The Indo-Asia Pacific and the Multi-Domain Battle Concept


The United States Armed Forces are at a crossroads, facing both institutional and operational challenges. The character of war continues to change at a quick pace, requiring military leaders to reassess some of their core beliefs. This situation has led to the testing and refinement of concepts, capabilities, and people to ensure U.S. forces are ready for the conflicts of today and tomorrow. Without doubt, any future conflict will be increasingly complex and distributed, involving actions across multiple domains—land, air, sea, space, and cyber—by multiple military services, at times simultaneously. The nascent Multi-Domain Battle concept, some elements of which are described in a forthcoming white paper jointly authored by the Army and the Marine Corps, addresses the increasing complexity of the battlefield and its requirement for service integration. While still in development and experimentation, the concept is already affecting operational and resource decisions, especially in the Indo-Asia Pacific.

This article presents three topics to illustrate how we are thinking about the implementation of the Multi-Domain Battle concept in the Pacific Command area of...
responsibility. First, it briefly discusses the strategic situation in the Indo-Asia Pacific, which typifies the need for a new operating concept to integrate all the United States Armed Forces. Next, it describes the Multi-Domain Battle concept, including the three elements that help define its desired effects: joint integration, technology, and people. Finally, it presents a vignette of multi-domain battle as it might apply at the tactical level.

**The Strategic Context in the Indo-Asia Pacific**

Given that the international state of play in this region is more tenuous than ever, the Multi-Domain Battle concept is sorely needed. The region contains thirty-six countries in sixteen time zones, more than half the world's population, and twenty-four of the thirty-six megacities on Earth, and it covers more than half the world's surface area. The region contains three of the world's largest economies, seven of the largest militaries, and five of the United States' seven mutual defense agreement partners. According to Adm. Harry B. Harris Jr., commander of United States Pacific Command, “approximately $5.3 trillion in annual global trade relies on unimpeded access to sea lanes [such as those in the Straits of Malacca and the South China Sea, and] $1.2 trillion of this sea-based trade destined to, or exported from, the United States.” Additionally, “the Strait of Malacca alone sees more than 25 percent of oil shipments and 50 percent of all natural gas transits each day.” In addition, the area is disaster-prone, with its typhoons, earthquakes, volcanoes, tsunamis, and other events representing “over 60 percent of the world’s natural disasters.” In short, global prosperity hinges on the stability and security of this vast and complex region.

These demographic and economic dynamics interact with the increased rate of technological change to add to the political and military complexity found in the Indo-Asia Pacific. Dramatic technological shifts created by unmanned capabilities, robotic learning, artificial intelligence, nanotech, biotech, and big data are only expanding military competition between geopolitical rivals. Much of these new technological tools depend on the use of digital connectivity—with seven billion devices being connected to the Internet in 2016 and a projected fifty billion by 2020—only increasing the already dangerous situation in cyberspace and its dependence on space assets for connectivity.

Technological shifts are also feeding and increasing security challenges in the Indo-Asia Pacific, with some the world's most intractable problems among them.
Challenges include an increasingly belligerent North Korea that is sharing its increasingly capable missile technology with Iran, a growing China that is challenging international rules and norms, a revanchist Russia that is increasingly active in the Pacific with a provocative military posture, a continuing nuclear-backed friction between India and Pakistan, increasing activities by violent extremist networks operating in partner and ally nations, and political and diplomatic instability from changes in executive leadership of key regional allies and partners. The most dangerous threat in the Indo-Asia Pacific comes from regional actors with nuclear arsenals and the intent to undermine the international order. Sophisticated denial capabilities and less-than-military forces managed by the state but backed by large militaries with interior lines of communication create the danger of faits accomplis.

Like the international state of play, the military situation is also increasingly dangerous. Adversaries and enemies have learned from U.S. successes and failures over the last few decades. They recognize that U.S. strengths based on power projection, joint operations, and technological overmatch led to unprecedented tactical success. As such, adversaries have developed capabilities and concepts that attempt to remove those advantages, increasing the complexity of the battlefield for the United States Armed Forces. This has led to an increasingly contested global commons, with a loss of U.S. military dominance in the air and sea due to denial technologies and tactics. Whether opponents take gradual or sudden actions, the United States needs to significantly improve its strategic advantage in the Indo-Asia Pacific, or it will risk losing ground militarily, diplomatically, and economically.

Because of these strategic trends, both positive and negative, U.S. and partner forces need to maintain current military advantages and recapture those that have been lost. Reducing the risk of conflict and ensuring the stability of the current international system depend on our ability to deter key actors from aggressive and detrimental actions. We must interrupt enemy decision cycles and present enemies with multiple dilemmas that create uncertainty and paralyze their efforts. If aggression leads...
to conflict, however, we must be prepared to defeat our enemies unambiguously.

This approach is the driving force behind the Multi-Domain Battle Concept, which is designed to overcome denial technologies and jointly affect all domains to create localized areas of overmatch. These effects will then re-enable maneuver for the entire joint force operating in any region, thereby placing an enemy in a position of disadvantage so U.S. forces can gain the initiative.

**Elements of the Multi-Domain Battle Concept**

The Multi-Domain Battle concept may at first sound like nothing more than traditional joint operations. There is some truth to this. What we are trying to achieve—cross-domain effects—is not entirely new. For example, at Thermopylae and Salamis, the ancient Greeks employed both land and naval forces to defeat the invading Persians. Much closer to our own time, the United States of America owe their independence to the effective employment of American and French ground and naval forces against Lord Cornwallis’s army at Yorktown.

Another historical example is the Vicksburg Campaign during the American Civil War. With its ability to control navigation on the Mississippi River, Confederate Vicksburg’s artillery, infantry, and cavalry forces constituted a formidable anti-access and area denial challenge to Union forces. Union Gen. Ulysses S. Grant overcame that challenge only by combining the capabilities and effects of his own artillery, cavalry, and infantry forces with the naval ships led by Flag Officer Andrew Hull Foote.

The introduction of the airplane, the submarine, and the aircraft carrier in World War I, and the incorporation of mobile radio communications and radar systems in World War II, vastly increased a strategic commander’s ability to operate across several domains simultaneously. More recently, the development of AirLand Battle in the 1980s and then Air-Sea Battle in 2013 show military thinking evolving along the same general line—how to win decisively, even if outnumbered or technologically overmatched, by integrating operations in multiple domains to present enemies with multiple dilemmas. Different services have regularly supported each other in all domains. Therefore, when Harris says he wants the Army to provide effects outside the land domain, he is not asking it to do something without precedent. From 1794 to 1950, the Army was responsible for coastal and harbor defense, and later for the air defense of the homeland. The Army’s Warrant Officer Corps originated from the need in World War I for technical specialists to staff the Army’s undersea Mine Planter Service. The idea of or desire for cross-domain effects is not new.

While all the services are being asked to perform their missions in a manner not terribly different from the past, there will be differences. We in the Army can no longer simply focus on the land, leaving the air and sea to other services. Nor can the Marine Corps, Navy, Air Force, or Coast Guard simply focus on “their” domains. We must all better integrate our planning, operations, command and control, and effects across all the domains.

To achieve integration requires a new approach, a new mind-set. All U.S. forces must change their distinct service cultures to a culture of inclusion and openness, focusing on a “purple (or joint) first” mentality. The Army must further integrate a mission command mindset, where every person is empowered to gain the initiative based on his or her role and function. And it must focus on developing leaders who thrive in ambiguity and chaos.

**Joint integration.** The Multi-Domain Battle concept is expected to integrate three key areas: organizations and processes, technology, and people. Changes in organizations and processes will be designed to provide different and better-focused Army tools to joint forces to overcome the United States’ loss of superiority or parity in certain domains, particularly in the air, at sea, and within cyberspace. The Army can no longer focus exclusively on the

---

**Gen. Robert B. Brown, U.S. Army,** is the commanding general of United States Army Pacific (USARPAC). He has served over twelve years with units focused on the Indo-Asia Pacific region, including as commanding general, I Corps and Joint Base Lewis-McCord; deputy commanding general, 25th Infantry Division; director of training and exercises, United States Pacific Command (USPACOM) J7 (now J37); executive assistant to the commander, USPACOM; plans officer, USARPAC; and commander, 1st Brigade Combat Team (Stryker), 25th Infantry Division. Assignments in the generating force include commanding general, U.S. Army Combined Arms Center, and commanding general, Maneuver Center of Excellence.
land domain; as part of a joint force, Army forces must provide other services effects in their domains to overcome their operational challenges, and vice versa. This means change must focus on greater ability to have cross-domain effects and more seamless and effective integration across joint forces.

In United States Army Pacific (USARPAC), we are attempting this through three areas. The first is to design and experiment with flexible command and control designs, tailorable and scalable units, and flexible policies in key areas. Second, most of this experimentation will occur as a part of a redesigned exercise program designed to make all events joint and multinational, with the aim point being the Navy’s Rim of the Pacific exercise in 2018. Finally, we are supporting increased innovation across the services in cross-component and combatant-command processes.

Technology. Another key area is technological change. We must overcome and leverage the velocity of technological change, rather than losing our overmatch capabilities through slow acquisitions programs. The Department of Defense and the Army have already created the foundation for rapid material solutions with the Strategic Capabilities Office at the Office of the Secretary of Defense and the Rapid Capabilities Office at Headquarters, Department of the Army. These offices are doing an admirable job of repurposing current technology to innovate in application, a key component of recapturing our tactical edge. USARPAC is tied tightly into these efforts. It is including every piece of equipment in exercises and experimentation. As has been the case in this theater for years, USARPAC takes advantage of the great “battle lab” culture this command has developed over the past decade or more. Technology offers key tools to support decision making, lethality, and protection. We must leverage this technology to empower our men and women and increase their lethality and effectiveness.

People. The final area the Multi-Domain Battle concept addresses is people. The U.S. Armed Forces must use its people to overcome the challenges of being outnumbered, outdistanced, and “outlearned” by adversaries and enemies. People are America’s greatest strategic advantage. To leverage this advantage, the Armed Forces must develop agile and adaptive leaders through education and training. Rigorous iterations of decision making, including “impossible” scenarios or “black swans” that soldiers would not expect, can help develop critical thinking skills. Failure must be an option, under the principle that learning exercises develop leaders who will respond better in actual conflicts. Leaders must also receive some measure of cultural education and training that would allow them to experience different ways of thinking. In USARPAC, we are addressing both critical thinking and cultural understanding through a regional leader development program run by and for personnel at the Army service component command level. As the Army’s advise-and-assist brigades come online, we will also include unit personnel headed to the Pacific in this education and training pipeline to prepare them for operations in this region.

Multi-Domain Battle in Practice

The following fictional vignette illustrates the Multi-Domain Battle concept applied at the tactical level. This example is based on a hypothetical location in the Indo-Asia Pacific region.

Let us say there was an island chain or a coastal land mass whose location would make it decisive terrain, influencing aerial or maritime navigation or access to a strategic port. Possession of this feature by a certain hostile power would constitute a serious threat to the international order and the stability and security of the Indo-Asia Pacific region.

The hostile power then seized control of the feature and announced it would restrict commercial air and sea traffic, denying access to any nation aligned with the United States. Treaty obligations would require the United States to intervene militarily, though the enemy’s arsenal of weaponry and electronics was formidable.

A military option that applied the Multi-Domain Battle concept might include using cyber and space capabilities to temporarily blind and disrupt enemy command and control systems so special operations forces could move in and gain a foothold in the island chain. They then would facilitate Marine amphibious forces to secure the beachhead, an airfield, and other major structures required to create a secure beachhead. Immediately behind them would be Army watercraft loaded with heavy engineering equipment to repair the airstrip, if necessary, and construct hardened defensive positions. Simultaneously, Air Force C-17s and C-130s would bring in an Army Stryker battalion task force with a High-Mobility Artillery Rocket System battery,
specially equipped with anti-ship cruise missile pods and a battery of the Indirect Fire Protection Capability weapon system for short-range air defense. In addition, a battery of 155 mm howitzers with hypervelocity rounds would be offloaded as the Marines retrograded in the newly empty aircraft to reconstitute for subsequent forced-entry operations, if needed.

Within ninety-six hours, the Stryker battalion task force would be dug in and ready. With Air Force manned and unmanned systems, Navy ships and underwater drones, a suite of Army radar systems (such as AN/TPQ-36, AN/TPQ-37, or Sentinel) and the aerial threat detection Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System to see over the horizon, there would be an overlapping multi-domain network of sensors that could operate indefinitely to identify, target, and employ lethal and electronic fires in all the domains—land, sea, air, cyber, and space—simultaneously.

The task force might be cut off from resupply or communication for indefinite periods. That is why this task force of about one thousand personnel would be able to support itself for up to thirty days—ten times the current doctrinal requirement of seventy-two hours for a unit of this size. But with advancements in mobile water purification, solar panels, batteries, wind turbines, and wave and tidal energy, as well as additive manufacturing printers to make repair parts, such a unit could be self-sufficient far longer than even much larger ones were in the previous century. They would still need fuel for their vehicles, but with drones and other autonomous platforms enhancing force protection, they could limit the need for fossil fuel-powered vehicles and supplement organic support assets with Air Force’s Joint Precision Airdrop System.

Multinational forces march in formation 15 February 2017 after the official opening ceremony of Cobra Gold 2017 in Utapao, Thailand. Cobra Gold, in its thirty-sixth iteration, is the largest Theater Security Cooperation exercise in the Indo-Asia-Pacific. This year’s focus is to advance regional security and ensure effective responses to regional crises by bringing together a robust multinational force to address shared goals and security commitments in the Indo-Asia-Pacific region. (Photo by Petty Officer 2nd Class Marc Castaneda, U.S. Navy)
To reiterate, these units might have to operate in extremely austere conditions with limited resources and without a constant ground, sea, or aerial line of communication linking them to other friendly forces. However, these men and women would be ready, with exceptional leaders exercising mission command.

Again, this is just a thought exercise based on how Army forces in the Pacific are thinking about and experimenting with multi-domain battle. Application of the concept may look different in other parts of the world, or even in different areas of the Indo-Asia Pacific. However, it is clear that no matter the geography or the adversary, Army units must be well led, well trained, and well equipped to operate in and across multiple domains in support of a joint force.

One way to ensure this is the case is through holistic operational testing, with Army service component command and subordinate units working hand in hand with the concepts and doctrine developers at United States Army Training and Doctrine Command. Today in the Pacific, this is occurring. We are applying the joint integration, technology, and people aspects of the Multi-Domain Battle concept through rigorous inclusion of concepts and capabilities in all our exercises, which will culminate in a major test at the Navy’s Rim of the Pacific exercise in 2018. Moreover, we are considering how to integrate a multi-domain approach with our planning, equipping, and leader-development efforts.

The Army should not hesitate to resource and test this effort. Many of the concepts and capabilities found in the Multi-Domain Battle concept will be needed not just for future conflict but also for near-term conflicts that might require us to be ready to “fight tonight.” Make no mistake: testing and implementing a multi-domain approach will increase our readiness today, as well as prepare our men and women to win wars if the Nation requires it.

Notes


12. Numerous resources address each of these aspects the U.S. Army’s history at the Center of Military History website, accessed 27 February 2017, http://www.history.army.mil.

13. Nassim Nicholas Taleb, The Black Swan: The Impact of the Highly Improbable (New York: Random House, 2010). The author describes the term “black swan” as an occurrence that is a rarity, is extremely impactful, and has retrospective (though not prospective) predictability.