bangladesh University of Professionals (BUP).

is hit by a cyberattack while facing a threat in the air or on land, its defense force would need to respond to all these threats together, using the best tools and strategies from every domain.

This approach is becoming more important as enemies find new ways to attack, especially through cyberspace and even space. Cyberattacks can shut down communications or damage important systems, while control of space—like satellites that are used for navigation or surveillance—has become critical for military operations. The ability to defend and attack across all these domains gives a country more options and flexibility in handling threats. As the nature of warfare continues to evolve, countries that build multi-domain defense forces will be better equipped to face modern challenges. This type of force will help them stay prepared and strong, no matter where or how future battles are fought.

Evolution of Warfare: From Single to Multi-Domain Conflicts

The intricacy of some of the current security challenges is reflected in the evolution of modern warfare, where conflicts are no longer limited to geographical locations. Recent conflicts, like the Armenia-Azerbaijan war over Nagorno-Karabakh (2020, 2023), highlight the shift to multi-domain operations. Azerbaijan's use of drones for reconnaissance and precision strikes played a key role in gaining air superiority, while cyberattacks targeted Armenia's military communications.[2] The integration of cyber, air, and space technologies, including satellite intelligence, allowed Azerbaijan to coordinate more effective strikes and maintain an advantage on the ground.

Source: Wikipedia

[2]Dixon, Robyn. 2020. "Azerbaijan's Drones Owned the Battlefield in Nagorno-Karabakh — and Showed Future of Warfare." *Washington Post*, November 11, 2020.

Another recent example of multi-domain operations is the ongoing tensions in the South China Sea between China and neighboring countries like the Philippines, Vietnam, and Taiwan. China has employed a combination of naval patrols, air operations, and cyber intrusions to assert its dominance in the region. In 2023, there were multiple reports of Chinese cyberattacks targeting the infrastructure of Southeast Asian countries, aiming to gather intelligence and create instability, while simultaneously deploying naval and air forces to assert territorial claims.[3] This blend of military and non-military tactics shows how multi-domain conflicts are shaping modern warfare.

Source: The Pacific Report

Key Domains in Modern Warfare: Land, Sea, Air, Space, and Cyberspace

CASE STUDY- The Russia-Ukraine War

Land Domain: The land domain remains the traditional battlefield where ground forces engage in direct combat. In the ongoing Russia-Ukraine war (2022-present), ground operations have been central to the conflict. Ukrainian forces, supported by Western-supplied weapons such as HIMARS rocket systems, have successfully used land-based artillery and infantry units to push back Russian

[3]Sebenius, Alyza. 2023. "China's Hackers Are Expanding Their Strategic Objectives." Default. December 5, 2023. https://www.lawfaremedia.org/article/china-s-hackers-are-expanding-their-strategic-objectives.

forces in key areas, including the successful counteroffensive in the Kharkiv region in 2023.[4] These land operations, though conventional, have been integrated with other domains for greater effectiveness.

Sea Domain: In the Russia-Ukraine war, control of the Black Sea has been crucial. Russia's naval blockade of Ukrainian ports severely impacted Ukraine's grain exports, causing a global food crisis. In response, Ukraine used sea drone named Magura V5 to strike Russian naval ships recently in 2024, including the 2022 sinking of the *Moskva*, the flagship of Russia's Black Sea Fleet.[5] This demonstrated the growing importance of naval power and maritime control in modern warfare, with drones and naval forces being used to disrupt enemy supply lines and maritime operations.

Source: Al Jazeera

Air Domain: Russia has used cruise missiles and drones to target critical Ukrainian infrastructure, including power grids and communication networks. In response, Ukraine has deployed air defense systems, including advanced Western technology like the NASAMS, to counter these air

[4]Motamedi, Maziar. 2024. "Long-Range Missiles to Hit Russia: Where Does NATO Stand on Ukraine Demand?" Al Jazeera. September 25, 2024. https://www.aljazeera.com/news/2024/9/25/long-range-missiles-to-hit-russia-where-does-nato-stand-on-ukraine-demand.

[5]*Www.bbc.com*. 2024. "Ukraine War: The Sea Drones Keeping Russia's Warships at Bay," March 12, 2024. https://www.bbc.com/news/world-europe-68528761.

threats. Additionally, Ukraine's use of drones in the air domain has been critical for reconnaissance and precision strikes.

Space Domain: Ukraine has relied heavily on satellite services like Starlink, provided by SpaceX, for secure communications after Russian cyberattacks disrupted its traditional communication infrastructure.[6] Space-based intelligence has also been critical in providing Ukraine with real-time battlefield information, helping its forces to track Russian troop movements and target key military installations. Russia, in turn, has attempted to jam or disrupt these satellite services, highlighting space as a critical battleground in modern warfare.

Cyberspace Domain: Russia launched extensive cyberattacks against Ukraine, targeting its banking systems, energy grids, and government communications. These attacks were designed to cripple Ukraine's ability to respond effectively and create chaos within the country. However, Ukraine, with the support of international cyber defense teams, has managed to counter many of these attacks. In addition, Ukrainian hackers have launched retaliatory attacks on Russian websites and infrastructure.

Source: MDPI

[6]Gak, Nick Paton Walsh, Alex Marquardt, Florence Davey-Attlee, Kosta. 2024. "Ukraine Relies on Starlink for Its Drone War. Russia Appears to Be Bypassing Sanctions to Use the Devices Too." CNN. March 26, 2024. https://edition.cnn.com/2024/03/25/europe/ukraine-starlink-drones-russia-intl-cmd/index.html.

Countering Multi-Domain Threats: Adapting Defense Strategies

Recent global conflicts show that a multi-domain approach is essential for defending against the wide variety of modern attacks, which often happen across multiple platforms at once. A key example can be seen in the escalating tensions between China and Taiwan. Since 2021, China has demonstrated multi-domain operations through a combination of military exercises and cyberattacks aimed at pressuring Taiwan. In response, Taiwan has adapted by investing in comprehensive multi-domain defense strategies. It has enhanced its air and naval capabilities, strengthened cyber defenses, and increased cooperation with allies like the United States and Japan for intelligence sharing and military support.[7] Taiwan has also focused on building cyber resilience, developing rapid response strategies to counter cyber intrusions while maintaining robust air and sea defenses.

Some different defense strategies that can be adapted and be proved crucial for concerning countries are discussed below.

Joint Operations: A key method is integrating capabilities across various military branches. For instance, during *Operation Inherent Resolve* in Syria, U.S. forces combined airpower, cyber operations, and intelligence to degrade ISIS's command structure.[8] This exemplifies how forces can adapt by synchronizing efforts across domains for a shared goal

Leveraging Technological Innovation: As military domains converge, adopting new technologies becomes critical. The Israeli Defense Forces (IDF) have integrated unmanned aerial vehicles (UAVs), cyber tools, and AI to execute precision strikes on Hamas in recent conflicts

[7]Uppal, Rajesh. 2024. "Taiwan's Military Renaissance: Advanced Capabilities for a Double-Level Deterrence - International Defense Security & Technology." International Defense Security & Technology. 2024. https://idstch.com/geopolitics/taiwans-military-renaissance-advanced-capabilities-for-a-double-level-deterrence/.

[8]"Special Report: Operation Inherent Resolve." 2017. U.S. Department of Defense. 2017. https://dod.defense.gov/OIR/.

which reveals how technology can enhance battlefield awareness and accuracy.[9] By adapting their strategies, they improved both offensive and defensive operations.

Embracing Non-Traditional Domains: Modern warfare requires incorporating the cyber and space domains. In 2023, NATO's joint training exercises emphasized space and cyber capabilities, preparing forces to defend against cyberattacks and enhance satellite communication reliability.[10] Such adaptations highlight the importance of staying versatile when operating across both physical and digital realms.

Challenges in Building a Multi-Domain Defense Force

Building a Multi-Domain Defense Force (MDDF) presents a range of challenges that involve integrating complex systems, coordinating efforts across different domains, and ensuring seamless communication. Modern conflicts demand flexibility and rapid adaptation, but achieving this across land, sea, air, space, and cyber domains is a true hurdle. Recent examples highlight these challenges:

Technological Integration: One of the biggest difficulties is the integration of advanced technologies across domains. Military units must adopt cutting-edge systems like drones, artificial intelligence (AI), cyber tools, and satellite communication, which need to operate in a unified way. In the 2020 Nagorno-Karabakh conflict, Azerbaijan faced coordination issues despite their advanced UAV systems. While their drone technology was successful in striking Armenian forces, integrating cyber intelligence and communication systems with ground units and air power remained a challenge.

Interoperability Between Forces: Ensuring that military branches and allied forces can work together is a significant challenge. The U.S. and Japan, for example, have been working to improve joint operations across air, land, and sea. In 2023, during joint exercises in the Indo-Pacific, they

[9]Davies, Harry, Bethan McKernan, and Dan Sabbagh. 2023. "'The Gospel': How Israel Uses AI to Select Bombing Targets in Gaza." *The Guardian*, December 1, 2023, sec. World news. https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets.

[10]NATO. 2024. "Cyber Defence." NATO. July 30, 2024. https://www.nato.int/cps/en/natohq/topics_78170.htm.

found challenges in communication and coordinating intelligence sharing across different platforms, as both militaries used separate technologies and systems.[11] Such challenges limit the effectiveness of multi-domain operations, especially when real-time data is crucial.

Coordination Across Domains: Synchronizing operations across different domains is another hurdle. The U.S. Air Force's *Red Flag* exercises (2022) highlighted how difficult it can be to coordinate simultaneous attacks across air, land, and cyber domains.[12] During these exercises, integrating data from various sources (satellites, drones, and ground units) and ensuring rapid decision-making in fast-paced scenarios exposed gaps in coordination. These coordination challenges can weaken the overall effectiveness of multi-domain strategies.

Cybersecurity Risks: As militaries become more reliant on advanced technology and interconnected systems, they also become more vulnerable to cyberattacks. A recent example is the cyberattacks faced by the Australian government in 2021, which targeted critical defense and infrastructure systems. The attacks revealed vulnerabilities in Australia's defense systems and highlighted the growing need for strong cyber resilience within multi-domain operations. These attacks showed how digital infrastructure can be compromised, weakening the entire defense strategy.

Prospects for Multi-Domain Defense Integration in 2025

The prospects for MDDF in 2025 appear to be advancing rapidly, with several countries and alliances actively developing integrated capabilities to address the increasingly complex security environment.

- One significant development is the U.S. Army's Multi-Domain Task Forces (MDTFs), which are central to its future defense strategy. The MDTFs' success has already been seen

[11]"Modernizing US-Japan Command & Control Relationships for New Challenges | next Alliance Conference Summary: Tokyo 2023 < Sasakawa USA." 2023. Sasakawa USA. July 12, 2023. https://spfusa.org/publications/modernizing-us-japan-command-control-relationships-for-new-challenges-next-alliance-conference-summary-tokyo-2023/.

[12]"Red Flag-Nellis 24-2 Shapes the Future of Air Combat." 2024. Air Force. March 27, 2024. https://www.af.mil/News/Article-Display/Article/3720103/red-flag-nellis-24-2-shapes-the-future-of-air-combat/.

in their experimental deployment in the Indo-Pacific and Europe, where they are preparing for conflicts in regions where adversaries might use Anti-Access/Area Denial (A2/AD) capabilities.[13] In 2025, the continued refinement of MDTFs, including integration with new technologies like long-range hypersonic weapons and advanced cyber and electronic warfare tools, will be key to U.S. strategic deterrence efforts.

- NATO is also working on its Multi-Domain Operations (MDO) framework. By 2025, NATO aims to establish stronger doctrinal alignment, allowing member nations to operate cohesively across domains, particularly in countering near-peer adversaries like Russia and China.[14] This will require advanced systems for real-time data sharing and secure communications, ensuring rapid responses to multi-domain threats.
- Japan and Australia are also expected to bolster their MDDF capabilities by integrating cyber and space assets more effectively into their defense frameworks. Japan, for instance, has focused on counter-space and missile defense operations, while Australia is enhancing its partnerships with the U.S. for integrated deterrence in the Indo-Pacific

Way Forward

While it would be great to live in a world without war, where strategies like the Multi-Domain Defense Force (MDDF) are not needed, reality is different. Human history has shown that conflicts often come from people's desires for power, control, and selfish goals. As long as these exist, the need for strong defense systems will remain. MDDF is important because it combines operations across land, air, sea, space, and cyber domains, making it more capable of handling modern threats. We do not wish for war, but we have to accept that conflicts are likely to happen, and being prepared is essential. The MDDF helps ensure countries can protect themselves in an increasingly unpredictable world. So, while we might hope for peace, we must also be ready for whatever comes.

[13]"Multi-Domain Effects Battalion: Space Integration and Effects in Multidomain Operations." n.d. Www.armyupress.army.mil. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-2024/Multi-Domain-Effects-Battalion/.

[14]2024. Nationaldefensemagazine.org. 2024. https://www.nationaldefensemagazine.org/articles/2024/7/11/nato-to-adopt-overarching-russia-policy-at-2025-summit.