Cyberspace in Multi-Domain Battle

Lieutenant General Paul M. Nakasone
Major Charlie Lewis

For months, a nation state has covertly infiltrated a neighboring state's critical networks while massing armored forces along its common border with a US ally. While the adversary prepares to launch a massive cyber-attack on its neighbor state, its tanks are readied to roll over the border. Nearby, a U.S. Division, engaged in an allied training exercise prepares to become the first line of defense against aggression. Unknown to the adversary, Allied and US forces have hardened their networks and at the first indication of aggression, have temporarily cut power to a nearby city to deceive the enemy. Simultaneously, a U.S. Navy warship fires an Electro Magnetic Pulse (EMP) missile at the adversary, disabling their electronic systems. Facing a numerically superior enemy, Allied forces, take advantage of the window of opportunity created by the EMP weapon to engage the crippled and confused enemy forces across multiple domains.

Today, United States superiority in any domain is no longer a guarantee. The continued low barriers to entry and use of relatively inexpensive cyberspace technologies may create advantages across any domain as well as the human dimension. Domination in any domain no longer makes for a successful military operation. Instead, leveraging multiple domains at specific points of opportunity creates the competitive advantage required to defeat adversaries on future battlefields. Recognizing this new paradigm, the Army and Marine Corps developed the Multi-Domain Battle Concept to deter and defeat enemies. [1]

Multi-domain battle is not a new concept. Throughout history, militaries have attempted to conquer their enemies by coordinating simultaneous attacks by land and sea, and later by air. The harnessing of the electromagnetic spectrum and the advent of modern communications technologies have allowed militaries with advanced warfighting capabilities to seize the advantage by engaging in multiple domain battle. *To win across a 21st-century multi-domain battlefield, the Army and Joint Force must first aggressively defend its networks, deliver cyberspace effects against its adversaries, and*

Lieutenant General Paul M. Nakasone assumed command of U.S. Army Cyber Command on Oct. 14, 2016. A native of White Bear Lake, Minnesota, the general is a graduate of Saint John's University in Collegeville, Minnesota, where he received his commission through the Reserve Officers' Training Corps.

LTG Nakasone has held command and staff positions across all levels of the Army with assignments in the United States, the Republic of Korea, Iraq, and Afghanistan. Prior to his appointment as Commander of U.S. Army Cyber Command, LTG Nakasone commanded the Cyber National Mission Force at U.S. Cyber Command.

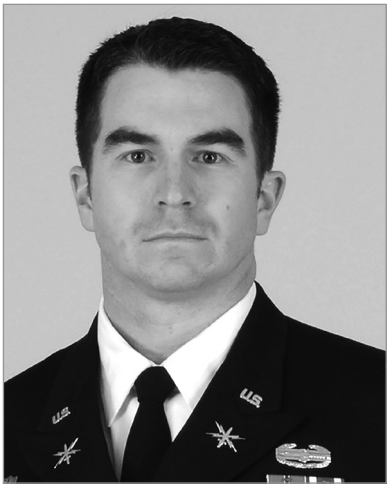
LTG Nakasone is a graduate of the U.S. Army War College, the Command and General Staff College, and the Defense Intelligence College. He holds graduate degrees from the U.S. Army War College, the National Defense Intelligence College, and the University of Southern California.

integrate cyber capabilities for the future fight across all domains.

During the early stages of World War II, Great Britain found itself exposed and threatened by imminent invasion from Nazi forces. The British military faced losing to a tactically superior and larger force, while the German Army marched across much of Europe virtually unchecked. German Wolfpack U-boat tactics closed shipping lanes, prevented critical resupply, impacted commerce and rendered the once great British Navy vulnerable. The British military faced invasion and defeat to the tactically superior and larger German force, a fact painfully played out, alongside French and Belgian allies during the Battle of Dunkirk and the fall of France.

Despite falling behind in three domains, the British development of radar at the end of the interwar period and utilizing integrated air and land defenses during the Battle of Britain proved pivotal. Using the electromagnetic spectrum, the British removed the element of surprise from the Luftwaffe.[2] Instead of waiting until spotters identified German aircraft by sight, the British employed an integrated air defense system that included radar, which provided a crucial over-the-horizon warning. British Army anti-aircraft batteries sat with rounds loaded while Royal Air Force fighters launched from airfields to engage the enemy in air-to-air combat. Radar allowed the British to maintain air superiority over the mainland and protect their naval defenses, thwarting Germany's invasion plans.

As evidenced by the British actions on land, sea, air, and the electromagnetic spectrums, combining efforts across multiple domains creates relative advantages that ultimately lead to victory. In preparing for a variety of conflicts, the Army and Marine Corps recognize that emphasizing one domain may lead to losses in battle. Instead, fighting across



A Cyber Operations Officer, Charlie Lewis currently serves as the Executive Officer of the U.S. Army's Cyber Training Battalion at Fort Gordon, Georgia. Commissioned in the Field Artillery, he first served as Fire Support Officer to Company Commander with 3rd Brigade, 101st Airborne Division. Following graduate school, he taught as an Assistant Professor in the Department of Social Sciences at USMA, serving as Department Executive Officer his last year. Most recently, he directed the Cyber Leader College at the U.S. Army Cyber School. His military education includes the Army's Ranger, Airborne, Air Assault, Pathfinder, and Combat Diver schools. Charlie is a 2004 graduate of the United States Military Academy and holds a Master's in Public Policy from Harvard University. He is an Assistant Editor for Army Cyber Institute's *The Cyber Defense Review* and a Term Member on the Council on Foreign Relations. He recently served as a Madison Policy Forum Cybersecurity Fellow.

multiple domains, including cyberspace, increases the effectiveness of US forces while adding complexity to the battlefield. Success in this new concept relies heavily on the integration of cyberspace operations, which this paper defines.

A NEW WAY OF THINKING

Chief of Staff of the Army, General Mark Milley offered, "... we are on the cusp of a fundamental change in the character of war." Changes in technology, geopolitics, and demographics are shifting how American forces fight wars.[3] Preparing now to allow the Army to meet simultaneous challenges across all domains is imperative if we hope to avoid first battle losses. The velocity of future conflict demands that we not wait for our adversaries to adopt new techniques and technologies.[4]

American technological overmatch has ceded territory to near-peer adversaries, regional threats, and non-state actors.[5] According to the Chairman of the Joint Chiefs of Staff, General Joseph Dunford, the proliferation and rapid development of technologies makes it easy for not only Russia and China to close the American advantage, but also for smaller actors to "frustrate U.S. interests".[6,7] Even as the Joint Force uses robotics as force multipliers, improved radio-frequency weapons, and continues exploitation of vulnerabilities in weapons systems, adversaries will keep pace and do the same.[8] Swarming formations of robots, micro-Unmanned Aerial Vehicles, and various other technologies will create confusion and overwhelm US decision-making in future battles.[9] Adversarial technological adoption can render US firepower impotent, no matter how powerful, before crossing the line of departure unless the military prepares for new technologies.

Advancing the proven success of combined arms in a joint environment, the Multi-Domain Battle Concept envisions future ground combat forces providing commanders options across multiple domains to deter and defeat adversaries while working with a variety of different partners. This concept will apply combined arms maneuver across all domains to create multiple dilemmas for the enemy.[10] Dominance across all domains all the time is not required. Instead, Commanders will maneuver within each domain at a given point in time to create windows of opportunity and temporary domination to gain the advantage.[11]

Multi-Domain operations rely on interdependent networks that also serve as the base for the cyberspace domain.[12] Presenting both opportunities and vulnerabilities, cyberspace serves as a significant option for strategic operations.[13] It is up to our cyber forces to prepare for victory across the information environment.

DEFENSE OF NETWORKS, DATA, AND WEAPON SYSTEMS

Well before any battlefield engagement on land or in air, Army Cyber forces enter combat against an enemy set to disrupt US network operations. Small elements of cyber defenders protect tactical networks, responding to breaches of integrated air defense systems. Soldiers continue to update systems, ensuring each weapon and tactical warfighter possesses the latest patches or logical armor. Back at Fort Gordon, Cyber Protection Teams defend broader swathes of networks remotely, hunting for advanced persistent threats, and maintaining the strategic picture to defend cyber key terrain to enable mission command.

To win across a 21ST century multi-domain battlefield, the Army and Joint Force must first aggressively defend its networks.

Without the network, there is no Multi-Domain Battle. The sinew of maneuver across all domains is the network.[14] Army forces are not just reliant on the network for communication and operations; the network is also the weapon system upon which all cyber forces project power. Failure to defend the network exposes cyberspace's base of operations. Like its old coastal artillery mission, the Army must recognize that defending well in one domain requires defense across all others. Admiral Harry B. Harris, Jr., described the Army's role as "defending the sea from land."[15] Coastal artillery enhanced the ability of other domains to deny access to the enemy by protecting logistics hubs, seaports, and airbases.[16] Cyber forces protect the network through layered defenses while also securing air, sea, and land force communications. Complexity with serial defense in-depth hinders enemy operations while enabling friendly maneuver.

Cross-domain defense starts with each domain defending itself first. Because what was once a minor nuisance—cyber-attacks—can now inflict damage with significant military

implications, effectively operating and defending the network must be the first priority of all operations.[17] Threats against our networks eclipse current potential gains achieved through offensive cyberspace operations. Moreover, as we look for greater capabilities within cyberspace, we become even more vulnerable to adversary intrusions and preemptive strikes.[18] The importance of effectively operating and defending our networks cannot be overstated.

The enemy seeks information and each user on the Department of Defense Information Network (DoDIN) provides an avenue of approach to their objective. Securing the DoDIN not only allows ground forces to communicate across domains, but it also allows offensive cyberspace operations to maneuver into enemy terrain. Unity of command across cyberspace, allowing for both the operation and defense of the network will better integrate defenses within cyberspace.

The velocity of future conflict demands that we do not wait for our adversaries to adopt new techniques and technologies.

Fortifying the network affords commanders opportunities in other domains by enabling mission command. Various warfighting components from aviation to fires must communicate with land forces while maneuvering to access information on adversaries, the terrain, and the disposition of friendly forces. Gaining and maintaining a decisive advantage in conflict requires accurate and timely decisions based on information gathered.[19] The network allows for the sharing and consolidation of data across various organizations, commands, and even domains. Intelligence reporting, orders, targeting, and execution commands will not happen unless there are strong and secure lines of communication. The synchronization and integration necessary to win across a multi-domain battlespace cannot occur without the network.

DELIVERING EFFECTS AGAINST OUR ADVERSARIES

Army Cyber operators move through enemy networks. Enemy battle plans disappear while supply trains fumble through traffic jams created by incorrect orders and railroad signals. Adversarial forces receive confusing messages about their leaders abandoning them via social media while preparing their equipment. Enemy observation drones crash due to signal jamming from electronic warfare forces at the front lines.

One domain can create "temporary windows of advantage" for another.[20] Extending the battlefield over multiple domains provides commanders options to exploit vulnerabilities when they appear as opposed to engaging based on linear constructs.[21] Just as the British exploited the electromagnetic spectrum with radar to grow their engagement area during the Battle of Britain in 1940, cyberspace must do the same today.[22] Delivering effects against the enemy through the network and across the

information environment empowers US commanders while increasing the complexity of the battlefield for the adversary who will not know where Army cyber forces lurk in their networks.

One of the goals of the Department of Defense's (DoD) Cyber Strategy is the "need to maintain viable cyber options" integrated into plans to achieve precise objectives.[23] To meet this goal, cyber forces project power through cyberspace in support of various levels of command. From development to employment, cyberspace effects must connect to commander's intent and objectives. Cyber forces must use their diverse problem-solving skills to anticipate requirements and create tools and capabilities to meet requirements. Unlike artillery shells or bombs, cyber tools are limited and may even be a one-time use system. While ground forces can call for multiple artillery rounds to destroy a power transformer, cyber forces may have one opportunity to deliver their capability to destroy the same piece of equipment. Commanders must synchronize their use during the right window to apply resources wisely within the cyberspace domain.

The network is also the weapon system upon which all cyber forces project power.

Beyond networks, attacking through the electromagnetic spectrum provides another option. Electronic warfare successfully supported recent Russian land operations in Crimea and demonstrated how swarming of threats across multiple domains confuses an enemy.[24] Currently, electronic warfare capabilities reside at the tactical level, providing ground commanders responsive and flexible options to conduct an electronic attack, support, or protect. Using the equipment and talent located within their formation, commanders can incorporate fires through the electromagnetic spectrum to support their maneuver operations. By jamming enemy communications at a given point while also masking their own signatures, ground forces can move freely across the battlefield. No matter what method of operation within cyberspace, gaining a temporary advantage, in conjunction with combined arms maneuver, increases the adversaries' complexity. Cyber forces must deliver effects in creative ways to maintain this advantage.

INTEGRATED CAPABILITIES

US forces maneuver to regain border towns lost to enemy forces. US aircraft race overhead and artillery screams past their buildings, but the munitions only land on the vehicles camouflaged outside of the town. As an enemy detachment keys their microphone to report activity, a message comes across their computer telling them to surrender and providing the current grid of every soldier in that town. US troops maneuver closer, releasing a swarm of drones. Electronic warfare operators start spoofing the size of the small force, confusing enemy leaders who now think it is a battalion. Panicked, forty enemy combatants surrender their

defenses. A drone developed by an Austin startup flies to each enemy soldier, scans their irises, confirms accountability, and relays directions. An Electronic Warfare specialist jams any potential enemy communications as they surrender, not to a battalion, but instead to an expeditionary cyber team of five personnel.

From defense to offense, capabilities must span cyberspace, electronic warfare, and information operations. Just as British leaders exploited a new technology, radar, to gain an advantage over the Nazis, joint force commanders must do the same today in support of Multi-Domain Battle. Developing new cyberspace capabilities starts with framing the problem and then innovating throughout the integration process. New DoD initiatives stress the research and development cycle but more is needed to meet the speed and agility required by the Army.[25] Over the past decade, adversaries created new products, spent more money, and even pilfered American research to counter traditional US strengths.[26] To regain the advantage, DoD has undertaken numerous initiatives to accelerate the acquisition process of cyberspace technologies, including Defense Innovation Board, the Strategic Capabilities Office, and the Defense Innovation Unit Experimental (DIUx).[27] Instead of years in development acquisition, the Army hopes to purchase capabilities and deploy them much faster in support of ground forces.

> Cyber forces must use their diverse problem solving skills to anticipate requirements and create tools to meet requirements.

Equally important, force structure and education shifts must occur to incorporate new technologies. Commanders must integrate the opportunities new capabilities provide as rapidly as acquired.[28] Preparing commands through professional military education's new emphasis on cyberspace increases Army leaders' understanding of cyber threats and cyberspace capabilities. Today, opportunities exist to enable commanders with cyber and electronic warfare capabilities against the Islamic State in Iraq and Syria along with fulfilling U.S. Army Europe's call for an urgent operational need to address current warfighting shortfalls.

The Army's Cyber Electromagnetic Activity (CEMA) Support to Corps and Below (CSCB) initiative today demonstrates how cyberspace operations can be integrated into a combined arms maneuver force to succeed at lower echelons.[29] Moreover, While Electronic Warfare (EW) personnel provide planning prowess, their minimal structure limits operations across the entire cyberspace domain. However, CSCB efforts integrating EW with Cyber, Information Operations, and Intelligence personnel, equipment, and capabilities provide commanders with offensive and defensive cyber capabilities to gain an advantage in a domain previously limited to them.[30] Moreover, CSCB shows forces how to adapt processes and use their organic Electronic Warfare cells.[31]

Even with force structure and weapons platforms, commanders must also visualize cyber terrain the same way they do land to understand the battlefield.[32] From maneuvering forces to de-confliction, visualization mitigates conflicts within the military and interagency, allowing for a faster response to adversarial actions.[33] Finally, visualization can lessen one of the main risks in cyberspace, crossing into another area of responsibility. Authorities constrain operations to limit risk because many cannot see the ultimate effect; adding a picture can show full movement on the battlefield and will speed up the approval process.

One of the goals of the DoD Cyber Strategy is the need to maintain viable cyber options integrated into plans to achieve precise objectives.

CONCLUSION

Confused, the enemy retreats well beyond the border. US forces overwhelmed their decision-making processes and information flow. Key communication devices crashed. A numerically inferior US and allied force somehow defeated a well-defended force connected to its logistics bases. Fighting over multiple domains created a complex battlefield the enemy could not control or defeat.

Multi-Domain Battle succeeds when each domain gains the advantage in support of others, requiring innovative approaches to integrating cyber operations, just as the British did with radar. A failure to layer operations across multiple domains creates gaps that adversaries will expose. Combining maneuver across domains creates many dilemmas for the enemy. The network today is the piece that best ties operations across all domains. With the network connecting all domains, success within cyberspace is imperative. From defending the network as a base to achieving effects against the enemy, the Army must prepare to fight in an environment that changes exponentially and will look much different tomorrow. Starting with the defense of the network, cyberspace protects "bases" upon which offensive forces can deliver effects through fiber and the spectrum. Integrated throughout the levels of command, the cyberspace domain's integration in multi-domain conflict will be critical for future Joint Force commanders.

NOTES

1. David Perkins, "Multi-Domain Battle: Joint Combined Arms Concept for the 21ST Century" *Army Magazine.* Retrieved on November 22, 2016 from https://www.ausa.org/articles/multi-domain-battle-joint-combined-arms-concept-21st-century.

2. Alan Beyerchen, "From Radio to Radar: Interwar Military Adaptation to Technological Change in Germany, the United Kingdom, and the United States." *In Military Innovation in the Interwar Period,* edited by Williamson Murray and Allan R. Millett, Cambridge: Cambridge University Press, 1996, 265, 299.

3. General Mark A. Milley, "Changing Nature of War Won't Change Our Purpose," *AUSA Greenbook 2016-2017,* October 2016, 15-16.

4. First battles comment based on *America's First Battles, 1776-1965,* edited by Charles Heller and William A. Stofft.

5. "Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World," *Joint Chiefs of Staff,* Washington D.C., 14 July 2016, 15.

6. General Joseph Dunford, "Posture Statement of General Joseph Dunford Jr., USMC, 19TH Chairman of the Joint Chiefs of Staff Before the 114TH Congress Senate Armed Service Committee Budget Hearing," *United States Senate Armed Services Committee,* March 17, 2016.

7. "Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World," *Joint Chiefs of Staff,* Washington D.C., 14 July 2016, 15.

8. "Joint Operating Environment 2035," 16-19.

9. Paul Scharre, "Unleash the Swarm: The Future of Warfare," *War on the Rocks,* retrieved from http://warontherocks.com/2015/03/unleash-the-swarm-the-future-of-warfare/ on December 28, 2016.

10. Albert Palazzo and David P. Mclain, III, "Multi-Domain Battle: A New Concept for Land Forces." *War on the Rocks.* Retrieved from http://warontherocks.com/2016/09/multi-domain-battle-a-new-concept-for-land-forces/, accessed November 22, 2016.

11. Perkins.

12. "Joint Operating Environment 2035," 33.

13. "Joint Operating Environment 2035," 33.

14. Chris Telley, "The Sinews of Multi-Domain Battle," *RealClearDefense,* retrieved from http://www.realcleardefense.com/articles/2016/12/30/the_sinews_of_multi-domain_battle_110564.html on December 30, 2016.

15. Harry B. Harris, Jr. "Role of Land Forces in Ensuring Access to Shared Domains." Speech given to the AUSA Institute of Land Warfare LANPAC Symposium on May 25, 2016.

16. Eric Lindsey, "Beyond Coast Artillery: Cross-Domain Denial and the Army," *Center for Strategic and Budgetary Assessments.*

17. General Mark Milley, "Remarks at the AUSA Conference 2016," *Association of the United States Army.*

18. Jacquelyn Schneider, "Digitally-Enabled Warfare," *Center for a New American Security,* retrieved from https://www.cnas.org/publications/reports/digitally-enabled-warfare-the-capability-vulnerability-paradox on August 29, 2016.

19. Patrick J. Murphy and Mark A. Milley, "Record Version Statement by The Honorable Patrick J. Murphy, Acting Secretary of the Army, and General Mark A. Milley, Chief of Staff, United States Army, on the Posture of the United States Army" *United States Senate Committee on Armed Services,* April 7, 2016.

20. Perkins.

21. Perkins.

22. Beyerchen.

23. Office of the Secretary of Defense, *The Department of Defense Cyber Strategy,* April 2015, 14.

24. Paul Scharre, "Commanding the Swarm," *War on the Rocks,* retrieved from http://warontherocks.com/2015/03/commanding-the-swarm/ on November 25, 2016.

25. Secretary of Defense Ash Carter, "Remarks on "The Path to an Innovative Future for Defense" *Office of the Secretary of Defense,* October 28, 2016, retrieved from https://www.defense.gov/News/Speeches/Speech-View/Article/990315/remarks-on-the-path-to-an-innovative-future-for-defense-csis-third-offset-strat on December 27, 2016.

NOTES

26. Bob Work, "The Third U.S. Offset Strategy and its Implications for Partners and Allies," speech given at the Willard Hotel in Washington D.C. on January 28TH, 2015, retrieved from https://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies on December 29, 2016

27. "Remarks on "The Path to an Innovative Future for Defense."

28. The Path to an Innovative Future for Defense.

29. Formerly Army Cyber's, Cyber Support to Corps and Below, CSCB is now the overarching effort to combine cyber, electronic warfare, and Information Operations to tactical forces. It incorporates support to select rotations to Combat Training Centers that will guide future Army decisions on doctrine, organizational structure, training, materiel, integration, logistics, personnel, and facilities to close known capability gaps across the Army.

30. U.S. Army Cyber Command, "Integration of cyberspace capabilities into tactical units, *Army.mil,* retrieved from https://www.army.mil/article/163156 on November 25, 2016.

31. David Vargan, "Expeditionary cyber aids maneuver commanders," *Army News Service,* r etrieved from http://www.riley.army.mil/News/Article-Display/Article/933299/expeditionary-cyber-aids-maneuver-commanders/ on November 25, 2016.

32. Mark Pomerleau, "What is ISR in non-physical domains?" *C4ISRNET,* retrieved from http://www.c4isrnet.com/articles/what-is-isr-in-non-physical-domains on December 30, 2016.

33. Mark Pomerleau, "How can cyber contribute to multi-domain battle?" *C4ISRNET,* retrieved http://www.c4isrnet.com articles/how-can-cyber-contribute-to-multi-domain-battle on December 27, 2016.