Topical Essays

America's Joint Force and the Domains of Warfare

James Jay Carafano, PhD

The term "joint" has been well established in the U.S. military lexicon for many decades. While the word's meaning may remain a constant, its significance for the American military is changing.

The essays on the dimensions of warfare in the *2018 Index of U.S. Military Strength* reflect a crucial dynamic that affects thinking about how militaries ought to be employed. Dominance in war will not be gained through domination of a single domain. The future focus of jointness will be on ensuring that U.S. armed forces retain the ability to operate effectively in all domains in a theater (land, sea, air, subsurface, cyberspace, and space) and to exploit the ability to use advantages in one domain to operate in another. For the U.S., having the capacity to check an adversary or take the initiative across all domains will be essential to establishing a competitive advantage in future conflicts.

The Dimensions of War

One of the great truisms of war was expressed by the British military historian B. H. Liddell Hart: "The real target in war is the mind of the enemy commander, not the bodies of his troops."[1] This maxim touches the core of understanding the nature of warfare. War is a competition. War is a competition between adversaries, a contest of action and counteraction that concludes or changes based on the agency of competitors, and this competition unfolds in the domains accessible to each competitor: land, sea, air, space, and cyberspace. Dominating in war is not about dominating a domain. It is about dominating an enemy.

In contemporary conflict, as competitors increasingly gain access to all domains of warfare, it becomes more likely that adversaries will seek to offset a competitor's dominance in one domain by acting more aggressively in another space. As transnational terrorists like ISIS have lost physical ground in the Middle East, for example, they have redoubled their cyber operations to stay in the fight against the West. Alternatively, competitors might redouble their efforts to defeat an adversary's capacity to dominate them in a particular domain. This has become a feature of Chinese military strategy, which seeks to prevent adversaries from achieving a dominant advantage in space, air, sea, and cyber operations in the Asia–Pacific theater.

Thus, dominance in one or more domains is important, but to dominate an enemy, the ability to conduct operations in more than one domain at a time, to shift between them, and to use one domain to affect another is more important.

The elements of the U.S. armed forces increasingly operate across domains, each service specializing in one but increasingly having an effective presence in the others and/or relying on the other services to create opportunities for exploitation and to prevent an enemy

from using a domain for their own purposes. No one service bears sole responsibility for military operations in any domain. Each of the uniformed military services, for example, uses cyberspace. All conduct or depend on space operations. Forces from land bases can affect operations at sea. Naval forces can influence land battles. Air force operations routinely have an impact on multiple domains.

The nature of contemporary warfare has implications for how the armed forces address jointness now and in the future. Further, the evolution of the joint force and how the U.S. military thinks about conducting joint operations has significant consequences for how national leaders understand military strength and its utility in securing national interests.

Evolution of the Joint Concept

For the Pentagon, "joint" "[c]onnotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate."[2] In the case of the United States, that means the Army, Air Force, and Navy Departments, the last of which includes the Navy and Marine Corps. The U.S. Coast Guard, when operating in concert with them, also could be considered part of the joint force. U.S. Special Operations Forces (e.g., SEALs and Rangers) are provided by the services; when they operate across service components or with conventional forces (e.g., Army brigades), they are also conducting joint operations.

The U.S. military's appreciation of jointness is built on a historical understanding of Western warfare and its own contemporary experiences. While joint operations, the cooperative use of forces operating in their respective domains, may not be as old as war itself, there are certainly many antecedents from the times of ancient warfare. Most notably, histories of the Peloponnesian Wars, the decades-long struggle between alliances led by the Greek city-states Athens (primarily a naval power) and Sparta (the dominant land power), turned on joint operations.[3]

Athens and Sparta. One instructive example of joint operations in the ancient world was the land–sea campaign in Sicily from 415 BC to 413 BC. An Athenian expeditionary force was dispatched to secure the strategic island off the coast of Italy that, some of their leaders argued, would provide a decisive advantage in the war with Sparta. The Athenian force was joint, composed of a naval force of some 100 triremes (Greek war galleys, or rowed fighting ships); numerous transport and cargo ships; and more than 5,000 hoplite infantrymen and additional archers and slingers that could conduct ground operations.[4]

Once establishing themselves in Sicily, the Athenians were slow to advance on their main objective, the city of Syracuse. This allowed time for the Spartans to dispatch reinforcements to their Syracusan allies. The Athenians lost the land battle against the superior combined land force of Sparta and Syracuse. When they tried to withdraw by sea, the Spartans, having developed their own navy, intercepted the retreating fleet, soundly defeating the Athenians in a massive sea battle.

Using the Athenian naval assets to maneuver ground units into a superior position was a classic exercise in joint operations, leveraging forces that operate in one domain to provide a competitive advantage to forces operating in another. But coordinating different forces and operating in different domains is complex. Effective command and control of the Athenian expeditionary force broke down, leaving it vulnerable to the Spartan counterstrike.[5] In this respect, the operation illustrated both the potential advantages and possible pitfalls of employing joint forces in a campaign.

Joint operations, principally cooperation between land and sea forces, have been a feature of Western warfare through the ages. U.S. military history also includes exemplars of joint operations, notably including the defeat of the British at Yorktown in 1781[6] and the siege of Vicksburg in 1863.[7]

Yorktown. The siege of Yorktown included both joint operations and combined operations (operations involving forces of more than one nation). After a vigorous campaign in Virginia, British forces withdrew to the

Yorktown Peninsula to rearm and refit, resupplied and protected by British naval forces. As the Continental Army conducted a forced march from New York to the Tidewater region in the Chesapeake Bay to block the British by land, a French fleet intercepted and destroyed reinforcements dispatched to the British at Yorktown by sea. While the Continental Army laid siege to the garrison by land, the French Navy blockaded Yorktown by sea. Pressed by the advance of combined American–French forces and cut off from reinforcement and resupply, the British surrendered, a catastrophic military defeat that led to the end of the war and the securing of American independence.

Napoleon in Egypt. The battles of the American Revolution presaged the transition from the early modern era of warfare to the Napoleonic Age, which saw significant innovation in both land and sea warfare in terms of technology, tactics, and logistics. The practice of joint operations—such as Napoleon's aborted invasion of Egypt in 1798, in which the future emperor transported an army of over 30,000 by sea only to see the force eventually cut off and defeated in detail—looked not much different from the conduct of joint operations in previous decades.[8]

In many ways, the American Civil War continued the practices and tactics of the Napoleonic era. One area in which there were glimpses of change was in the conduct of joint operations, which indicated the potential promise of coordinating land and sea operations to achieve strategic objectives—practices that would emerge more fully during the two great world wars of the 20th century.

Vicksburg. The most illustrative battle was the siege of Vicksburg.[9] A joint land–naval force isolated and reduced the Confederate strong point at Vicksburg, Mississippi. The victory gave the Union control of the Mississippi River, effectively cutting the Confederacy in two. Not only did the battle preview new technology, such as armored ships and rifled cannon, but Union operations demonstrated the effective coordination, command, and control of joint forces, with General Ulysses Grant succeeding where Athens and Napoleon had failed.

Throughout the evolution of war in the early modern and Napoleonic eras and into the modern era, joint operations were a matter of practice, but there was scant emphasis on the development of doctrine, tactics, training, or force development. Even massive joint operations, such as the Gallipoli campaign of 1915–1916 during World War I, were largely improvised.[10]

Gallipoli. While war on the European Western Front stagnated in trench combat, operations in the Dardanelles were intended to knock the Ottoman Empire out of the war by employing the swift maneuver of forces that could be achieved by joint operations. A British-led Allied expeditionary force moved to secure Gallipoli, a strategically important peninsula that controlled Mediterranean access to the Black Sea, but the operation was protracted and suffered from numerous delays, giving the Turks time to move adequate defenses into place, after which the battle devolved into trench warfare that soon resembled the stalemate on the Western Front. Though the Allies had the means to transport a land force by sea and support its employment from the sea, and enjoyed effectively uncontested use of the sea, their failure to move swiftly, decisively, and in well-practiced form ceded all of the important advantages to the Turks, who used their control of the land to greater effect.[11]

World War II. The modern age of warfare arrived during World War II when operations in several theaters required the integrated use of land, sea, and air forces. Most notably in the Pacific Theater, amphibious operations to sustain land campaigns from the sea, designed to seize a beachhead in order to conduct more expanded operations ashore, required joint operations as a matter of course.

Dramatic advances in airpower during the 1930s added a new dimension to warfare. Forces and supplies could be moved by air, either air-landed or inserted by glider or parachute forces. Airpower could also provide airborne reconnaissance and fire support for both land

and sea services (e.g., sub hunting and attack by air of an opposing fleet).

Another but little discussed aspect of emerging joint warfare was the electromagnetic dimension, from radio communications to intercept, radar, and electronic jamming. Forces had to learn how to operate across a new dimension of war that did not transit a geographical space and was not the purview of any one service. This was a sign of times to come, as all of the services would find themselves operating increasingly in multiple domains, which requires a great degree of coordination and deconfliction.

In response to the demands of the war, the military services developed operations, command and control organizations, equipment, doctrine, and training to facilitate joint operations. However, while military operations and campaigning were joint, many other aspects of military operations including education, intelligence, and logistics were often done as single-service activities or only loosely integrated.

The Post–World War II Era. Even after the experience of the Second World War, military thought continued to focus on the competition between domains for dominance in warfare. The classics still mattered. The Army favored Prussian military theorist Carl von Clausewitz, who focused his writing on victory in land battles;[12] the Navy had Alfred Thayer Mahan, who concentrated on control of the sea;[13] and new-to-the-scene airpower enthusiasts referenced Giulio Douhet, who championed victory through airpower.[14] With the invention of nuclear weapons, strategists like Bernard Brodie argued for the strategic dominance of nuclear weapons.[15]

Despite the prevalence of joint operations during World War II, little was done to institutionalize joint operations. The Defense Reorganization Act of 1958, under the tutelage of President Dwight David Eisenhower, drawing in part on his extensive experience with joint operations during the war as Supreme Allied Commander Europe, advanced efforts to establish unified command for joint forces, but little more.[16]

Goldwater–Nichols. Lack of effective joint operations at the operational level was one of the significant criticisms of U.S. military activities during the Vietnam War. The issue was famously addressed in Arthur T. Hadley's book *The Straw Giant*.[17] Among the many reforms instituted by the Goldwater–Nichols Department of Defense Reorganization Act of 1986 was a legislative effort to institutionalize jointness in the armed forces.[18] The legislation addressed the Unified Command Plan (the global command and control of U.S. forces); education, professional development, and training; and acquisition of weapon systems, platforms, and related equipment.[19] Thus, after Goldwater–Nichols, jointness emphasized integration of the military services across the full range of defense activities, not just warfighting.

The case for jointness, introduced by the Senate Armed Services Committee staff that spearheaded the Goldwater–Nichols legislative effort, was illustrated by the aborted Iranian hostage rescue operation (1980), popularly called the disaster at Desert One.[20] All of the services participated in the ad hoc effort to put together a special operation to rescue U.S. embassy employees who had been taken hostage in Tehran during the Iranian Revolution. Although the operation was joint, it failed.

In truth, however, the mission's most critical shortfalls had little to do with a failure of joint operations. The Marine helicopters were operating at the extreme edge of their operational range; that, combined with bad luck and some miscues on the ground, doomed the mission. Nevertheless, the story was one of dramatic and embarrassing failure and helped to galvanize support for the legislation, which was actively opposed by the Pentagon and the services, which viewed jointness as an imposition on their responsibilities for managing and employing military forces.

Despite opposition from the Pentagon, the legislation was passed and signed into law. This effort coincided with the Reagan defense buildup, which increased the size of the military force, as well as funding for operations and training, and greatly advanced the

modernization of key military platforms (ships, planes, and armored vehicles).[21] Flush with resources and responding to the challenge and demands of jointness imposed by Goldwater–Nichols, the military responded adroitly.

Goldwater–Nichols largely succeeded in institutionalizing joint warfare. From professional military education to operations in the field, U.S. military activities today are inherently joint. Further, the U.S. military has decades of extensive combat experience in joint operations at the operational and tactical levels across the spectrum of conflict. Joint integration has been so successful that when major defense reforms (e.g., Goldwater–Nichols II) are suggested, they rarely substantively address joint matters.[22]

Of course, innovations in jointness did not erase the intellectual debate about which dimensions of war ought to be considered the most important and which service forces would dominate future conflict. The debate was renewed in the wake of the First Gulf War (1991). Air Force advocates, with the introduction of the proliferated use of precision-guided weapons, argued that post–Cold War military operations would be dominated by airpower. This vision was reflected in the Air Force-sponsored Gulf War Air Power Survey.[23] In contrast, the official Army history, *Certain Victory*, argued for the returned dominance of land power.[24] The Navy, which played a subordinate role in the conflict, looked beyond the "lessons" of the war to make the case that U.S. security in the post–Cold War world would be protected by sea-centric military dominance.[25]

The renewed debate about domain dominance that emerged after the Gulf War was as likely a reflection of competition between the services for scarce defense dollars as it was influenced by new technologies and warfighting concepts. In the wake of the war, the Pentagon suffered from an end-of-the-Cold War "peace dividend" that saw a reduction in forces and military spending throughout the 1990s.[26] Increasingly, the services squabbled over pieces of an increasingly smaller budget pie, with each service arguing in part that it delivered more bang for the buck because of its capacity to dominate battle space in its domain.

Despite the renewal of interservice intellectual rivalry, in practice, the trend toward increasing jointness in the development and employment of forces continued. There were many controversial aspects to military operations in Afghanistan and Iraq following the terrorist attacks of September 11, 2001, but shortfalls in the capacity to undertake joint operations were far down the list of items noted by critics.

Joint Future

While some military reformers and theorists continue to propose ways of war predicated on dominance of particular domains, most modern military thinking envisions future operations that are inherently joint. In recent years, for example, the U.S. Army and Marine Corps have advanced the concept of Multi-Domain Battle, the notion that the U.S. should be prepared to fight in an environment in which all domains are contested.[27] Whether the Army–Marine concept is useful remains a subject of some debate (and would eventually have to be proven in battle anyway), but it does reflect mainstream military thinking: The U.S. armed forces must have the expertise, capabilities, and capacity to operate in all domains in a contested theater and to leverage those domains more effectively than the enemy can. Developing and sustaining that capacity will be the key goal of joint future.

As previewed by Multi-Domain Battle, joint future will likely focus on the challenge of employing the armed forces in environments where operations are contested in multiple domains. Planning for military operations may likely be based on assumptions that the U.S. will not enjoy superiority,[28] much less supremacy,[29] in one or more domains. The services will likely focus more on what they can contribute to operations across the dimensions of war rather than arguing the unique contributions of their capabilities in a single domain. The U.S. military will likely continue to look at a mix of operational practices, technologies,

force structure, and capacity to achieve and sustain a competitive edge across the dimensions of warfare.

Most likely, other aspects of jointness will fade in priority: Logistics, infrastructure, education, planning, and training will become more inherently joint as a matter of practice. Joint future will focus on inter-domain dependencies and cross-dimension operations and effects.

A careful reading of the domain essays in this edition of the *Index of U.S. Military Strength* suggests both the challenges and opportunities involved in building U.S. military strength for the next fight. These range from human resources to warfighting systems, from alliances to enemies, from technological improvement to intellectual innovation. The essays raise important questions for the future of the joint force concept and its role in protecting the vital interests of the United States.

Endnotes

1. B. H. Liddell Hart, *Thoughts on War* (London: Faber and Faber, 1944), quoted in Air University, Cyberspace and Information Operations Study Center, "Influence Operations," http://www.au.af.mil/info-ops/influence.htm#top (accessed July 8, 2017).
2. See "joint," in U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms*, June 2017, p. 125, http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf (accessed July 6, 2017).
3. See, for example, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*," ed. Robert B. Strassler (New York: Touchstone, 1998).
4. Ibid., p. 375.
5. Edward S. Creasy, *The Fifteen Decisive Battles of the World: From Marathon to Waterloo* (Hertfordshire, UK: Oracle Publishing Ltd, 1996), pp. 54–82.
6. "The Winning of Independence, 1777–1783," Chapter 4 in *American Military History Volume 1: The United States Army and the Forging of a Nation, 1775–1917*, ed. Richard W. Stewart (Washington: United States Army, Center of Military History, 2005), pp. 98–102, http://www.history.army.mil/books/AMH-V1/PDF/Chapter04.pdf (accessed July 10, 2017).
7. Christopher R. Gabel, *The Vicksburg Campaign: November 1862–July 1863* (Washington: United States Army, Center of Military History, 2013), http://www.history.army.mil/html/books/075/75-8/CMH_Pub_75-8.pdf (accessed July 10, 2017).
8. David G. Chandler, *The Campaigns of Napoleon: The Mind and Method of History's Greatest Soldier* (New York: Scribner, 1966), Part 4, "Oriental Interlude: The Six Acres of Land."
9. Gabel, *The Vicksburg Campaign*, pp. 59–61.
10. Martin Gilbert, *Churchill: A Life* (London: Minerva, 1992), pp. 291, 299–302.
11. Martin Gilbert, *The First World War: A Complete History* (New York: Henry Holt, 1994), pp. 146–153.
12. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, Reprint Edition, 1989).
13. Alfred Thayer Mahan, *The Influence of Sea Power Upon History, 1660–1783* (Mineola, NY: Dover, 1987).
14. Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (New York: Coward-McCann, 1942), https://permanent.access.gpo.gov/airforcehistory/www.airforcehistory.hq.af.mil/Publications/fulltext/command_of_the_air.pdf (accessed July 8, 2017).
15. Bernard Brodie, *Strategy in the Missile Age* (Santa Monica, CA: RAND Corporation, 1959), http://www.rand.org/content/dam/rand/pubs/commercial_books/2007/RAND_CB137-1.pdf (accessed July 8, 2017).
16. Defense Reorganization Act of 1958, Public Law 85–599, 72 Stat. 514, 85th Cong., August 6, 1958, https://www.govinfo.gov/content/pkg/STATUTE-72/pdf/STATUTE-72-Pg514.pdf (accessed July 8, 2017).
17. Arthur T. Hadley, *The Straw Giant* (New York: Random House, 1986).
18. Goldwater–Nichols Department of Defense Reorganization Act of 1986, Public Law 99–433, 100 Stat. 92, 99th Cong., October 1, 1986, http://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf (accessed July 8, 2017).
19. Edward J. Drea, Ronald H. Cole, Walter S. Poole, James F. Schnabel, Robert J. Watson, and Willard J. Webb, *History of the Unified Command Plan 1946–2012*, U.S. Department of Defense, Office of the Chairman of the Joint Chiefs of Staff, Joint History Office, 2013, http://www.jcs.mil/Portals/36/Documents/History/Institutional/Command_Plan.pdf (accessed July 8, 2017).
20. Stuart L. Koehle and Stephen P. Glick, "Why the Rescue Failed," *The American Spectator*, September 14, 2012, https://spectator.org/34807_why-rescue-failed/ (accessed July 8, 2017).
21. Jonathan Reed Winkler, "Reagan and the Military," Chapter 10 in *A Companion to Ronald Reagan*, ed. Andrew L. Johns (Hoboken, NJ: Wiley Blackwell, 2015), pp. 167–183.
22. Colin Clark, "Carter to Reshape US Military: Goldwater–Nichols II," *Breaking Defense*, April 5, 2016, http://breakingdefense.com/2016/04/carter-to-reshape-us-military-goldwater-nichols-ii/ (accessed July 8, 2017).
23. Thomas A. Keaney and Eliot A. Cohen, *Gulf War Air Power Survey Summary Report*, Washington, DC, 1993, http://www.dtic.mil/dtic/tr/fulltext/u2/a273996.pdf (accessed July 8, 2017).
24. General Robert H. Scales, *Certain Victory: The US Army in the Gulf War* (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, Select Reprint, 1994), http://usacac.army.mil/cac2/cgsc/carl/download/csipubs/CertainVictory.pdf (accessed July 8, 2017).
25. Peter D. Haynes, "American Naval Thinking in the Post–Cold War Era: The U.S. Navy and the Emergence of a Maritime Strategy, 1989–2007," PhD dissertation, Naval Postgraduate School, Monterey, CA, June 2013, http://calhoun.nps.edu/bitstream/handle/10945/34675/13Jun_Haynes_Peter_PhD.pdf?sequence=1 (accessed July 11, 2017).

26. The term "peace dividend" refers to the post–Cold War period of the 1990s when, under the presumption that the world was entering a prolonged era of peace, the U.S. government drew down the funding for and size of the military to reduce the national deficit. For two differing perspectives, see Ann Markusen, "How We Lost the Peace Dividend," *The American Prospect*, July–August 1997, http://prospect.org/article/how-we-lost-peace-dividend (accessed July 8, 2017), and Lynn Woolsey, "Bill Clinton and the Decline of the Military," *Human Events*, December 21, 2006, http://humanevents.com/2006/12/21/bill-clinton-and-the-decline-of-the-military/ (accessed July 6, 2017).
27. United States Army, Training and Doctrine Command, "Multi-Domain Battle," updated June 23, 2017, http://www.tradoc.army.mil/multidomainbattle/ (accessed July 6, 2017).
28. For definitions of "superiority" across various domains, see U.S. Department of Defense, *DoD Dictionary of Military and Associated Terms*, *passim*.
29. See, for example, "air supremacy," in ibid., p. 14.

An Overview of Land Warfare

David E. Johnson, PhD

> "The past is never dead. It's not even past."
> —William Faulkner[1]

Since the dawn of time, as historian T. R. Fehrenbach wrote in *This Kind of War*, "the object of warfare [has been] to dominate a portion of the earth, with its peoples, for causes either just or unjust. It is not to destroy the land and people, unless you have gone wholly mad."[2] Fehrenbach was analyzing U.S. involvement in the Korean War, and in his preface, he draws a lesson from that war—fought in a time of great-power competition between nuclear-armed adversaries—that bears revisiting today:

> The great test placed upon the United States was not whether it had the power to devastate the Soviet Union—this it had—but whether the American leadership had the will to continue to fight for an orderly world rather than to succumb to hysteric violence.... Yet when America committed its ground troops into Korea, the American people committed their entire prestige, and put the failure or success of their foreign policy on the line.[3]

Over the past 15 years, the United States has become an expeditionary power, largely based in the Continental United States, accustomed to projecting power by dominating the air, maritime, space, and cyber domains. U.S. superiority was routinely contested only in the land domain, albeit largely by irregular adversaries, insurgents, and terrorists. U.S. domain supremacy is eroding, if not ending, with the renewal of great-power competition with state actors—principally China and Russia—that can contest U.S. operations to some degree in all domains. This reality will shape how land forces contribute to U.S. security now and into the future.

Where We All Live

Of all the domains, the land domain has the greatest ability to create operational friction. It is the environment that informed Clausewitz's admonition that "Everything in war is very simple, but the simplest thing is difficult."[4] Soldiers and Marines cannot "slip the surly bonds of earth."[5] It is the domain where humans live, and operating there almost certainly results in human interaction—for good or ill.

The Inherently Complex Physical Aspects of Terrain. The land domain, unlike other physical domains (air and maritime) is highly variable, and its very nature forces adaptation by ground forces. According to the Army's 2005 working definition:

> ["Complex terrain" is comprised of] those areas that severely restrict the Army's ability to engage adversaries at a time and place of its choosing due to natural or man-made topography, dense vegetation or civil populations, including urban, mountains, jungle, subterranean, littorals and swamps. In some locales, such as the Philippines, all of these features can be present within a ten-kilometer radius.[6]

Retired Army Lieutenant General Patrick M. Hughes succinctly summed up the implications of operating in complex terrain: "It is dam (*sic*)

hard to find a vacant lot to hold a war in...and in this new era of warfare, that's the last thing the enemy wants anyway."[7] Additionally, superiority in the other domains does not simplify the demands that land places on ground forces.

Operations in Afghanistan, both now and during occupation by the Soviet Union, show the effects of complex terrain. The absence of roads and the mountainous terrain make helicopters important in movement of forces, medical evacuation, and resupply. However, the weather and terrain (cool and thin air at high altitudes affecting lift) also make flying helicopters much more difficult than in Iraq (hot air at low altitudes with good lift).[8]

The continued global trend toward urbanization means that dense urban terrain is a likely future operational environment. "In the future," Army Chief of Staff General Mark Milley noted in October 2016, "I can say with very high degrees of confidence, the American Army is probably going to be fighting in urban areas."[9] While dense urban terrain can affect all of the domains, it creates particularly difficult challenges for land forces, as recent U.S. experiences in Mogadishu, Fallujah, Baghdad, and Mosul demonstrate.

Dense urban areas enable an adversary to hide, both physically and among the population, move unobserved, and achieve positions of advantage over friendly forces. Dense urban terrain occludes target acquisition by reducing targetable signatures and target exposure times. Beyond slowing the advance of ground forces, urban areas have a canalizing effect on mobility that not only affects approach speed, but significantly increases the risk to maneuver elements. It slows ground operations and often involves clearing buildings one by one, putting friendly ground forces at risk. Subterranean features like subways and sewer tunnels, multistory buildings, and "urban canyons" only further complicate operations in cities, as experienced by Germany in Stalingrad during World War II and by Russia in Grozny during its Chechen Wars.[10]

Weather. Weather, notoriously unpredictable and ever changing, can conspire with terrain to complicate the inherent challenges of land domain operations. Weather can impede the ability to employ maritime and air domain capabilities in support of ground operations and can make ground maneuver difficult. A sandstorm caused a pause in ground maneuver during the coalition drive to Baghdad in 2003.[11] Furthermore, as the Germans realized during Operation Barbarossa, winter in Russia can be a formidable adversary. Weather and tides were critical decision points for the invasion of Normandy in June 1944 and Incheon in September 1950. Bad weather enabled the German offensive in the Ardennes in late 1944 by grounding Allied air support.

Fog, rain, dust storms, sandstorms, and darkness can affect the ability to see the enemy and employ air support and can limit the effective range of weapons that require line of sight to the target. In addition, cold and heat can affect the performance of soldiers and increase logistical demands: Hot weather, for example, increases the demand for water.

Opportunities and Challenges. The principal opportunity that land forces offer is the ability to impose a decision on adversaries that the other domains cannot: taking and holding ground, destroying enemy forces in detail, and controlling and protecting populations. Many of the types of military operations required by U.S. policy and joint doctrine shown in Table 1 can be accomplished, in whole or in part, only with elements operating in the land domain.

Politically and strategically, operations in the land domain signal U.S. commitment because land forces, once deployed, can be difficult to extract. They are there for the duration. Ground forces are also essential for deterrence, even in relatively small numbers. As Charles Krauthammer has noted:

> Today we have 28,000 troops in South Korea.... Why? Not to repel an invasion. They couldn't. They're not strong enough. To put it very coldly, they're there to die. They're a deliberate message to the enemy that if you invade our ally you will have to kill a lot of Americans first. Which will galvanize us into a full-scale war against you.[12]

At the tactical and operational levels, the physical qualities of the land domain can

TABLE 1

Examples of Military Operations and Activities

- Stability activities
- Defense support of civil authorities
- Foreign humanitarian assistance
- Recovery
- Noncombatant evacuation
- Peace operations
- Countering weapons of mass destruction
- Chemical, biological, radiological, and nuclear response
- Foreign internal defense
- Counter-drug operations
- Combating terrorism
- Counterinsurgency
- Homeland defense
- Mass atrocity response
- Security cooperation
- Military engagement

SOURCE: U.S. Department of Defense, Joint Chiefs of Staff, "Joint Operations, Joint Publication 3–0," January 17, 2017, p. V–2, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf (accessed August 14, 2017).

heritage.org

provide opportunities that other domains do not, such as physical protection. Adversaries and friendly forces can hide from observation and avoid accurate attack from the other domains, particularly the air domain. Fortifications, foxholes, barriers, gullies, subways, buildings, etc., all provide the ability to avoid the effects of enemy weapons. There are no foxholes in the sky.[13]

This was the case in the 2006 Lebanon War, when Hezbollah hid rockets and other systems in forested areas and in bunkers to avoid detection by and attack from Israel's air force. Similarly, the Islamic State (ISIS) went to ground in Mosul, using congested, dense urban areas and hiding among the people to avoid destruction from the air and to force Iraqi ground forces to clear the city block by block. The Germans used the "impassable" Ardennes Forest to marshal forces for their attack and achieved surprise over Allied forces. Similarly, the North Vietnamese used the cover of thick jungles to move troops and supplies into South Vietnam throughout the Vietnam War, despite U.S. air supremacy.

The land can also be used to conceal hazards like mines, booby traps, and obstacles that impede movement. There are also other inherent advantages for land forces in comparison with forces from other domains because they can:

- Maneuver on the land and take advantage of terrain;
- Counter adversary maneuver and protect against adversary special operations forces (SOF) activities;
- Build partner capacity by training and advising;
- Operate more easily without the highly "nodal" structures of air and maritime forces;
- Harden, conceal, and disperse their capabilities;
- Network with terrestrial links (e.g., buried fiber optics) that are hard to access and disrupt;
- Stockpile relatively large amounts of ammunition that can be protected;
- Reload, resupply, and refuel in theater and away from large, vulnerable bases;
- Maneuver in the absence of overhead intelligence, surveillance, and reconnaissance (ISR) and global positioning system data with analog systems and target enemy forces; and
- Enable operation in the other domains from ground positions (e.g., counter integrated air defense fires).

These advantages, however, are not without their challenges. The forces and capabilities have to be in place on the ground with sufficient capacity to turn the land force element into more than a speed-bump deterrent. Furthermore, as noted, the land domain's principal challenges are posed by its inherent nature. Movement, the sustainment of forces, protection from the elements—and the adversary—all make land operations different from those in the other domains.

The nature of operations on land, shaped by the ability of land forces to traverse expanses of varied terrain quickly, makes the positioning of forces a critical matter. Being close to an expected area of action confers important advantages over a competitor who is farther away. Consider the physical posture of U.S. forces in Europe just three decades ago. During the Cold War, U.S. ground forces were essentially toe-to-toe with the Warsaw Pact along the German border, with substantial forces prepared to reinforce from the United States. Since the end of the Cold War, U.S. ground forces have been based mostly in the Continental United States. The difference between U.S. levels in Europe toward the end of the Cold War and those maintained there today are startling.

Until the resurgence of Russia, a reduced posture seemed adequate to protect U.S. interests while minimizing the costs of overseas bases. The current U.S. posture in NATO, however, is now problematic, particularly in Eastern Europe in the face of recent Russian adventurism.

The Baltic States, made members of NATO in its post–Cold War expansion, are vulnerable with little U.S. or NATO presence to provide a deterrent. The lone rotational U.S. Army armored brigade combat team in Poland and the Baltics is the only capability on the ground to deter Russia, aside from the modest Polish and Baltic State defense forces. War games held by a variety of organizations have repeatedly demonstrated that Russian forces could likely reach the outskirts of Baltic capital cities in 60 hours or less, leaving U.S. and allied forces little time to deploy.[14] Although the armed forces of the Russian Federation are much smaller than those maintained by the Soviet Union during the Cold War, they are physically located on NATO's eastern flank. Today, the two permanently stationed U.S. brigades, neither of which is armored, are distant from the Baltics in Germany and Italy. Geography alone thus suggests a high probability that the Russians could rapidly present NATO with a fait accompli if they chose to invade the Baltics.

Restoring a credible deterrent in Europe is an expensive proposition. It would require stationing more forces in Europe (particularly in NATO's frontline states), negotiating basing rights, establishing prepositioned equipment sets in sufficient quantities, and a host of other tasks to convince the Russians that military aggression is not a good option while restoring Allied confidence in American resolve. Deterring in Eastern Europe is different from defending along the German border during the Cold War. The distance from the United States is greater, and reinforcements would have to come across land from Western Europe or risk attempting to arrive by air or sea under a formidable Russian anti-access/area-denial (A2/AD) complex that covers much of Eastern Europe and the Baltic Sea.

Today, U.S. forces deploy from bases at home to conduct operations globally, which include rotational forces in Afghanistan and Iraq and modest forward-stationed ground forces in South Korea and those already mentioned in Europe. This view that forces were better maintained at home but kept available for global deployment was a logical consequence of the collapse of the Soviet Union. It was further buttressed by the conclusion that China's military rise was principally a challenge for the air, maritime, space, and cyber domains, even though ground forces could contribute with maneuver forces, SOF, long-range fires, and complementary capabilities in electronic warfare, cyber, and intelligence, reconnaissance, and surveillance.[15]

As important as the physical positioning of forces is the ability of those forces to win in battle, which depends in no small measure on their technological edge when compared with

the enemy's forces. Investments in ground force modernization are urgently required to reverse the situation described by Lieutenant General H. R. McMaster in testimony before Congress in 2016: "We are outranged and outgunned by many potential adversaries."[16] After a decade of relative peace followed by 15 years of counterinsurgency operations, modernization of U.S. Army capabilities for high-end conventional combat has repeatedly been shelved in favor of other priorities.

The Nature of Adversaries and Implications for Operations

The characteristics of the adversary, like terrain, create an inherent complexity that determines what can be done, what cannot be done, and the difficulty of the operation. As the old saying goes, the enemy always gets a vote.

Understanding enemy strengths, capabilities, locations, activities, and possible courses of action are key questions for commanders to understand as they frame their own plans.[17] What has become increasingly apparent since the 2006 Lebanon War is that there are three broad categories of adversaries that the United States could confront in the future: non-state irregular, state-sponsored hybrid, and state forces.

Importantly, the nature of the enemy and his will to continue fighting often can be countered and defeated only by ground forces. Protracted air operations can be costly and eventually result in diminishing returns. Naval power has little, if any, ability to overturn enemy seizure or control of land. This is also true for cyber and space.

Non-State Irregular Adversaries. These are the main types of adversaries the United States has fought since 9/11, including the Taliban, al-Qaeda, and now the Islamic State. The Russians faced this type of adversary in the mujahedeen during the early stages of its Cold War–era war in Afghanistan, as did the Israelis during the intifadas in the West Bank and Gaza. These adversaries are generally limited to small arms; rocket-propelled grenades (RPGs); improvised explosive devices (IEDs); and the occasional mortar, rocket, or man-portable air defense system (MANPADS). Their activity is limited primarily to operations in the land domain.

Operations to counter non-state/irregular forces often require large numbers of ground forces for protracted periods, as seen in Afghanistan and Iraq. The luster of rapid victories in Afghanistan (2001) and Iraq (2003) quickly faded as insurgencies grew in both countries. U.S. counterinsurgency doctrine demands forces on the ground to augment, train, and advise the supported government and its security forces until they can take the lead with less direct U.S. assistance, and operational demands can be significant:

> Counterinsurgents can apply pressure on an insurgency by conducting raids on cell members; recovering enemy caches; interdicting supply routes; searching or seizing resources from cars, homes, and personnel entering the area of operations; isolating the insurgents from access to markets, smugglers, and black-market goods; and by conducting offensive operations that diminish guerrilla numbers.[18]

These activities, focused on protecting the population, require significant numbers of ground forces, as seen in the 2006 U.S. Army and Marine Corps counterinsurgency doctrine: "Twenty counterinsurgents per 1,000 residents is often considered the minimum troop density required for effective COIN operations; however as with any fixed ratio, such calculations remain very dependent upon the situation."[19] The Surge in Iraq succeeded in large part because it "achieved a 50 per thousand ratio in Iraq, with 30 million people being protected by 600,000 counterinsurgents (160,000 coalition troops, 340,000 Iraqi security forces, and 100,000 Sons of Iraq)."[20]

Conventional ground forces are augmented by special operations forces that "provide conventional forces with important cultural and advising capabilities. They also provide important offensive capabilities. SOF capable of conducting direct action might be able to conduct raids and gain intelligence that conventional forces cannot execute."[21]

Insurgents are often fixed in the close fight and defeated using direct and indirect fires (artillery and air strikes). Rarely is a U.S. platoon or larger formation at risk.[22]

If the objective of U.S. policy is to change conditions on the ground in an enduring way, large numbers of ground forces are likely to be needed.[23] Nevertheless, over time, the goal is that most (eventually all) land forces will be indigenous, with U.S. land forces providing trainers and advisers and supporting the operations of local forces by employing enablers from the other domains. This transition is occurring now in Iraq in the fight against ISIS, and it is a major goal of the International Security Assistance Force in Afghanistan.

One of the most difficult aspects of countering an insurgency is maintaining the political will to endure the costs in blood and treasure of a protracted conflict. As that will fades, political restrictions on force levels and engagements may result, easing the pressure on insurgent groups. The burden on the counterinsurgent is that he must win, while the insurgent need only avoid losing to maintain influence.

State-Sponsored Hybrid Adversaries. State-sponsored or other hybrid forces may reflect many of the attributes and behaviors of an insurgent force yet possess a significantly higher level of lethality and sophistication. Russian-backed separatists in Ukraine and Hezbollah represent two modern hybrid forces, and U.S.-backed anti-Soviet mujahedeen in Afghanistan were an early example.

The challenge posed by these adversaries is qualitatively different from the challenge posed by irregular opponents—similar to major combat operations but at a lower scale and with a mix of niche but sustainable high-end capabilities such as anti-tank guided missiles (ATGMs), MANPADS, and intermediate-range or long-range surface-to-surface rockets provided by a state actor that may allow hybrid forces to employ lethal force from greater range and with greater survivability.[24] Hybrid adversaries not only attempt to hide from overhead ISR systems by using terrain or mixing with the civilian population, but also may seek to jam or otherwise counter key ISR capabilities directly.

Land forces, using combined arms maneuver, are required to make these adversaries visible and then defeat them in close combat augmented by indirect fires (artillery and air strikes). The United States has not fought adversaries approximating the hybrid capabilities of Hezbollah or the Ukrainian separatists since it confronted North Vietnamese main force units during the Vietnam War. These types of adversaries can also inflict substantial casualties, as seen in the destruction of Ukrainian battalions by separatist rocket fire.[25]

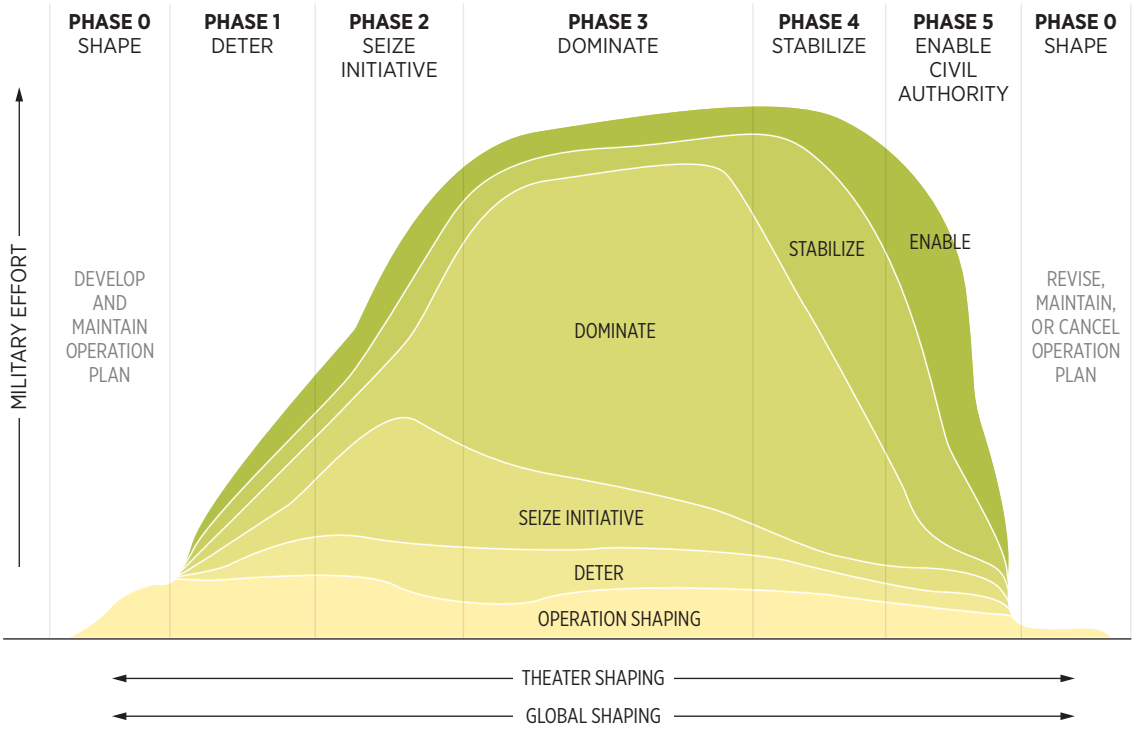
The U.S. military has not suffered mass casualties of the kind these systems could impose since the Korean War, and the U.S. Army, in particular, is increasingly aware that it needs new capabilities (e.g., active protection for combat vehicles against RPGs and ATGMs) to operate against state-sponsored hybrid adversaries. As Acting Secretary of the Army Patrick J. Murphy and Army Chief of Staff General Mark A. Milley acknowledged in their 2017 posture statement, "While we are deliberately choosing to delay several modernization efforts, we request Congressional support of our prioritized modernization programs to ensure the Army retains the necessary capabilities to deter and if necessary, defeat an act of aggression by a near-peer."[26]

Beyond military capabilities, hybrid adversaries may also enjoy political advantages that make wholly defeating them difficult. Hybrid forces may have cross-border sources of supply that are difficult to interdict. Further, they may enjoy the support of the local populace, as Hezbollah does in Lebanon. If they are seen as the legitimate government or at least as a strong political actor, their defeat could be regionally destabilizing.

State Adversaries. Events in Ukraine, Syria, and the Pacific have drawn U.S. attention once more to high-end state adversaries (Russia, China, North Korea, and Iran) that have capabilities ranging from small arms to nuclear weapons. They have long studied U.S. capabilities and are modernizing their militaries to contest the United States across all

FIGURE 1

Phasing an Operation Based on Predominant Military Activities



NOTE: Figure is illustrative only.
SOURCE: U.S. Department of Defense, Joint Chiefs of Staff, "Joint Operations, Joint Publication 3–0," January 17, 2017, p. V-13, http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf (accessed August 14, 2017).

heritage.org

domains, seeking in particular to undermine the advantages that the U.S. military has enjoyed since Operation Desert Storm, including but not limited to uncontested use of close-in air bases and logistics facilities, overhead and/or persistent ISR, and relatively unprotected, high-bandwidth communications.

Again, the Russians present a particularly difficult challenge because of their proximity to Eastern European NATO members, the lack of NATO forces on the ground in Eastern Europe, and the comparatively small militaries of the NATO frontline states. As noted, this situation is different from the U.S. speed bump in South Korea, where substantial Republic of Korea forces deter North Korean action. Although land forces in the Pacific can make contributions in many areas, they are central to deterring Russian activity in NATO. This will require forward-positioned land forces that are large enough and capable enough to convince Russia that the game is not worth the candle—a case not made clearly in Georgia, Ukraine, and Syria.

Old Concepts and Better Adversaries

Complicating deterrence demands in Eastern Europe and the Pacific is the advent of a tough, layered A2/AD environment designed to thwart U.S. operations.[27] This challenges the long-standing U.S. operational phasing model shown in Figure 1.

What is important in this figure is the requirement for a steady increase of military effort during Phase I (deter) and Phase II (seize the initiative) before reaching Phase III (dominate). In large-scale operations since the end of the Cold War, Phase II and Phase III have required moving the majority of forces, particularly land forces and their sustainment, from the Continental United States (CONUS) to the theater of operations.

Operations Desert Shield and Desert Storm are good examples of how the United States has employed this phasing construct since the end of the Cold War. While the President and the executive branch of the U.S. government worked to establish coalitions, basing rights, and other agreements, the Department of Defense began to move forces forward to deter Saddam Hussein from attacking Saudi Arabia. This involved activity across the domains, with significant air and maritime components rushing to theater and a quickly deployable buffer force on the ground, initially provided by the rapidly deployable 82nd Airborne Division, backed by overwhelming U.S. superiority in all other domains.

Over the next five months, the U.S. coalition built up sufficient forces and sustainment capacity to seize the military initiative and then dominate in air and ground offensive operations against the Iraqi force occupying Kuwait. What is extremely important from this example—and from the initial operations in virtually all large-scale U.S. operations since World War II—is the fact that the United States initially had unchallenged supremacy in all but the land domain, and this dominance enabled a sanctuary for the buildup of forces sufficient to win in Phase III.

This will not be the case against near-peer regional adversaries. U.S. abilities to project power into their regions or steadily build up combat power and sustainment capacity will be confronted by formidable A2/AD capabilities that could interdict reinforcements as they close on the conflict zone. Thus, there is likely to be greater emphasis in the future on having greater combat power forward not just for deterrence, but to also conduct the initial stages of a conflict while the joint force seeks to regain freedom of maneuver, an arduous process of methodically degrading or defeating the enemy's efforts to impede U.S. operations.

This rising challenge of reinforcement stems from the emergence and adoption of new technologies across all domains that are contesting U.S. capabilities to deploy and operate. Secretary of Defense James Mattis testified in June before the House Armed Services Committee that:

> For decades, the United States enjoyed uncontested or dominant superiority in every operating domain or realm. We could generally deploy our forces when we wanted, assemble them where we wanted, and operate how we wanted. Today, every operating domain is contested.[28]

Furthermore, getting to the operational area is only half of the problem; operating there will also be heavily contested. In his written testimony, Secretary Mattis elaborated, noting that "the introduction of long-range air-to-surface and surface-to-surface guided weapons, advanced armored vehicles and anti-tank weapons, and tactical electronic warfare systems" threatens U.S. dominance on land.[29]

General Joseph Dunford, Chairman of the Joint Chiefs of Staff, shares Mattis's concern, testifying in the same session that "[i]n just a few years, if we don't change our trajectory, we will lose our qualitative and quantitative competitive advantage." He also said that the Budget Control Act denies the U.S. military the "sustained, sufficient and predictable funding" that it needs. If this situation is not rectified, Dunford warned, the United States will lose "our ability to project power," and the U.S. military will be "much smaller" or "a hollow force."[30] The Army's *Future Force Development Strategy* sums up what this means for a service whose role is sustained land combat:

> The Army faces the triple effect of a reduced force combined with an aging combat fleet and a severe reduction of research and

development spending. This reduction comes just as revisionist powers are aggressively challenging the world order and modernizing their own militaries. Modernization resources are close to historic lows since 1945. The Army requires resources in order to maintain tactical overmatch.[31]

Thus, there is an urgent need for new concepts and capabilities across the U.S. armed forces that can be used to solve the access challenge. For land forces, these concepts and modernization initiatives will need to assist the U.S. Army and Marine Corps to operate and win in increasingly contested land environments while under threat from combined arms fires that include missile, air, and other potential challenges.

Air and naval forces can mitigate the access challenges posed by increasingly capable competitors, but only to the extent that they can get enemy targets within range of the weapons they carry (increasingly a problem for naval forces in particular) and sustain an effective posture overhead (a growing problem for air forces). Thus, the Army must have better organic capabilities that are relevant to conducting land warfare in the modern age. To improve warfighting capabilities for these future battlefields, the Army has established modernization priorities to close the capability gaps that U.S. land forces face against capable adversaries:

1. Air and Missile Defense (SHORAD, short-range air defense);
2. Long-Range Fires such as improvements to multiple launch rocket systems (MLRS) and advanced weapons like the Army Tactical Missile System (ATACMS);
3. Munitions;
4. Mobility, Lethality, and Protection of brigade combat teams (BCTs);
5. Active Protection Systems, Air and Ground;
6. Assured position, navigation, and timing (PNT);
7. Electronic Warfare/Signals Intelligence;
8. Cyber (offensive and defensive);
9. Assured Communications (i.e., protected from enemy compromise or denial); and
10. Vertical lift (e.g., next-generation helicopters or tiltrotor aircraft).[32]

Together, these capability areas will help to improve Army resiliency in the event joint control of other enabling domains is disrupted. Further, they would provide the Army (and the Marine Corps) with the ability to impose cross-domain effects on an adversary in support of joint operations, such as through ground-based counter-air and electromagnetic warfare systems. As air and naval forces can enable land operations, so too can land forces facilitate operations in other domains by leveraging their ability to bring "fires" to bear against targets that threaten platforms and forces operating in the air and naval domains. It is not enough just to develop next-generation systems, however. The Army and Marine Corps must integrate these capabilities together in functional warfighting concepts, exercise those concepts, and then prepare to fight that way in the field.

How Are the Domain and Related Warfare Concepts Changing?

The resurgence of Russia has brought the role of land operations to the fore again, back to the war Fehrenbach described in *This Kind of War*, which highlighted the centrality of the land domain and the need to put boots (and fires, electronic warfare, and other land-based capabilities) on the ground to achieve policy objectives and enable success in the other domains:

> Americans in 1950 rediscovered something that since Hiroshima they had forgotten: you may fly over a land forever; you may bomb

> it, atomize it, pulverize it and wipe it clean of life—but if you desire to defend it, protect it, and keep it for civilization, you must do this on the ground, the way the Roman legions did, by putting your young men into the mud.[33]

Technology and special operations forces will not provide universal solutions. These are the central points that make land forces a key component of a force that deters adversaries, as U.S. ground forces have done on the Korean Peninsula since the Korean War and did in NATO during the Cold War. Ground forces are also important to compel adversaries if deterrence fails; Operation Desert Storm accomplished this by physically forcing Iraqi forces out of Kuwait.

Arguments abound that dominance in new domains—airpower following World War II or cyber today—can render land power all but obsolete by deterring or defeating adversaries or at least sufficiently degrading their capabilities to the point that they are no longer a significant threat to the interests of the United States or its partners. The protracted aftermaths of the initial "victories" in Afghanistan and Iraq, both states with only limited capabilities to contest U.S. operations in other domains, have not yet put these arguments to rest, despite the difficulty with which the United States pursued its policy objectives. Possible future conflicts with peer competitors, who will possess far more sophisticated domain-denial capabilities, will likely bear little resemblance to recent U.S. warfighting experiences and reflect the difficulties of achieving victories through a single dominant domain.

Additional arguments similar to those extolling the primacy of technology have risen in the post–9/11 world as the United States has begun to rely on relatively small numbers of highly trained special operations forces in its fight against disparate insurgent and terrorist organizations. Special forces have enormous utility because they can direct precision attacks by air and maritime forces and can also conduct precision raids to kill or capture high-value targets. Both special forces and small detachments of conventional ground forces can deploy to train and advise partner forces and enable their use of our capabilities without becoming directly engaged in combat themselves. Yet special forces cannot hold terrain against determined adversaries and cannot retake land seized through acts of aggression.

Thus, an assessment of the continued relationship between ground forces and the attainment of U.S. policy objectives is fundamental to understanding the full portfolio of capabilities and capacities that the United States will likely require in the future. Land forces will continue to be a vital part of future conflicts, whether they are the supported element of a principally land-based war or serve as an enabling force assisting other elements to retake control of the skies and seas of a littoral conflict. Many elements of military competition in the 21st century will be defined by air, naval, and cyber forces, but the fate of lands and peoples will continue to be determined principally by the staying power of land forces.

The Nature of the Competition

The global military challenges that confront the United States are evolving, and they are doing so in different ways. Managing these disparate challenges will be an added complication for the joint force. Today, just as Japan and Nazi Germany represented unique challenges in the 1930s and 1940s, a rising China and resurgent Russia pose problems that are dramatically different from anything else that the United States has faced since the end of the Cold War. Coupled with these near-peer competitors are the continued challenges posed by North Korea, Iran, turmoil in the Middle East, and global terrorism.

Concepts and capabilities that work in one setting and the mix of land with other forms of military power may have little relevance in other settings. What is clear is that capabilities that put the joint force at risk against even mid-tier competitors are proliferating. The need for force modernization to restore overmatch in the land domain is urgent. Also needed are

new concepts for how to employ these modernized forces—with the understanding that what might work against one adversary might not work against another.

Understanding the problem is the first step in developing solutions. In the land domain, as already discussed, distance, terrain, weather, and the nature of our adversaries combine to create complex problems that often only land forces can solve.

In the *2017 Index of U.S. Military Strength*, Antulio Echevarria discussed the central importance of and challenges involved in crafting new operational concepts to "provide a way to convert military strength into military power: the ability to employ military force where and when we want to employ it."[34] While noting the success of some U.S. concepts like Air-Land Battle, he highlights the failure of Effects-Based Operations and the incomplete nature of Air-Sea Battle.[35] What all of these concepts share is that they began as a way that U.S. forces wanted to fight and then later evolved into general-purpose solutions for confronting any adversary.

The recently published Army–Marine Corps white paper, "Multi-Domain Battle: Combined Arms for the 21st Century," recognizes the military problem that the current and future operating environments pose for the United States across the domains: "U.S. ground combat forces, operating as part of a joint, interorganizational, and multinational teams [*sic*], are currently not sufficiently trained, organized, equipped, nor postured to deter or defeat highly capable peer enemies to win in future war."[36] The paper also includes a "Solution synopsis":

> *Multi-Domain Battle: Combined Arms for the 21st Century requires ready and resilient Army and Marine Corps combat forces capable of outmaneuvering adversaries physically and cognitively through the extension of combined arms across all domains.... Through credible forward presence and resilient battle formations, future Army and Marine Corps forces integrate and synchronize capabilities as part of a joint team to create temporary windows of superiority across multiple domains and throughout the depth of the battlefield in order to seize, retain, and exploit the initiative; defeat enemies; and achieve military objectives.*[37]

While a good starting point, however, the Multi-Domain Battle concept is just the beginning. Much work remains to be done as the United States is now in a competition for the first time since the Cold War with adversaries who can challenge, and perhaps defeat, America's armed forces in their local regions.

Conclusion

For the first time since the 1940s, the United States faces the prospect of peer competitors in the Pacific and Europe that can challenge U.S. capabilities in their regions. Coupled with these high-end adversaries are other actors, ranging from rogue states (North Korea and Iran) to hybrid adversaries (Hezbollah) to irregular terrorist threats (al-Qaeda, the Taliban, and ISIS). In this evolving security environment, the land domain will be particularly important both in crafting concepts and capabilities to support U.S. deterrence regimes and in defeating America's enemies if deterrence fails.

Time and current resourcing levels, however, are not on our side. If the United States does not approach these challenges with the urgency required, it will forfeit its credibility as a great power.

Endnotes

1. William Faulkner, *Requiem for a Nun* (New York: Vintage Books, 2011), p. 73. I want to thank my colleagues Ryan Boone, Tom Mahnken, Whitney McNamara, and Rick Russo for their helpful comments on earlier versions of this essay.
2. T. R. Fehrenbach, *This Kind of War: The Classic Military History of the Korean War* (Dulles, VA: Potomac Books, 2008), p. 290.
3. Ibid., p. x.
4. Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), p. 119.
5. Peter Armenti, "John Gillespie Magee's 'High Flight,'" Library of Congress, September 3, 2013, https://blogs.loc.gov/catbird/2013/09/john-gillespie-magees-high-flight/ (accessed June 19, 2017).
6. Brad Andrew, "It's More Than Urban...," *Military Intelligence Professional Journal*, Vol. 31, No. 2 (April–June 2005), pp. 61–62, https://fas.org/irp/agency/army/mipb/2005_02.pdf (accessed June 19, 2017).
7. Ibid.
8. Mark Thompson, "Why Flying Choppers in Afghanistan Is So Deadly," *Time*, October 27, 2009, http://content.time.com/time/nation/article/0,8599,1932386,00.html (accessed June 19, 2017).
9. Michelle Tan, "Army Chief: Soldiers Must Be Ready to Fight in 'Megacities'," *Army Times*, October 5, 2016, http://www.defensenews.com/articles/army-chief-soldiers-must-be-ready-to-fight-in-megacities (accessed June 19, 2017).
10. For recent studies on urban operations, see David E. Johnson, Matthew Wade Markel, and Brian Shannon, *The 2008 Battle of Sadr City: Reimagining Urban Combat* (Santa Monica, CA: RAND Corporation, 2013), http://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR160/RAND_RR160.pdf (accessed June 19, 2017); Gian Gentile, David E. Johnson, Lisa Saum-Manning, Raphael S. Cohen, Shara Williams, Carrie Lee, Michael Shurkin, Brenna Allen, Sarah Soliman, and James L. Doty III, *Reimagining the Character of Urban Operations for the U.S. Army: How the Past Can Inform the Present and Future* (Santa Monica, CA: RAND Corporation, 2017), http://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1602/RAND_RR1602.pdf (accessed June 19, 2017); and Colonel Marc Harris, Lieutenant Colonel Robert Dixon, Major Nicholas Melin, Command Sergeant Major Daniel Hendrex, Sergeant Major Richard Russo, and Michael Bailey, *Megacities and the United States Army: Preparing for a Complex and Uncertain Future* (Washington: Chief of Staff of the Army, Strategic Studies Group, June 2014), https://www.army.mil/e2/c/downloads/351235.pdf (accessed June 20, 2017).
11. CNN Student News, "U.S. Troops Weather Sandstorm, Cross Euphrates River," March 25, 2003, http://www.cnn.com/2003/fyi/news/03/25/iraq.war/ (accessed June 20, 2017).
12. Charles Krauthammer, "To Die for Estonia?" *The Washington Post*, June 2, 2017, p. A19, https://www.washingtonpost.com/opinions/global-opinions/to-die-for-estonia/2017/06/01/465619a6-46f1-11e7-a196-a1bb629f64cb_story.html?utm_term=.7cb38c158156 (accessed June 19, 2017).
13. From the book title: George C. Henry, *No Foxholes in the Sky and Guns of Ploesti* (Dallas: G. C. Henry, 2007).
14. For output from one such war game, see David A. Shlapak and Michael W. Johnson, *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics* (Santa Monica, CA: RAND Corporation, 2016), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1253/RAND_RR1253.pdf (accessed June 20, 2017).
15. See Evan Braden Montgomery, *Reinforcing the Front Line: U.S. Defense Strategy and the Rise of China*, Center for Strategic and Budgetary Assessments, 2017, p. 38, http://csbaonline.org/research/publications/reinforcing-the-front-line-u.s.-defense-strategy-and-the-rise-of-china (accessed June 20, 2017), and Timothy M. Bonds, Joel B. Predd, Timothy R. Heath, Michael S. Chase, Michael Johnson, Michael J. Lostumbo, James Bonomo, Muharrem Mane, and Paul S. Steinberg, *What Role Can Land-Based, Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression?* (Santa Monica, CA: RAND Corporation, 2017), https://www.rand.org/pubs/research_reports/RR1820.html (accessed June 20, 2017).
16. Sydney J. Freedberg Jr., "McMaster: Army May Be Outnumbered AND Outgunned in Next War," *Breaking Defense*, April 6, 2016, http://breakingdefense.com/2016/04/mcmaster-army-may-be-outnumbered-and-outgunned-in-next-war/ (accessed June 20, 2017).
17. U.S. Department of the Army, Field Manual No. 3-0, *Operations*, June 2001, p. 5-4, http://cnqzu.com/library/Anarchy%20Folder/Combat/Operations%20-%20FM%203-0.pdf (accessed June 19, 2017).
18. U.S. Department of the Army, Field Manual No. 3-24/U.S. Marine Corps, Warfighting Publication No. 3-33.5, *Insurgencies and Countering Insurgencies*, May 2014, p. 5-4, https://fas.org/irp/doddir/army/fm3-24.pdf (accessed June 20, 2017).
19. Ibid., p. 1-13.
20. Conrad C. Crane, *Cassandra in Oz: Counterinsurgency and Future War* (Annapolis, MD: United States Naval Institute Press, 2016), p. 288, https://www.usni.org/store/books/transforming-war-series/cassandra-oz (accessed June 19, 2017).
21. U.S. Department of the Army/U.S. Marine Corps, *Insurgencies and Countering Insurgencies*, p. 6-6.

22. David E. Johnson, *Hard Fighting: Israel in Lebanon and Gaza* (Santa Monica, CA: RAND Corporation, 2011), pp. 148–149, http://www.rand.org/content/dam/rand/pubs/monographs/2011/RAND_MG1085.sum.pdf (accessed June 19, 2017).
23. See James T. Quinlivan, "Force Requirements in Stability Operations," *Parameters*, Vol. 25, No. 4 (Winter 1995–1996), pp. 59–69, http://ssi.armywarcollege.edu/pubs/parameters/Articles/1995/quinliv.htm (accessed June 20, 2017). Quinlivan's analysis informed Army and Marine Corps doctrine on this topic: "Twenty counterinsurgents per 1000 residents is often considered the minimum troop density required for effective [counterinsurgency] operations; however as with any fixed ratio, such calculations remain very dependent upon the situation.... As in any conflict, the size of the force needed to defeat an insurgency depends on the situation." U.S. Department of the Army/U.S. Marine Corps, *Insurgencies and Countering Insurgencies*, pp. 1–13. See also David E. Johnson, "Fighting the 'Islamic State': The Case for U.S. Ground Forces," *Parameters*, Vol. 45, No. 1 (Spring 2015), p. 14, https://ssi.armywarcollege.edu/pubs/parameters/Issues/Spring_2015/4_Special-Commentary_Johnson.pdf (accessed June 19, 2017): "One could argue that they were not met across Iraq during the surge, but within Baghdad, considered by many to be the center of gravity of the war, there were approximately 131,000 U.S.–Iraqi security forces in a city with a population of some 7,000,000, which came close to the doctrinal ratio."
24. Johnson, *Hard Fighting*, pp. 153–154. "The term hybrid threat captures the seemingly increased complexity of operations, the multiplicity of actors involved, and the blurring between traditional elements of conflict. **A *hybrid* threat is the diverse and dynamic combination of regular forces, irregular forces, terrorist forces, or criminal elements unified to achieve mutually benefitting threat effects.**" Emphasis in original. U.S. Department of the Army, Army Doctrine Reference Publication No. 3-0, *Operations*, November 2016, p. 1-3, http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/ADRP%203-0%20FINAL%20WEB.pdf (accessed June 25, 2017). Italics and bold in original.
25. U.S. Army Training and Doctrine Command, Army Capabilities Integration Center, Maneuver, Aviation, and Soldier Division, *The U.S. Army Combat Vehicle Modernization Strategy*, September 15, 2015, p. 15, http://www.arcic.army.mil/app_Documents/CVMS_SEP_Master.pdf (accessed June 23, 2017), and Amos C. Fox, "The Russian–Ukrainian War: Understanding the Dust Clouds on the Battlefield," Modern War Institute, January 17, 2017, https://mwi.usma.edu/russian-ukrainian-war-understanding-dust-clouds-battlefield/ (accessed June 19, 2017).
26. The Honorable Patrick J. Murphy, Acting Secretary of the Army, and General Mark A. Milley, Chief of Staff, United States Army, statement "On the Posture of the United States Army" before the Committee on Armed Services, U.S. Senate, 114th Cong., 2nd Sess., April 7, 2016, p. 6, https://www.armed-services.senate.gov/imo/media/doc/Murphy-Milley_04-07-16.pdf (accessed June 25, 2017).
27. Eric S. Edelman and Whitney Morgan McNamara, *U.S. Strategy for Maintaining a Europe Whole and Free*, Center for Strategic and Budgetary Assessments, 2017, pp. 13–26, http://csbaonline.org/research/publications/u.s.-strategy-for-maintaining-a-europe-whole-and-free/publication (accessed June 25, 2017). See also David E. Johnson, "The Challenges of the 'Now' and Their Implications for the U.S. Army," RAND Corporation *Perspective* No. 184, 2016, https://www.rand.org/pubs/perspectives/PE184.readonline.html (accessed June 25, 2017). Other state adversaries like North Korea and Iran, while perhaps not as formidable as China and Russia, can present significant challenges. Both possess large land forces, air defenses, and large amounts of long-range artillery, rockets, and missiles. North Korea also has nuclear weapons.
28. James Mattis, Secretary of Defense, statement in support of President's FY 2018 budget request before the Committee on Armed Services, U.S. Senate, June 13, 2017, p. 5, https://www.armed-services.senate.gov/imo/media/doc/Mattis_06-13-17.pdf (accessed August 15, 2017).
29. Ibid., p. 6.
30. Patrick Tucker, "Dunford: Without Better Funding, U.S. Will Lose 'Competitive Advantage' in Just a Few Years," *Defense One*, June 12, 2017, http://www.defenseone.com/politics/2017/06/without-better-funding-us-will-lose-competitive-advantage-just-few-years-top-general/138618/ (accessed June 25, 2017).
31. U.S. Army, *Future Force Development Strategy*, May 2017, p. 4.
32. U.S. Department of the Army, Assistant Secretary of the Army (Financial Management and Comptroller), *FY 2018 President's Budget Highlights*, May 2017, p. 18, https://www.asafm.army.mil/documents/BudgetMaterial/fy2018/pbhl.pdf (accessed August 15, 2017).
33. Fehrenbach, *This Kind of War*, p. 290.
34. Antulio J. Echevarria II, "Operational Concepts and Military Strength," in *2017 Index of U.S. Military Strength*, ed. Dakota L. Wood (Washington: The Heritage Foundation, 2016), p. 41.
35. Ibid., p. 43.
36. U.S. Army, Training and Doctrine Command, "Multi-Domain Battle: Combined Arms for the 21st Century," white paper, February 24, 2017, p. 3, http://www.tradoc.army.mil/MultiDomainBattle/docs/MDB_WhitePaper.pdf (accessed June 19, 2017).
37. Ibid., p. 4. Italics in original.

The Naval Warfare Domain

Thomas Callender

The maritime domain, in and through which operations on and under the oceans and seas are conducted, presents unique challenges as well as advantages to maritime nations and military forces. The domain is generally subdivided into two primary categories: littoral (coastal) and open ocean ("blue-water"). The littorals are defined by relatively shallow waters and close proximity to the coasts and include the territorial waters of coastal nations. Open-ocean operations, as the name suggests, are marked by waters beyond the maritime boundaries of nations, with their extreme depths and vast spaces.

While the maritime domain demands some common capabilities and operational concepts for all naval forces, littoral and blue-water environments require very different forces and warfighting strategies. The maritime domain drives some common characteristics for naval vessels: relatively large size and payloads compared to land and air platforms, slow speed, limited organic sensor range, long-range communications requirements, and naval logistics. In addition, the maritime domain shapes naval concepts of operations with tactics such as layered defense, forward presence, and sea control.

Importance of the Maritime Domain

Since prehistoric times, the world's oceans and seas have played a critical part in the development of mankind and many of man's dominant civilizations. Evidence suggests that the earliest man-made boats date back as far as 45,000 years.[1] Initially, these vessels were used for coastal fishing, but as they became larger and more sophisticated, people used them to trade with other coastal civilizations. Once man learned to navigate beyond sight of land and to harness the wind, exploration and trade routes developed across the Mediterranean Sea, the Arabian Sea, the Indian Ocean, and the Pacific Ocean. Maritime exploration also led to human migration between continents and island archipelagos.

The development of larger vessels made it possible to transport greater quantities of commodities both faster and more cheaply than was possible over land routes. These maritime trade routes eliminated the need to transit through the sovereign territory of other nations and pay often exorbitant tolls. However, the movement of large amounts of precious commodities by sea soon led to the rise of piracy. Just as land armies arose to defend national borders and trade routes, armed naval vessels soon arose to help protect these maritime trade routes. From the Ancient Egyptians to the Greeks and on to the rise of the British Empire, dominant maritime trade and naval power were critical to the rise and expansion of these empires.

The oceans and seas still play a vital role in the prosperity and protection of most of the world's population. Of the world's 195 nations, 147 border an ocean or sea, and 40 percent of the world's population lives within 100 kilometers (62 miles) of an oceanic coast.[2] In addition, maritime trade through international shipping

lanes comprises over 90 percent of global commerce.[3] In a modern world that appears to be dominated by wireless communications and satellite broadcasts, 99 percent of all international data (phone, texts, and Internet) is transported over approximately 200 undersea fiber optic cables at speeds eight times faster than satellites.[4] While typically very robust, these submarine cables are susceptible to landslides and other seismic events.

Challenges and Advantages of the Maritime Environment

For those whose experience with the oceans is limited to the coasts, the vastness of the world's oceans is difficult to convey. The five recognized oceans (Atlantic, Pacific, Arctic, Indian, and Southern) cover 71 percent of the Earth's surface with an average depth of 13,000 feet.[5] The Atlantic Ocean covers "approximately 41,105,000 square miles," and the Pacific Ocean covers "more than 60 million square miles," or approximately 20 percent and 46 percent, respectively, of the Earth's surface.[6] For comparison, the Pacific Ocean is larger than all of the Earth's land masses combined;[7] the continental United States covers only 3,120,426 square miles (1.58 percent) of the Earth's surface.[8]

The vastness of the world's oceans presents both advantages and challenges. The immense oceanic distances and limited speed of ships (10–15 knots on average for transoceanic travel) create natural barriers of time and space. For example, these barriers prevented transoceanic exploration and colonization for centuries until shipbuilding technology and seafaring techniques became advanced enough to withstand storms, navigate safely, and carry sufficient supplies to survive weeks or months of travel. While land forces can resupply along their route with local fresh water and food, transoceanic vessels must be self-sufficient for extended periods, carrying or making adequate fresh water, food, and fuel.

The limited speed of naval vessels limits their rapid responsiveness or repositioning. For example, the great circle route (the shortest distance between two points on the curved surface of the Earth) between Norfolk, Virginia, and the Strait of Gibraltar at the entrance to the Mediterranean Sea is 3,326 nautical miles. For a ship traveling at an average speed of 12 knots—a common economical speed for commercial shipping—it would take 11.5 days to make this transit, while a modern jet passenger aircraft traveling at 500 knots would take approximately six hours and 40 minutes.

This time and distance effect requires preplanning or prepositioning of naval forces if a nation desires a timely transoceanic response to maritime crises. For the United States, this has meant development of a forward-deployed blue-water Navy. Maintaining a credible deterrent force constantly deployed near potential naval adversaries enables the U.S. to respond rapidly to maritime security crises before they approach America's shores. This could not be accomplished with naval forces that remain predominantly in their home ports or near territorial waters.

The expanse of the oceans and the lack of landmarks once a sailor gets beyond sight of land present unique navigational challenges when traversing thousands of miles of ever-changing ocean surface. The fact that the ocean's surface varies from one second to the next and does not offer any geographical reference points has led to the development of rather sophisticated navigation techniques and technologies. Satellite navigation systems such as the Global Positioning System (GPS) provide a highly accurate real-time ship's position for both military and commercial vessels. GPS and related technologies have afforded military naval vessels the required positioning, navigation, and timing (PNT) accuracy that enables use of precision-guided munitions and coordinated military operations.

With the advent and subsequent proliferation of GPS-denial or degradation technologies, it has become essential for modern military vessels to have backup navigation systems that are resilient and reliable even in the face of enemy actions. Celestial navigation—the

determination of one's position on the Earth's surface based on the position of celestial bodies, typically the sun, moon, or specific stars—is one such technique that relies on a clear sky and a highly accurate chronometer. An essential skill for sailors across the centuries, celestial navigation is again being taught to young sailors as navies recognize that they cannot rely solely on GPS. Another critical GPS-denied navigation method is inertial navigation, which provides the speed and position of a ship or other platform by measuring its acceleration in all three dimensions. Once extremely large and expensive, current solid-state inertial navigation units are getting smaller and cheaper, enabling their use on small surface vessels and even on unmanned undersea vehicles (UUVs).

The vast ocean expanses have also provided a measure of stealth for naval vessels, although this is becoming less and less true. For years, most modern naval vessels relied primarily on organic radar and electronic support measures (ESM) systems to locate and target adversary naval vessels at over-the-horizon (OTH) ranges beyond the line of sight. Maritime patrol craft and carrier aviation early-warning aircraft were able to extend the ability of these warships to locate and engage adversaries, but the ocean is a very big place, and even with radar, finding a comparatively small ship was still a challenge.

With the rise of intelligence, surveillance, and reconnaissance (ISR) satellites, this "stealth via vastness" was further reduced. The limited number of ISR satellites, however, precluded continuous coverage of any specific area, affording naval vessels opportunities in specific time and location windows to avoid detection.

The current proliferation of commercial and military electro-optic/infrared, radar, and electronic intelligence (ELINT) satellites is providing greater coverage of and more frequent revisit rates to the world's oceans. In addition, maritime domain awareness technologies such as the Automatic Identification System (AIS) provide the location and identity of commercial shipping, thereby helping to clarify the maritime picture. The proliferation of ISR unmanned aerial vehicles (UAVs) is also changing maritime surveillance by greatly increasing the capacity for real-time OTH ISR and targeting information for naval platforms. Not only can long-range land-based UAVs provide ISR coverage hundreds of miles from shore for 12 hours or more at a time, but smaller UAVs are being fielded that can be launched and recovered from naval platforms, providing naval fleets with organic ISR and cueing.

While these systems still have gaps in coverage and some require complex algorithms to scour the vast amounts of imagery required for open-ocean searches, it is getting harder for a large surface naval vessel such as an aircraft carrier to hide in the open ocean. To this end, many modern navies are regularly practicing electromagnetic emission control (EMCON) operations as well as developing technologies and tactics to deny or degrade ISR satellites and related platforms.

The ocean's depths provide their own condition of stealth for submarines and other undersea platforms such as UUVs, enabling undersea forces to move unseen and relatively undetected by adversary forces. This is because the environment below the ocean's surface is drastically different from the world above it. While light and radio waves can travel thousands of miles through the Earth's atmosphere, they penetrate the ocean's depths only from several inches to a maximum of several hundred feet depending on the frequency of the electromagnetic wave (light or radio waves). For example, only a minuscule fraction of sunlight penetrates the ocean's depths beyond approximately 650 feet, and for much of the ocean's depths, visibility is less than 100 feet in any direction. Radar and other radio transmissions cannot be used to search for objects or to communicate with submerged submarines or other undersea platforms. Although this limits the ability of submarines or other undersea platforms to communicate with ships, aircraft, or land-based headquarters, it also hides them from all but the most advanced search techniques.

While the air is the domain of radio waves and light, the ocean's depths are the domain of sound. Sound is the most effective means to communicate or to detect objects across the vast expanse of the oceans. Compared to light and radio waves, sound can travel from thousands of yards up to thousands of miles in water. For example, the vocalization of blue whales (at frequencies as low as 14 Hz) has been detected thousands of miles away.[9] Sound also travels eight times faster in water than in air, and sound waves travel faster as temperature, water pressure, and salinity increase. The deeper, warmer, and saltier the water, the faster sound travels.

The variance in ocean temperature and pressure with depth and geographic location can be exploited to benefit naval operations. Differences in temperature and pressure cause sound waves to bend (or refract) toward the area of slower speed of sound. This bending of sound waves can create "acoustic blind spots" as well as deep-sea sound channels where sound energy is easily transmitted for long distances. Lower-frequency sound travels further in water than higher-frequency sound does. Submarines, surface ships, and aircraft hunting for submarines, as well as land-based command centers communicating with submarines, will use these characteristics to hide from acoustic search or to pulse acoustic energy into the water to affect communications or locate an object.

Background ocean noise can mask quieter noise sources such as submarines. The primary factors contributing to ocean background noise are the sea state (how big the waves are); the amount of local shipping traffic; seismic events such as undersea earthquakes, volcanic eruptions, rock slides, and thermal vents; other noisy maritime evolutions such as fishing and offshore drilling; and even the animal life of the ocean including clicking shrimp, whales, and other marine mammals like porpoises.

Finally, undersea topography can affect the transmission of sound. The ocean's bottom varies from extraordinarily deep trenches to broad plains and undersea mountains, with the floor rising dramatically at times to form walls that stretch upward to the continental shelves. Acoustically, the shallow littoral waters behave differently from the deep oceans as sound waves repeatedly bounce off rocky bottoms and the ocean's surface or are attenuated by muddy sea floors. As on land, these undersea terrain features can affect the transmission of sound and the flow of currents, which in turn can affect temperature gradients as water flows, rises, and falls. The complexity and variability of ocean waters drives undersea naval forces to monitor these changes continuously and alter their tactics and operating profile to exploit any acoustic advantage as effectively as possible.

There are two main types of sound navigation and frequency ranging (SONAR) that provide an acoustic "picture" of the undersea world. The first is passive sonar, which essentially is listening for any noise sources on or below the ocean's surface. Passive sonar provides only the direction from which the sound came.

Active sonar provides a much more complete picture of the undersea environment. Like bats and whales, ships and submarines can transmit sound and then listen for the return echo as the sound wave bounces off an object. Most surface vessels, from small pleasure boats to large commercial transports and naval vessels, use high-frequency active sonar (tens to hundreds of kHz) "depth sounders" to determine the ocean depth beneath them. Active sonars used by submarines and other naval vessels are typically in the 1 kHz to 10 kHz range, with some high-definition sonars in the 100 kHz to 1 GHz or higher range. While the higher frequencies give better resolution of the ocean bottom and other undersea objects, their effective range is less than 100 meters. Conversely, low-frequency active sonars (less than 1,000 Hz) can potentially detect submarines at tens of thousands of yards in proper acoustic conditions.

The disadvantage of active sonar is that the transmitting platform gives away its own presence and position. Since they do not want to

surrender their acoustic stealth, U.S. submarines therefore operate their active sonar only in very select tactical situations.

The global maritime commons differ greatly from land, where nations have very visible geographic boundaries, and long-standing protocols—codified in laws, treaties, and recognized practices—govern how countries interact with each other. Whereas almost all of the Earth's land masses are claimed by one nation or another, the vast majority of the 139.7 million square miles of its oceans are international waters and not subject to any one nation's laws or control.[10] This means that ships can sail almost anywhere without needing the permission of or being subject to restrictions or obligations imposed by any one nation.

The 1982 United Nations Convention on the Law of the Sea (UNCLOS) defines a nation's territorial sea as a belt of coastal waters extending at most 12 nautical miles from its coast. The United States has not ratified UNCLOS because of concerns about some of its provisions, but it does recognize the agreement's conventions on territorial limits and freedom of navigation as customary international law and has established similar sovereign rights in U.S. law. While territorial waters are regarded as the nation's sovereign territory, foreign ships (both military and civilian) are allowed innocent passage through them, or transit passage for straits, under specific guidelines. This sovereignty extends to the airspace and seabed.

UNCLOS also establishes an Exclusive Economic Zone (EEZ) in which a coastal state assumes jurisdiction over the exploration and exploitation of marine resources in its adjacent section of the continental shelf, taken to be a band extending 200 miles from the shore. Another important aspect of UNCLOS and international maritime law is freedom of navigation, according to which ships flying the flag of any sovereign state shall not be subject to interference by other states.

Since no one nation's laws apply to these international waters, they are governed by several multilateral treaties. The most important is the 1972 Convention on the International Regulations for Preventing Collisions at Sea, which establishes among other things the "rules of the road" or navigation rules to be followed by ships and other vessels at sea to prevent collisions between vessels. Since there are no marked traffic lanes or stoplights on the open seas, all ships must remain vigilant with respect to the course and speed of other vessels. As the USS *Fitzgerald*'s June 2017 fatal collision with a Philippine container ship demonstrates, even routine at-sea training operations are dangerous and require a minimum safe level of proficiency.[11]

In short, international maritime laws afford the U.S. Navy the ability to project power in response to crises or attempt to deter potential adversaries by sailing U.S. warships anywhere around the globe without having to obtain the permission of any other nation. In similar manner, they also afford maritime competitors the opportunity to sail their naval platforms off the U.S. coast. Visible examples of this are the recent periodic deployments of Russian submarines off the east coast of the U.S. near U.S. naval bases (e.g., Kings Bay, Georgia).

While some nations focus their navies on coastal defense against adversaries operating near their coasts and territorial waters, the U.S. Navy has taken a different approach. The Navy's maritime strategy since World War II has focused on maintaining a continuous forward naval presence that strives to deter adversaries and, if necessary, engage them in the open ocean or near their own coasts, keeping the fight and threat far from U.S. shores. At present, no other nation can conduct routine, sustained naval operations far from its home waters as does the U.S. However, some near-peer competitors like Russia could attempt to deploy small numbers of nuclear-powered submarines off the U.S. coast to launch missiles armed with conventional explosives against targets of vital importance to the U.S. In light of this threat, the U.S. Navy and U.S. Northern Command (USNORTHCOM) maintain the ability to find and target adversary undersea forces closer to the U.S. homeland.

Implications of the Maritime Domain for Naval Forces

The ocean and its unique characteristics place demands on and drive the design of a nation's navy. This is most readily apparent in the difference between a littoral or coastal defense navy and a blue-water or global open-ocean navy.

A coastal navy is focused on protecting a country's territorial waters and adjacent international waters. How far a nation's maritime area of concern extends from its coast will depend on the nation's strategic focus and the size of its navy. A coastal navy that operates within several hundred miles from the coast can consist of smaller vessels such as fast attack craft, frigates, and diesel submarines. Since they generally will operate at sea for days to weeks rather than months, they do not require the size and ability to carry large amounts of supplies, fuel, and ammunition.

Coastal waters typically are more protected from severe storms and seas; as a result, coastal naval vessels can be smaller and less robust than open-ocean warships. Also, since they operate closer to shore, these naval vessels will be less dependent on satellite communications and long-range ISR than are their blue-water counterparts, which operate thousands of miles from their military commanders. If necessary, these navies can use line-of-sight UHF or VHF communications with aircraft or other surface vessels to pass urgent communications. Smaller fast attack craft employ shorter-range (tens of miles) OTH anti-ship missiles that can receive targeting information from onboard or, in some cases, even shore-based radars. Larger frigates will operate farther from shore and can support longer-range OTH weapons that can engage adversary surface vessels at ranges in excess of 100 miles, requiring timely and accurate targeting information from other ships, aircraft, or space-based ISR.

Diesel submarines are perfectly suited to the coastal defense mission. Usually operating in a defensive posture off a strategic area of the coast or near a choke point, diesel submarines can operate at very slow speeds (five knots or less) that allow them to conserve their battery energy, which provides propulsion and electrical power while submerged. In areas where the continental shelf extends into diesel submarine patrol areas, modern diesel submarines can even bottom themselves to conserve energy even further.

A modern diesel submarine operating on its battery or Air Independent Propulsion (AIP)[12] is extremely quiet and difficult to detect by passive sonar, especially when operating in or near congested coastal waters. A modern diesel submarine armed with wake-homing torpedoes requires only a moderately proficient crew to attack an adversary's surface ship as it transits through a choke point. A coastal defense approach can be supported by land-based aircraft (fighters, maritime patrol craft, and helicopters); OTH radars; and anti-ship cruise missiles. A coastal navy also does not require a large fleet of logistics ships, because its ships and submarines can return quickly to port for fuel, supplies, and weapons.

Naval mines are extremely well suited to a coastal defense strategy whose primary mission is to keep potential adversaries out of its area of concern or far enough away that they are unable or degraded in their ability to conduct maritime strikes ashore. Naval mines are relatively cheap compared to modern precision-guided munitions, and a littoral minefield can easily be laid by small naval vessels or even by militia vessels (civilian vessels that can be used for some low-end military missions). Just one ship hitting a mine effectively shuts down a choke point or area of concern until it can be confirmed that all mines are cleared. Since the high-frequency sonars required to detect undersea mines have limited range, it can take weeks or months to survey and clear a suspected minefield. This mission gets even harder if the local adversary has surface dominance over the minefield area, thus preventing the use of mine countermeasure ships.

Since the transit time to and from coastal navy's bases to desired operating areas is relatively short (hours to days), a smaller force can maintain a specific defensive posture.

Additionally, coastal navies can surge additional forces quickly if needed and have them on station within hours. Finally, coastal defense navies can use undersea acoustic arrays in or near their territorial waters to provide early warning of adversary submarines or unmanned undersea vehicles approaching their coastlines or critical undersea infrastructure.

A blue-water or global open-ocean navy like the U.S. Navy has very different demands that drive the design of its vessels as well as the overall structure of the force. Since these warships operate thousands of miles from their nearest naval base for months at a time, they must be larger than their coastal counterparts for a variety of reasons. First, blue-water naval vessels must be large enough to withstand the worst possible storms and seas; a ship with a maximum speed of 20–30 knots may not be able to outrun a hurricane or other large storm. They must also have larger crews to support sustained 24-hour operations for months on end and perform preventive maintenance to ensure maximum operational readiness.

Since forward-deployed warships cannot count on getting supplies from a port in their forward operating areas during a time of conflict, they must be able to carry sufficient supplies (food, spare parts, etc.) to operate for several months if necessary and must carry sufficient fuel for an operating range of several thousand miles to enable transoceanic crossings without refueling. Blue-water naval vessels also require weapons magazines that are large enough for them to perform their initial warfighting missions.

These warships are usually multimission, since operational commanders must have the flexibility to respond rapidly to numerous military contingencies without waiting weeks for the warship with the "right mission capability" to arrive. While not every ship can perform every mission, having a mix of numerous multimission ships forward deployed enables these naval forces to respond to the vast majority of contingencies. Blue-water navies also require a large logistics fleet to resupply warships with food, fuel, repair parts, and ammunition while underway, thereby enabling them to remain forward deployed and on station for months on end.

The level of training required for blue-water sailors to attain the required proficiency to operate safely and effectively in the harsh open-ocean environment is significantly greater than the level needed for short-duration littoral operations. This training must include at-sea local area operations to simulate the conditions they will face on deployment to ensure that the crew is proficient in all potential missions they could be called on to perform.

An open-ocean global navy requires a much larger force structure than its coastal counterpart. The typical rule of thumb for naval force structure is that it takes a minimum of four ships of a given class to have any one of those ships deployed. This accounts for one vessel in major extended maintenance, one on deployment, one just returned from deployment, and one preparing for deployment. Since it takes weeks for a ship to transit to a forward-deployed area, the geographic combat commanders must maintain a specific minimum number of deployed ships and submarines of various classes so that they can respond immediately to a major combat operation. Even in peacetime, the strategic deterrent provided by a sufficiently large forward naval presence can cause potential adversaries to refrain from taking hostile or other undesirable actions.

Blue-water submarines also have different demands on their designs compared with their coastal counterparts. Nuclear propulsion is more advantageous for a blue-water submarine than diesel electric or an air-independent battery recharge method.

- As noted, it can take weeks to transit an ocean even at an average speed of 12–15 knots. A diesel submarine can transit at that average speed for less than one day before it must slow and come near the surface to recharge its battery. A nuclear submarine, however, can operate at its maximum speed for days or weeks without surfacing if required to transit rapidly across the globe.

- With its greater propulsion power (~40,000 shaft horsepower compared to 4,000 for a diesel boat), a nuclear submarine can be much larger (~7,800 tons submerged) than a diesel submarine (less than 2,000 tons submerged) and therefore carry more weapons and a larger crew.

- A nuclear submarine's greater available power also enables it to have sufficient atmosphere control and fresh water–producing equipment to allow lengthy submerged operations.

The key drawback of a nuclear submarine compared to a diesel submarine is the noise generated by its power plant. The reactor support equipment and steam plant are inherently much louder than a diesel submarine operating an electric motor on the battery. These systems can be made extremely quiet and more closely approach the minimal noise levels of a diesel submarine, but the engineering is much more complicated and expensive. For example, it took the Russian/Soviet Navy and now the Chinese People's Liberation Army Navy (PLAN) decades to develop the expertise to quiet their nuclear submarines so that they could not be heard tens of thousands of yards away.

Similar demands drive the design of open-ocean aircraft carriers. Most immediately noticeable is the size of a modern carrier. For an aircraft carrier to provide sufficient power-projection capability anywhere on the globe, it must be able to store, launch, and maintain a variety and large quantity of aircraft in a carrier air wing. For example, a U.S. Navy carrier air wing typically consists of 68 aircraft of six different types.[13] Steam-driven catapults to launch aircraft and an arrested landing system to enable their recovery aboard ship provide significant decreases over traditional runways, but a minimum distance is still needed for aircraft to take off and land on the carrier's deck (modern U.S. carriers are more than 1,000 feet long). The carrier must also hold sufficient aviation fuel and ordnance to support carrier flight operations for several days without resupply, and the manpower required to operate both the carrier and the carrier air wing is substantial: A typical U.S. carrier deploys with over 5,000 personnel.

All of these requirements result in a vessel that is 60,000 tons to over 100,000 tons for the *Nimitz* class.[14] The large size, need for extended periods of high speed for carrier operations, and power requirements of support equipment (especially the catapult system) make nuclear power attractive for modern carriers.

A credible blue-water or global open-ocean navy is expensive to build, train, and maintain, but it provides the capability for global power projection and enduring forward presence.

Increasing Maritime Competition and Threats

The world's oceans have never been more critical to its prosperity and security. Global maritime traffic has increased almost fourfold over the past 20 years,[15] with even more dramatic increases in the Indian Ocean and the East and South China Seas. The sea-lanes connecting Asia with North America, the Mediterranean, and Northern Europe flow through the Suez Canal and account for over 15 percent of today's global shipping traffic.[16] These global shipping lanes are extremely congested and subject to increased risk of collisions, terrorism, or piracy as they pass through critical choke points. Each year, for example, 50,000 ships transit the Strait of Malacca, averaging more than 135 per day, and the Suez Canal handles upwards of 75 ships per day.[17] World seaborne trade accounts for 80 percent of global merchandise trade, some 10 billion tons of cargo.[18]

Although global maritime piracy has decreased significantly over the past few years due to the efforts of multinational naval task forces such as Combined Task Force 151 off the east coast of Africa and actions by the commercial shipping industry, piracy remains a prevalent concern. Some areas such as the Gulf of Guinea are seeing increased activity. The threat of maritime piracy affects shipping costs by causing commercial shipping companies

to route their ships farther out into the open ocean to avoid these small pirate vessels, thus creating longer and less efficient routes; to deploy armed guards and other self-defense measures; and to transit areas of increased threat at faster speeds that burn more fuel per distance traveled.

The search for oil, gas, and mineral resources has fueled an unprecedented increase in undersea exploration. The commercial use of remotely operated vehicles (ROVs) and UUVs to explore the ocean's bottom and to inspect and maintain deep-sea oil rigs has helped drive the technological maturation and increasing capabilities of small to medium-sized UUVs. Rapidly improving UUV and ROV technology also makes it possible for a growing number of state and non-state actors to find and cut undersea cables clandestinely.

The 2006 magnitude 7.0 Taiwan earthquake severed eight submarine cables in multiple places, resulting in a severe Internet disruption in China. It took 11 special cable-laying ships 49 days to repair the damage.[19] If an adversary or natural disaster cut the majority of cables to the continental United States or even to Hawaii, where U.S. Pacific Command Headquarters is located, it would likely take months to find and repair the damage. Trillions of dollars of international financial transactions would be affected, and secure military communications would be dangerously reduced. It should be noted that of the 56 commercial cable-laying/repair ships in operation worldwide, only one is registered in the U.S., and the U.S. government owns only one cable-repair ship, the USNS *Zeus*.[20] Just how many repair ships the commercial undersea industry would dedicate to such U.S.-focused repairs is therefore uncertain at best.

The search for undersea natural resources has political and legal implications. According to the United States Geological Survey, as much as one-fifth of the planet's undiscovered petroleum reserves may reside in the Arctic: roughly 90 billion barrels of oil and 1,670 trillion cubic feet of natural gas.[21] Under international maritime law, Canada, Denmark, Norway, Russia, and the United States all have a legal claim to this valuable seafloor territory. UNCLOS allows these nations to file claims for additional territory out to 350 nautical miles if they can prove their continental shelves extend into the Arctic seabed. To date, Russia, Denmark, and Norway have submitted claims to an extended continental shelf in the Arctic, providing yet another potential source of maritime conflict.

In the South China Sea, China has staked claims to maritime territory that includes the Spratly Islands, Paracel Islands, and Scarborough Shoal. These claims overlap with the EEZ claims of Brunei, Indonesia, Malaysia, the Philippines, and Vietnam. In addition to fishing rights, potentially lucrative oil and natural gas deposits are at stake. In the past few years, the Chinese have begun island-building projects on the Subi, Mischief, and Fiery Cross reefs to advance their disputed territorial claims. While the Chinese have claimed that these islands are being built for civilian purposes, to increase safety for ships transiting the waterway, analysis of recent construction shows airfields, radars, and hardened shelters that indicate a military focus.

Key Naval Warfare Competitors and Challenges for the U.S. Navy

The rapid maturation and proliferation of certain technologies have affected the maritime environment and security challenges for the U.S. The proliferation of commercial satellites has greatly improved the ability of many nations to conduct open-ocean command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR). Space-based electro-optical and synthetic aperture radar sensors permit wide-area search for surface vessels because, unlike the land with its forests, mountains, and other masking terrain, there is nowhere to hide on the ocean's surface. Commercial satellite communications provide global communications capabilities to nations and navies that do not possess their own, as well as redundant communications for near-peer adversaries.

Forty of the world's coastal nations currently possess submarines.[22] The capabilities and proficiencies of these submarine fleets vary significantly from nation to nation, but modern export submarines and weapon systems provide even a very small navy with a credible naval threat. The vast majority of these submarines are quiet diesel submarines that operate in coastal defense missions.

Since the passive radiated noise of modern diesel submarines is extremely low when operating on the battery, resulting in exceptionally short passive sonar detection ranges of less than 2,000 yards, active sonar is the most effective means by which to search for and locate diesel submarines. Their limited speed and endurance (most can sprint at speeds in excess of 20 knots only for less than one hour) prevent them from effectively evading a searching platform using active sonar. In addition, efforts by Russia and China to quiet their nuclear submarines have reduced their passive detection ranges, making open-ocean search and localization by U.S. naval forces more difficult and requiring the use of multiple anti-submarine warfare (ASW) assets, such as the Surveillance Towed Array Sensor System (SURTASS), maritime patrol aircraft, and destroyers.

Underwater acoustic arrays have become more prevalent in the littoral areas of most of the world's continents. Although the vast majority of these arrays are for oceanographic research, submarines operating in their vicinity could possibly be detected. Modern air-based and space-based surface search radars also have the ability to detect submarines operating at periscope depth, provided one knows exactly where to look or can apply sophisticated data analysis techniques designed to detect the unique radar signature of an exposed submarine periscope or antenna mast as it interacts with a constantly changing ocean surface.

Some argue that advancing non-acoustic anti-submarine warfare (NAASW) capabilities will soon make the oceans transparent,[23] but the laws of physics and projected technologies do not support this assessment. While the probability of detecting a submarine either acoustically or by means of NAASW increases significantly for a submarine operating in the littorals off near-peer adversaries, especially at periscope depth, a submarine or other undersea platform remains comparatively much harder to detect than even the stealthiest aircraft. The undersea environment continues to provide a significant military advantage to navies that are able to operate in it effectively.

The proliferation of precision-guided munitions, especially land-based and sea-based anti-ship cruise missiles (ASCMs), and other advanced weapons technologies provides an increasing threat to U.S. naval forces, especially when operating in choke points and the littorals. Just as the flat ocean expanses make it easy to see surface ships, they also provide an unobstructed field of fire for adversaries with the ability to field ASCMs. Since ships cannot hide at sea, they must have the capability to defend against these increasingly capable weapons. Although unsuccessful, the October 2016 Houthi missile attack from land-based launchers in Yemen against the USS *Mason* while it was operating in the Red Sea clearly illustrates the reality of this threat.[24] The development of long-range (greater than 1,000-mile) anti-ship ballistic missiles presents a potential threat to carrier strike groups and other surface naval forces.

Rapidly maturing UAV technologies and their proliferation to both state and non-state actors presents another growing maritime threat. Small military and commercial micro-UAVs can easily be "weaponized," allowing them either to drop small explosives on ships or other targets or to serve as "kamikaze" UAVs. These small and slow UAVs are hard to detect with traditional air-search radars, which are focused on larger and fast-moving military aircraft and missiles. While the very small commercial UAVs have a rather limited range of less than five miles, their range and endurance are rapidly increasing, and even today, they could be launched from shore or from a nearby civilian vessel against a naval vessel transiting a choke point.

Key Nations That Affect U.S. Navy Design and Missions

Iran. The Iranian Navy is a regional navy that has been shaped by its maritime operating environment on the Arabian Gulf and the Gulf of Oman. Aided by land-based aircraft and a very capable Russian-built integrated air defense system, the Iranian fleet consists primarily of coastal patrol frigates, fast attack craft, fast inshore attack craft, and submarines. Iranian diesel submarines and mini-submarines armed with torpedoes and anti-ship missiles are ideal platforms with which to lie in wait undersea in Iranian territorial waters and hold the Strait of Hormuz at risk. The Iranian Navy has been observed employing its fast attack craft (FAC) and fast inshore attack craft (FIAC) in swarm tactics meant to overwhelm the capacity of adversary warships to target and engage incoming vessels and their anti-ship cruise missiles.

Although the Iranian Navy possesses only a few dedicated mine-laying vessels, it could employ its FAC/FIAC and other vessels to deploy the over 2,000 naval mines in its inventory.[25] Naval mines would be extremely effective in controlling the relatively narrow Strait of Hormuz, as evidenced by the damage inflicted on the USS *Samuel B. Roberts* when it struck an Iranian floating contact mine in April 1988. Although not a naval capability, Iran's ballistic missile capabilities and their potential threat to Europe have led to a ballistic missile defense (BMD) mission for specified U.S. Navy cruisers and destroyers.

Russia. The Russian Navy, like Iran's, has been shaped by its unique maritime operating environment. With much of the Barents Sea covered with ice for part of the year, providing a "bastion" for its nuclear strategic submarines, it is logical that Russia has prioritized its submarine force over a large surface blue-water navy. A resurgent Russian Navy has focused its modernization efforts on submarines and small surface combatants (frigates and corvettes). Its new *Yazen*-class nuclear guided missile submarine is assessed as being extremely quiet and capable of launching conventional or tactical nuclear long-range cruise missiles. The new *Borei*-class nuclear ballistic missile submarine demonstrates Russia's continued prioritization of a submarine strategic nuclear deterrent.

The new Russian Maritime Doctrine illustrates the Russian Navy's focus on the Arctic and Atlantic Oceans with the ultimate goal of restoring its blue-water capabilities.[26] In the Black and Baltic Seas, the Russian Navy would assist any future efforts for Russian influence and territorial expansion in Eastern Europe. The past few years have seen a dramatic increase in provocative and sometimes unsafe engagements between Russian warships and fighter aircraft and U.S. Navy warships and maritime patrol aircraft in the Mediterranean, Baltic, and Black Seas.

China. Over the past two decades, the Chinese military has focused its modernization efforts on developing capabilities to disrupt the U.S. military's power projection forces in the Western Pacific, with a focus on its carrier strike groups and C4ISR enterprise. China's emphasis on denying U.S. access to the South China Sea and East China Sea has concentrated primarily on land-based anti-ship and anti-land ballistic missiles with effective ranges out to over 1,000 miles as well as land-based fighter aircraft best suited for control of the close-in air domain. Long-range land-based OTH radars and airborne early-warning aircraft and satellites provide the necessary detection and targeting data for these long-range weapons.

The development of these long-range, land-based anti-ship capabilities has lessened China's dependence on naval platforms (destroyers, frigates, fast attack craft, and diesel submarines) to disrupt or deny U.S. naval power projection in the South China sea. The Chinese saw the advantages presented by the South China Sea's maritime environment in the context of their strategy and developed new technologies to take advantage of them: the vast capacity advantage that land-based aircraft and anti-ship weapons can provide over a forward-deployed blue-water navy with limited weapons' magazines and extended logistic tail.

Although not critical to support this area denial strategy against the U.S., the PLAN has been slowly developing blue-water naval capabilities: indigenous aircraft carriers, advanced guided missile destroyers, and quiet nuclear attack submarines to supplement its regional naval force structure. These blue-water capabilities help China to protect its growing economic interests in Africa and other maritime areas far beyond the second island chain. It remains to be seen whether China is able to develop the logistics foundation to support a truly forward-deployed naval power—logistics ships, a network of friendly forward bases, and the operational proficiency to project naval power effectively far from its homeland—or whether platforms such as its aircraft carriers are merely symbols of China's economic and military strength.

Implications for U.S. Fleet Design

Given the characteristics of the maritime domain and the evolving challenges affecting the U.S. Navy's ability to protect U.S. national security interests, the Navy must likewise evolve to remain relevant.

The Navy must be able to operate in all subsets of the maritime domain—constricted choke points and archipelagos, the littorals, the Arctic seas, the expansive open ocean, and the complex depths of the undersea world—as well as to defeat potential maritime adversaries with capabilities ranging from swarms of fast attack craft to near-peer competitors' long-range anti-ship missiles. This should drive a force structure comprised of a mix of multimission naval platforms possessing the defensive and offensive capabilities necessary to control the sea when and where necessary and to project power from the sea against any competitor that attempts to deny the U.S. access to regions, markets, and allies.

The fleet must be large enough for forward-deployed naval forces to provide an enduring, credible deterrent to potential adversaries in all critical geographic maritime regions of concern. A sufficiently large, forward-deployed force also enables the Navy to respond rapidly to emerging and unforeseen crises wherever and whenever such response is needed.

Since the U.S. Navy always prefers to play the "away game," keeping enemies as far from the U.S. as possible, there is a pressing requirement for increased magazine size on naval platforms and secure intra-theater weapons replenishment and reload capability. Conflicts in distant theaters typically do not allow time for ships to return to a regionally local port, much less the U.S., for resupply. A robust logistics and airborne tanker fleet and a resilient and secure C4ISR enterprise provide the essential foundation for global maritime operations far from land-based defenses and logistics support.

Fortunately, the Navy's senior leadership has recognized these challenges and is striving to develop new naval strategies and capabilities to maintain America's advantages in this domain. These efforts include Distributed Lethality;[27] Design for Maintaining Maritime Superiority;[28] Undersea Domain Operating Concept (UDOC);[29] and Electromagnetic Maneuver Warfare (EMW).[30]

The key to success in all of these efforts will be a commensurate commitment by the U.S. Congress to provide adequate and stable funding so that the Navy can maintain a healthy, well-trained fleet of sufficient size and capability to secure U.S. interests in the maritime domain.

Endnotes

1. John Noble Wilford, "On Crete, New Evidence of Very Ancient Mariners," *The New York Times*, February 15, 2010, http://www.nytimes.com/2010/02/16/science/16archeo.html (accessed July 30, 2017).
2. Center for International Earth Science Information Network at Columbia University (CIESIN), Socioeconomic Data and Applications Center (SEDAC), "Percentage of Total Population Living in Coastal Areas," http://sedac.ciesin.columbia.edu/es/papers/Coastal_Zone_Pop_Method.pdf (accessed July 30, 2017).
3. International Chamber of Shipping, "Key Facts," 2017, http://www.ics-shipping.org/shipping-facts/key-facts (accessed July 30, 2017).
4. Declan McCullagh, "NSA Eavesdropping: How It Might Work," *CNet Magazine*, February 7, 2006, https://www.cnet.com/news/nsa-eavesdropping-how-it-might-work/ (accessed July 30, 2017).
5. U.S. Department of Commerce, National Oceanic and Atmospheric Administration, National Ocean Service, "How Many Oceans Are There?" revised July 6, 2017, http://oceanservice.noaa.gov/facts/howmanyoceans.html (accessed July 30, 2017).
6. U.S. Department of Commerce, National Oceanic and Atmospheric Administration, National Ocean Service, "How Big Is the Atlantic Ocean?" revised June 17, 2015, https://oceanservice.noaa.gov/facts/atlantic.html (accessed July 31, 2017); U.S. Department of Commerce, National Oceanic and Atmospheric Administration, National Ocean Service, "How Big Is the Pacific Ocean?" revised July 6, 2017, https://oceanservice.noaa.gov/facts/biggestocean.html (accessed July 31, 2017).
7. The Earth's total landmass is estimated to be 149 million square kilometers, or 57.5 million square miles, less than the 60 million square miles of the Pacific Ocean. See U.S. Central Intelligence Agency, *The World Factbook 2018*, entry for "World" statistics, "Geographic Overview," https://www.cia.gov/library/publications/the-world-factbook/geos/xx.html (accessed August 6, 2017).
8. U.S. Department of Commerce, U.S. Census Bureau, "State Area Measurements and Internal Point Coordinates," https://www.census.gov/geo/reference/state-area.html (accessed August 5, 2017). The Census Bureau estimates the total landmass of the continental United States (to include the District of Columbia) to be 3.12 million square miles. The CIA estimates the Earth's surface area to be 510 million square kilometers, or 197 million square miles. See CIA, *World Factbook 2018*, "Geographic Overview."
9. *National Geographic*, "Blue Whales and Communication," Video Highlights from *Kingdom of the Blue Whale*, March 26, 2011, http://www.nationalgeographic.com.au/science/blue-whales-and-communication.aspx (accessed July 31, 2017).
10. Global Development Research Center, "The World's Oceans," https://www.gdrc.org/oceans/world-oceans.html (accessed July 28, 2017); Sea Around Us, "High Seas," 2016, http://www.seaaroundus.org/data/#/highseas (accessed August 2, 2017).
11. U.S. Navy, "Special Report: USS Fitzgerald Collision," Navy Live: The Official Blog of the U.S. Navy, June 17, 2017, http://navylive.dodlive.mil/2017/06/17/uss-fitzgerald/ (accessed July 31, 2017).
12. Edward C. Whitman, "Air Independent Propulsion: AIP Technology Creates a New Undersea Threat," *Undersea Warfare Magazine*, Vol. 4, No. 1 (Fall 2001), http://www.public.navy.mil/subfor/underseawarfaremagazine/Issues/Archives/issue_13/propulsion.htm (accessed July 31, 2017).
13. U.S. Navy, "Aircraft Carriers–CVN," *Fact File*, last updated January 31, 2017, http://www.navy.mil/navydata/fact_display.asp?cid=4200&tid=200&ct=4 (accessed August 6, 2017).
14. Ibid.
15. Becky Oskin, "Ship Traffic Increases Dramatically, to Oceans' Detriment," Live Science, November 18, 2014, https://www.livescience.com/48788-ocean-shipping-big-increase-satellites.html (accessed July 31, 2017).
16. Jean-Paul Rodrigue and Theo Notteboom, "Strategic Maritime Passages," Chapter 1, Application 2, in *The Geography of Transport Systems*, ed. Jean-Paul Rodrigue, Hofstra University, Department of Global Studies and Geography, https://people.hofstra.edu/geotrans/eng/ch1en/appl1en/ch1a2en.html (accessed July 28, 2017).
17. Ibid.
18. United Nations Conference on Trade and Development, *Review of Maritime Transport 2016*, p. 6, http://unctad.org/en/PublicationsLibrary/rmt2016_en.pdf (accessed August 6, 2017).
19. Michael Sechrist, "New Threats, Old Technology: Vulnerabilities in Undersea Communication Cable Network Management Systems," Discussion Paper, Harvard Kennedy School, Belfer Center for Science and International Affairs, February 2012, http://www.belfercenter.org/publication/new-threats-old-technology-vulnerabilities-undersea-communication-cable-network (accessed July 28, 2017); Douglas Main, "Undersea Cables Transport 99 Percent of International Data," *Newsweek*, April 2, 2015, http://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072 (accessed July 28, 2017).
20. International Cable Protection Committee, "Cableships of the World," updated May 26, 2017, https://www.iscpc.org/cableships-of-the-world/ (accessed July 28, 2017).

21. Robert Lamb, "5 Most Coveted Offshore Petroleum Reserves," How Stuff Works, September 15, 2008, http://science.howstuffworks.com/environmental/energy/5-offshore-petroleum-reserves.htm (accessed July 28, 2017).
22. Global Fire Power, "Total Submarine Strength by Country," 2017, http://www.globalfirepower.com/navy-submarines.asp (accessed July 28, 2017).
23. Sydney J. Freedberg Jr., "Transparent Sea: The Unstealthy Future of Submarines," *Breaking Defense*, January 22, 2015, http://breakingdefense.com/2015/01/transparent-sea-the-unstealthy-future-of-submarines/ (accessed July 31, 2017).
24. Hope Hodge Seck, "USS Mason Fired on a Third Time Near Yemen, CNO Says," Military.com, October 16, 2016, http://www.military.com/daily-news/2016/10/16/uss-mason-fired-on-a-third-time-near-yemen-cno-says.html (accessed July 28, 2017).
25. Sydney J. Freedberg Jr., "Sowing the Seas with Fire: The Threat of Sea Mines," *Breaking Defense*, March 30, 2015, http://breakingdefense.com/2015/03/sowing-the-sea-with-fire-how-russia-china-iran-lay-mines-and-how-to-stop-them/ (accessed July 31, 2017).
26. Sean MacCormac, "The New Russian Naval Doctrine," Center for International Maritime Security, updated November 24, 2015, http://cimsec.org/new-russian-naval-doctrine/18444 (accessed July 31, 2017).
27. U.S. Navy, Commander, Naval Surface Forces, *Surface Force Strategy: Return to Sea Control*, January 9, 2016, p. 9, http://www.navy.mil/strategic/SurfaceForceStrategy-ReturntoSeaControl.pdf (accessed July 31, 2017).
28. Admiral John M. Richardson, Chief of Naval Operations, *A Design for Maintaining Maritime Superiority*, Version 1.0, January 2016, http://www.navy.mil/cno/docs/cno_stg.pdf (accessed July 31, 2017).
29. News release, "Undersea Domain Operating Concept Approved by Chief of Naval Operations," U.S. Navy, September 9, 2013, http://www.navy.mil/submit/display.asp%3Fstory_id%3D76420 (accessed July 31, 2017).
30. See *Naval Warfare Development Command's NEXT*, Vol. 3, No. 2 (Summer/Fall 2015), issue devoted to "Advancing Electronic Maneuver Warfare," https://www.nwdc.navy.mil/NeXT%20Assets/archive/NWDC_Mag_SUMMER_FALL%202015%20APP.pdf (accessed July 31, 2017).

The Air Domain and the Challenges of Modern Air Warfare

Harry Foster

It is difficult to imagine a modern world without flight and its associated technologies. The *speed* possible in the air domain shrinks time: A modern airliner travels 25 times faster than the fastest cruise ship on the Atlantic and seven times faster than the fastest locomotive in the 1950s. Militarily, operating in the air domain provides *vantage*: the ability to see not only over the next hill, but also over the horizon. It provides *maneuverability* unencumbered by mountain ranges, roads, river crossings, or rocky shoals at sea. Although navalists frequently remind us that 70 percent of the world is covered by oceans, 100 percent of the world is covered by air. The air domain is physically linked to every other domain, thus providing *flexibility* in operations, while its *range* provides an avenue for access anywhere in the world, anytime.

Over the past century, exploitation of the air domain's speed, vantage, maneuverability, flexibility, and range changed the nature of warfare. Specifically, it:

- Created new asymmetries that broke the stalemate of trench warfare after World War I, enabling combined-arms maneuver warfare that is with us today;
- Extended the reach of fleets and shore defenses beyond the sight of observation towers or the range of naval surface fires, making control of the air a requisite for operations on the sea;
- Allowed rapid insertion and resupply of forces at great distance from supporting bases; and
- Allowed air forces to go "over not through" the front lines of opposing armies, disrupting rearward logistics, denying maneuver, and taking war directly to capitals.

Today, from a military perspective, the degree to which the United States can exploit the air domain in its favor to find and hold at risk any target (fixed, mobile, hardened, and deep inland) anywhere on the globe is a key differentiator that makes it a military superpower.

Understanding the complexity of modern air power begins with a basic understanding of the air domain itself. This means understanding the air domain's unique attributes; how one can access and use the domain while exploring the limits of height and speed for platforms that operate in it; the domain's unique attributes of speed, range, persistence, and payload that have allowed the United States to dominate conflicts for the past 25 years; and current key shifts in the domain, driven by the evolution of technology and the return of state-based competition, and their implications for future military requirements.

Attributes of the Air Domain

The Atmosphere: Home to the Air Domain. The Department of Defense defines the air domain as "the atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible."[1] At its most fundamental level, the atmosphere is composed of air, a mixture of gases consisting of 21 percent oxygen, 78 percent nitrogen, and 1 percent argon, carbon dioxide, and other gases.[2]

The composition of air is perhaps its most extraordinary and important characteristic because it determines the very nature of the domain and dictates what can and cannot be done in it and drives the characteristics of the platforms that fly through it. Because these gases have mass, the distribution of the atmosphere is not uniform. For example, due to gravitational effects, nearly 50 percent of atmospheric mass is contained below 18,000 feet at the equator, 90 percent is contained below 52,000 feet, and 99.99 percent is contained below 330,000 feet or an altitude of 100 kilometers.[3] While some international organizations such as the Fédération Aéronautique Internationale define 100 kilometers as the beginning of space, the United States does not recognize a formal boundary either by treaty or by policy.[4]

The atmosphere is divided into several layers that are of varying degrees of significance to military operations.

- The lowest level, the troposphere, varies in height from the surface to 60,000 feet at the equator to 30,000 feet over the poles. All weather occurs in the troposphere. The top of the troposphere, called the tropopause, is the "cap" where summer thunderstorms flatten out to form an anvil shape. In the troposphere, the wind blows west to east in the Northern Hemisphere and east to west in the Southern Hemisphere. Temperature decreases by about 3.5 degrees Fahrenheit with every 1,000 feet of climb. Wind speed changes significantly with altitude, averaging 75 miles per hour from the west at 35,000 feet over the central United States in winter to as much as 200 miles per hour in the strongest jet streams.

- Above the troposphere is the stratosphere, which extends to about 180,000 feet. The stratosphere is where the ozone layer is located, and it is free from clouds and weather. Wind diminishes significantly with altitude in the stratosphere. Most of today's military operations occur in the troposphere and the stratosphere.

- Above the stratosphere at an altitude of about 34 miles is a region of the atmosphere that has proven easy to transit but difficult to operate in persistently. In this region, there is enough air to cause drag and surface heating but not enough to support aerodynamic control or air-breathing engine combustion.

- Sitting above the stratosphere, extending to 260,000 feet, is the mesosphere. Here, meteors burn up due to atmospheric heating. The ionosphere, which causes high-frequency radio waves to bounce off the atmosphere enabling long-range amateur radio operations, begins in this region.

- Above the mesosphere lies the final layer of the atmosphere, the thermosphere, which extends to as much as 600 miles above the Earth depending on solar activity. Atmospheric drag caused by gases in the lower portion of this layer limits the lowest unpowered, stable satellite orbit to roughly 120 miles.

Accessing the Air Domain for Military Advantage. From its earliest days, competition in the air domain has been enabled by constantly advancing technology. Warfighting in the air domain, however, is fundamentally a human endeavor, and as one learns about airspace technologies, it is important to keep technology in perspective. Technology

enables access to and exploitation of the air domain, but humans marshal this technology to gain advantage over others as a tool of statecraft and war. Competition in the air domain therefore centers on maintaining or denying this advantage and depends not only on mastery of technology, but also on its artful and creative organization and application in strategy and tactics.

The characteristics of air and the atmosphere make five modes of access to the air domain possible: lighter-than-air flight, heavier-than-air flight, missiles, ground-fired or sea-fired projectiles, and the electromagnetic spectrum.

Lighter-than-air flight is achieved by trapping gases lighter than oxygen and nitrogen, like hydrogen or helium, or heated air in a sealed casing. Because the gas inside the casing is lighter than the surrounding air, lift is produced. The volume of air contained in that casing, coupled with the characteristics of the gas inside, determines its lifting ability. This allows exploitation of the air domain using hot-air balloons, gas-filled balloons, or powered airships (dirigibles and blimps). Lighter-than-air aircraft can provide persistence and relatively heavy lift, but this means of access is both slow and heavily affected by weather.

Lighter-than-air flight was exploited in World War I by Germany, which used dirigibles, or powered airships, to bomb central London, and in World War II by the United States, which used blimps for antisubmarine warfare patrols.[5] Although the speed of heavier-than-air platforms made them dominant over their lighter-than-air brothers, a role remains for balloons and powered airships today. Tethered balloons (aerostats) extending up to 14,000 feet line the U.S. border with Mexico and have been used in Iraq to provide persistent surveillance coverage.[6] Powered airships used by the logging industry to extract harvested timber from remote areas could provide a slow-speed, heavy-lift logistics option for military purposes.[7] High-altitude balloons also offer military utility as a backup to space-based capabilities like communications satellites.[8]

Heavier-than-air flight, on the other hand, uses aerodynamic forces to produce and sustain lift. Aerodynamic lift is produced by moving an airfoil (wing) through volume of air or fluid. Design differences between the upper and lower surfaces of the airfoil force the air to move faster across the upper surface as the wing is propelled through the air. This creates an area of lower pressure on the top of the wing that generates lift. There are other factors involved, but if one produces enough aerodynamic lift to overcome the force of gravity, then a heavier-than-air machine can fly.[9]

There are two other forces at play in the creation of aerodynamic lift: the thrust required to propel a wing though the air to generate lift and the drag that the wing creates through the process of creating lift. Thus, balancing the problems of lift, gravity, thrust, and drag makes flight possible using vehicles that are powered (airplanes, cruise missiles, helicopters, tilt rotors, and quad copters) and unpowered (towed gliders, lifting bodies, and air-delivered guided munitions). Aircraft provide a reusable form of access to the air domain and offer an incredible degree of flexibility with regard to speed, range, payload, and endurance for military operations.

Missiles use the brute force of expanding, burning gases provided by liquid-fueled or solid-fueled rocket engines to overcome the effects of gravity and gain access to the air domain. As the vehicle accelerates, it takes on aerodynamic characteristics and can be controlled using aircraft-like control surfaces until it reaches mid-stratosphere. Above this altitude, small thrusters or gimbaled engines controlled by guidance systems allow the highest levels of precision in movement and endgame placement.

Missiles deliver high-speed effects in both the air and space domains without the risk associated with manned flight, but there are trade-offs. Lift is created on the sheer power of their engines, making this form of access markedly less efficient than winged aircraft. Moreover, missiles used for attack or defense are not reusable; an aircraft can return to base and reload with ordnance, but a missile is a one-time shot.[10]

Projectiles like bullets, mortars, rockets, and bombs use a controlled explosive charge, propellant, or the momentum gained by a parent platform to overpower the aerodynamic effects of weight and drag temporarily in order to enter and transit the air domain. Aimed downward, air-launched munitions provide an additional and incredibly potent axis of fire against land-based and sea-based targets. Aimed upward, ground-fired projectiles provide a low-cost, effective way to deny an enemy use of the air domain in a limited area. For example, the vast majority of aircraft losses in Vietnam were due to anti-aircraft artillery rather than surface-to-air missile defenses.

Today, new technologies like electromagnetic rail guns can fire projectiles from land-based or sea-based platforms at hypersonic speeds to attack other surface targets or defend against low-flying, supersonic cruise missiles and high-speed ballistic missile warheads.[11] In addition, long-range, precision-guided rocket artillery teamed with unmanned intelligence, surveillance, and reconnaissance (ISR) capabilities like satellites or "drones" are changing the way armies view fires.[12]

Finally, *the electromagnetic spectrum* provides a less obvious but equally powerful method of accessing the air domain to enable, disrupt, or deny air operations. This includes use of voice and data communications to direct and employ forces; optical, infrared, laser, and radar-based sensors to detect objects in the air domain and guide weapons; high-power lasers to deny optical sensors or to attack incoming aircraft, missiles, or bombs;[13] high-powered microwaves to disrupt operation of airborne vehicles and weapons;[14] electromagnetic decoys to confuse an opponent's systems;[15] and modern jamming techniques to deny, disrupt, or spoof radars, communication, and space-based navigation systems like the Global Positioning System (GPS).

The electromagnetic spectrum can be manipulated through combinations of low-observable (stealth) technology and active electromagnetic countermeasures to increase the survivability of both aircraft and munitions against increasingly sophisticated air defenses. This electromagnetic method of accessing the air domain also enables cyberspace effects to shape every aspect of offensive and defensive air operations.

Leveraging these five methods of access, nations develop offensive and defensive capabilities to gain or deny advantage across the spectrum of warfighting domains, but the air domain is more complex than simply pitting system against system. Sanctuary or advantage can lie in operating at high or low altitude, operating at speed, operating from range versus operating forward, hiding in the noise of the electromagnetic spectrum, or increasing weapons accuracy to reduce repeated exposure to the threat.

The U.S. has taken several different investment strategies within the air domain since the 1950s. From the opening days of the jet age through the 1970s, it pursued a "higher, farther, faster" strategy. As the Soviet Union mastered its integrated air defense system (IADS), U.S. efforts moved to a low-altitude strategy that stayed in place through the opening days of Operation Desert Storm, when precision and stealth capabilities became dominant. A closer look at the limits of altitude and speed in the air domain therefore helps one to understand the constraints of the operating environment.

Defining the Air Domain's Upper Limit. Defining the upper limit of the air domain, "where its effects on operations becomes limited," is difficult. As noted, most military operations occur in the troposphere and lower stratosphere. Commercial aircraft operate up to about 40,000 feet, while military aircraft routinely operate as high as 60,000 feet. "Controlled airspace" over the United States ends at 65,000 feet. Operations above this altitude are sometimes called "near space."

The glider-like wings of the U-2 aircraft enable it to operate at the very edge of controlled flight while flying at subsonic speeds in the 70,000-foot regime.[16] Due to the thinning atmosphere, however, operations above this altitude require either increasing supersonic speeds with altitude to produce adequate lift

or, paradoxically, no speed at all. For example, the Mach 3.0 SR-71 operated near 85,000 feet,[17] while the Mach 3.0 Mig-25 holds the absolute manned takeoff to altitude record of 123,523 feet.[18] On the other hand, the highest manned balloon reached 135,890 feet,[19] and unmanned balloons have reached the top of the stratosphere at over 176,000 feet.[20]

Going higher still requires different forms of propulsion and materials. Rocket planes carried aloft by a mother ship, like the 1960s-era X-15 (transported to high altitude by a B-52 bomber) or Virgin Galactic's Spaceship One flights, operate in the mesosphere and beyond in what are known as "suborbital" operations. Spaceship One holds the altitude record for an air-launched rocket plane at 367,487 feet or 70 miles, but it does not have the ability to persist in this regime for any meaningful length of time.[21]

Achieving persistence in the flight regime above the stratosphere is technically difficult, but it can be realized through atmospheric "skipping" where platforms use their speed to "skip" off denser layers of atmosphere at hypersonic speeds like a rock skipping across water. Such a capability offers a range of military benefits between the air and space domains (roughly 34 miles to 120 miles above the Earth), making it possible to maneuver and maintain altitude without the limitations of orbital mechanics that are imposed by operations in space.[22]

A hypersonic glide vehicle (HGV), a capability being pursued by the United States, Russia, and China, can be deployed from an intermediate-range ballistic missile to enable such atmospheric skipping.[23] An alternative approach might be found in new propulsion techniques such as air-breathing, plasma-fueled engines, which are in early research and development.[24]

Defining the Speed Limit in the Air Domain. Mach numbers play a crucial role in understanding the difficulty of going higher and faster in the atmosphere. A Mach number is a speed expressed as the percentage of the speed of sound. For example, Mach .82, a typical airliner speed, is 82 percent of the speed of sound. Mach 1.0 occurs at 667 knots (nautical miles per hour) at sea level.[25] Above Mach 1.0 in the atmosphere, shock waves form on the nose and tail of an aircraft. If these shock waves reach the ground, sonic "booms" are heard and felt along the flight path as the shock waves pass by in close succession.

The basic formulation of aerodynamics that balances lift, draft, gravity, and thrust works well up to speeds of about .80 Mach or the beginning of the "trans-sonic" speed regime. Here, compressibility of air becomes a factor. Unlike water, air compresses as its velocity over a surface increases. As one goes faster, this changes the drag profile of traditional airfoils, requiring substantially more energy to sustain speed or go faster. In addition, shock waves begin to form in this flight regime that disrupt normal airflow over the airfoil.

For traditional, straight-wing airfoils, these pressures shift suddenly as one approaches the speed of sound, resulting in buffeting and loss of control. This phenomenon sets the speed limit of propeller-driven aircraft, even in a steep dive, due to drag increases and shock wave formation on the propeller blades.[26] Thus, "the sound barrier" was a significant obstacle in military aviation until it was broken in October 1947 thanks to propellerless propulsion, thin wing designs, and new control surfaces.[27]

Today, aircraft designed to go faster than .80 Mach have swept wings and other design features to reduce the effects of transonic drag. Since airliners cruise at speeds of .8 to .87 Mach, research into the transonic drag reduction, transonic airfoil optimization, and engine efficiency in the transonic regime remains important for airplane and engine companies.

Two speed regimes are relevant militarily in the air domain above Mach 1.0: supersonic (Mach 1.2–Mach 5.0) and hypersonic (Mach 5.0–Mach 10.0). Each regime poses different problems for designers.

Supersonic speed increases the range of air-to-air missiles, improves responsiveness for intercepts, expands the flight envelope for operations, and allows sustained high-altitude flight.

In the supersonic regime, designers must solve the problem of creating a subsonic airstream in the engine to support combustion despite air entering the engine at supersonic speed. To accomplish this, most military fighter aircraft utilize afterburning turbofans, which use a combination of inlet design and a spinning compressor to squeeze and slow the airflow coming into the engine to subsonic speed before injecting fuel and burning it.[28] Afterburning turbofans are far less efficient than the subsonic "high bypass" turbofans used by the airlines, although research is underway to improve their efficiency during subsonic flight.[29]

As one goes faster than about Mach 3.0, however, turbofan engines reach material limits to handle high heat and pressures. To go faster with an air-breathing engine, a ramjet is required. A ramjet uses a movable fixed inlet to achieve compression without rotating parts. Combustion still occurs in subsonic air, however. Ramjets can operate to Mach 6.0 but work best in the Mach 2.0–Mach 4.0 range. For example, a combined-cycle turbojet/ramjet engine enabled the SR-71 to reach speeds above Mach 3.0. While Mach 3.0 speed provided survivability against air defenses through the 1980s, this speed regime would become well within the capability of air defense systems like the Russian SA-20 and U.S. Patriot and Aegis by the 1990s.[30]

To improve survivability and reduce reaction time for today's most contested airspace, one must maneuver at hypersonic speeds. The cost to operate above Mach 5.0 within the atmosphere has risen at exponential rates with increasing speed due to shifts in structural material requirements to mitigate extreme heat and special requirements for air-breathing engines to handle extreme speeds.[31] Both China and the United States are actively pursuing research to reduce cost in these areas.[32]

To reduce the cost of hypersonic speed, air-breathing engines are more desirable than rocket engines because they produce more thrust for a given amount of weight. Moreover, the combination of speed and better fuel efficiency enables a hypersonic vehicle to travel longer distances on a small amount of fuel, in turn allowing for vehicles that are more compact.[33] For example, a powered hypersonic vehicle travels 560 miles on only eight minutes of fuel at Mach 7.0.

To achieve this, a scramjet engine that can sustain combustion in supersonic airflows is needed. Because these engines do not operate below Mach 4.5, a scramjet-powered hypersonic vehicle requires a rocket-motor "kick start" to accelerate to its engine start speed. Research into these engines is ongoing. In 2004, NASA's X-43 achieved 10 seconds of powered flight at Mach 9.6, the fastest jet-powered flight on record.[34] In 2013, the Air Force X-51A testbed achieved 240 seconds of hypersonic flight with a scramjet at Mach 5.1, the longest powered flight of a scramjet on record. Given the capability of improving modern air defenses and the growing importance of striking mobile targets, air-breathing hypersonic vehicles and weapons are likely to become an area of intense competition.[35]

Denominators for Exploitation of the Air Domain

Having discussed the speed and altitude attributes of the air domain, one must consider the denominators that are needed to exploit it. These break down into two major areas: being able to project power through range, persistence, and payload and being able to see and act using the electromagnetic spectrum.

Range, Persistence, and Payload. The ability of aircraft in the air domain to operate and survive at range and persist over time with intelligence, surveillance, and reconnaissance sensors and flexible weapons is key to exploiting the domain. This capability connects the air domain with other domains through missions like counterair, strike, close air support, ISR overwatch, airborne anti-submarine warfare, assault aviation, or airborne cyberspace operations. Twenty-five years after Desert Storm, the success of U.S. operations in largely permissive air environments has solidified the perception that American air power is an omnipresent force with an unblinking eye that wields a rapid, precision hammer.

TABLE 2

Effect of Distance on Sortie Production

Distance from Base (nautical miles)	Total Sortie Duration (hours)*	Sorties per Aircraft/Day**	Pilot Manning (per aircraft)***
650	4.7	~2.90	1.5
1,300	7.4	~2.00	2.0
1,950	10.1	~1.55	2.5
2,600	12.8	~1.25	3.5

* Assumes 2.0 hour on-station time.
** Assumes 1.5 hour regeneration time and 6.0 hours maintenance non-availability per day per aircraft. Times vary by aircraft, maintenance manning, and carrier deck cycles.
*** 12.0 hour sustained pilot duty day, 125 hours maximum per 30 days.
SOURCE: Author's calculations.

heritage.org

Unlike the land and sea domains, where persistence consists of holding ground or patrolling in a geographically limited area, persistence in the air is about radius of action that leverages the speed and vantage that the air domain provides. For example, an aircraft loitering at 20,000 feet that is 80 miles away from a U.S. ground patrol in Syria is within easy radio contact of the ground patrol, can immediately bring sensors to bear, and can arrive overhead at Mach 1.0 in eight minutes. Should tensions escalate, other airborne forces can mass quickly. Should fuel run low, air refueling tankers arrive to provide inflight refueling. Thus, the operation can quickly scale and protract, especially in permissive environments (areas where there is little or no threat to U.S. air operations). Range and persistence make this possible.

Range and persistence are related concepts that revolve around fuel. For example, a pilot can travel point to point at speed, translating fuel into range, or orbit around a point at speed, translating fuel into persistence. Thus, fuel on board, expressed as combat radius or the unrefueled mission radius of action, is critical to exploitation of the air domain as well as to force posture and basing. For example, the United States developed air refueling in the 1950s to allow basing of jet bombers in depth from all sides of the Soviet Union. Without air refueling, aircraft could be based only within the range of the aircraft, which was strategically disadvantageous. As air refueling capability was incorporated into fighters, the idea of assured air refueling allowed designers to trade fuel capacity (which translates to weight) for airframe maneuverability (which also translates to weight) that was needed for air-to-air combat. Thus, the combat radius of most of today's U.S. fighters is 550–650 nautical miles. As a result, operations beyond this range require refueling about every two hours.

These basic time, combat radius, and distance economics incentivized a 60-year U.S. reliance on forward basing and forward carrier stations to project power in the air domain.[36] (See Figure 2.) There were good reasons for this approach. Operating from range taxes human endurance. In 2001, for example, fighters operating from the Arab Peninsula to Afghanistan had to transit 1,200 miles each way to fly around Iran. Thus, a six-hour mission time over Afghanistan required an 11-hour sortie

that consisted of four to five air refuelings from four to five different air refueling aircraft. These air refueling aircraft transited similar distances with similar sortie durations. Thus, sustained operations from range require more pilots, more aircraft, and more fuel.

Forward basing, on the other hand, allows commanders to use aircraft and pilots multiple times per day.[37] This enables a high tempo of operations and allows persistence through multiple revisits or cycling of aircraft across the battlespace. Forward-based air refueling tankers enhance this capability for fighter/attack-sized aircraft, allowing aircraft to operate well beyond their organic combat radii and ensuring that enough fuel is always airborne and available. (See Figure 2.)

The ability to base forward also allowed the United States to divest aircraft with large payloads like the Navy's A-6 and the Air Force's fleet of bombers, since a higher number of sorties from fighter-sized aircraft at forward bases could make up the difference in payload. Recognizing this fact, China has invested in a new generation of ballistic and cruise missiles designed to hold forward bases and aircraft carriers at risk through massed, raid-style attacks designed to overwhelm active defenses.[38] In addition, China is taking other measures to increase U.S. force requirements by expanding the range of contested airspace. (See Figure 2.)

As forward bases come under increasing threat, which in turn drives increased basing distances, pressure on the air refueling force becomes extreme unless the organic combat radius of combat aircraft is increased. Protecting large air refueling tankers is difficult. Sheltering of forward-based air refueling tankers has proven unaffordable at scale thus far and was not attempted during the Cold War.[39] Left unsheltered, these aircraft are particularly susceptible to attacks using a variety of weapons, ranging from ballistic and cruise missiles to rockets and mortars to sniper rifles. In addition, the short combat radii of today's force increase the vulnerabilities of tankers in flight, since they must operate closer to the expanded threat envelopes of modern threat systems to provide adequate fuel for operations as illustrated in Figure 2.

Improved combat radius may therefore become increasingly important to exploitation of the air domain for power projection. Fortunately, the capabilities of modern missiles are rendering fighter maneuverability less important, allowing airframe weight to be traded for fuel. However, a greater emphasis is needed on larger payloads to make up for the potential loss of high-sortie production from forward bases and on unmanned operations to improve human abilities to sustain protracted operations from range.

The Electromagnetic Spectrum. In addition to projecting range, persistence, and payload, exploiting the air domain requires the capability to see, decide, and act. It is therefore difficult to separate operations in the air domain from the electromagnetic spectrum or the electromagnetic spectrum from weather. The relevant portions of the electromagnetic spectrum within the context of the air domain include visible light; infrared light, which is used for sensing temperature; and all radio frequencies, which enables communications and various forms of radar. From eyeballs to radar, if it is detected in the air domain, it is by and through the electromagnetic spectrum.

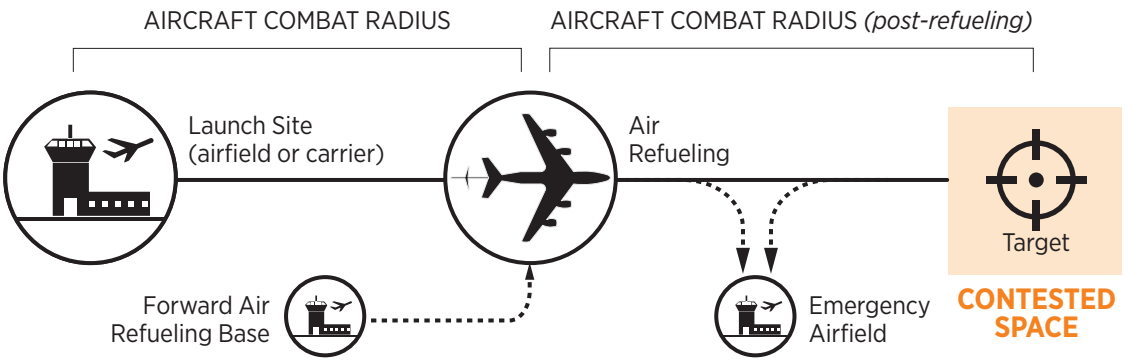
Weather, on the other hand, presents hazards like thunderstorms and severe icing, as well as wind and temperature, that affect operations. Most important, however, it shapes the degree to which the electromagnetic spectrum can be exploited. The line of sight distance to the horizon from an aircraft operating at 35,000 feet is 229 miles, but how much of this distance is usable? Looking up into the stratosphere, a great deal may be: The weather is generally clear, and the background is cold and free from clutter, perfect conditions for visible, infrared, and radar sensors.

Looking down toward the thicker atmosphere and the ground is another matter. In the visible spectrum, dust and clouds may obscure the view. For example, clouds cover most of North Korea more than 50 percent

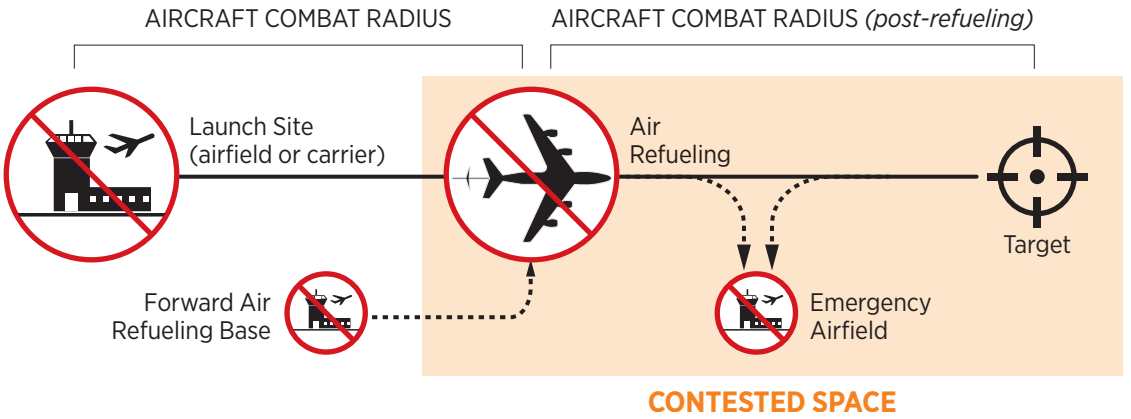
FIGURE 2

How the U.S. Projects Air Power

Historically, the U.S. has been able to project air power by using airfields, carriers, and air refueling systems to minimize the size of contested space — the area in which aircraft would engage in conflict.



China is investing in missile systems that would significantly hinder the U.S.'s forward operating launch points, which would as a result make the contested space much larger.



heritage.org

of the time from May to September. In the infrared spectrum, water vapor may attenuate temperature signatures, and clouds may block them completely. In the radar spectrum, synthetic aperture radar provides a means to see through clouds, but power dissipates rapidly with range (i.e., $1/\text{range}^4$), and rain attenuates signals at higher frequencies. In addition, airborne radars must contend with the "ground clutter" moving below them, complicating their operation.

Moreover, aircraft are limited in the amount of power they can produce and the sizes of radar antenna they can carry. Thus, antenna size tends to herd aircraft radars into a narrow range of operating frequencies and power. This means that a true all weather, day/night ISR capability requires a combination of sensors to

be effective and that aircraft may be required to fly close to an area of interest for its sensors to "see" it, especially if the target is mobile.

Meanwhile, actors accessing the electromagnetic spectrum on the ground or at sea are not limited by power or radar size as aircraft are. They can develop powerful radars to detect and target air vehicles and employ severe jamming to disrupt airborne radar and precision navigation like the Global Positioning System. In addition, ground-based radars have the advantage of looking up away from clutter. This dynamic of air-based and ground-based competition in the air domain through the electromagnetic spectrum is what eventually forced the development of stealth.

As competition between nation-states intensifies, the competition to place sensors close enough to "find" targets, especially mobile ones, versus defensive efforts to prevent these actions will continue. Stealth, enhanced by active electronic countermeasures, remains relevant and essential for survivability in this environment in order to hold mobile and deep targets at risk. Other approaches, such as hypersonic speed or employing large numbers of vehicles to saturate defenses, also enhance survivability and may become key contributors to this competition. The question then becomes: How may the character of the domain change as technology advances?

Key Shifts Likely to Affect the Air Domain

Because exploitation of the air domain depends on technology that is constantly advancing, competition in the domain has never stood still. As technology accelerates and renewed nation-state competition drives new moves to counter U.S. capabilities, at least four key shifts are underway that are likely to alter the character of the air domain.

First, exploitation of the air domain is no longer just about aircraft. The proliferation of mobile advanced air defenses, mobile ballistic missiles, land-launched and sea-launched hypersonic boost glide systems, and air-launched powered hypersonic vehicles provides new means to deny air refueling, attack forward bases, and deny forward carrier stations through the air domain. This undercuts the force posture assumptions on which the present force is built. Given this development, increased combat radius of aircraft, larger payloads, and expanded use of long-range unmanned systems improve the ability of the U.S. to operate from range.

Second, the most important targets are mobile. The increasing importance of countering the above-described mobile targets increases the importance of ISR and the ability to direct forces in contested environments. Fully leveraging the leading edge of technology in the electromagnetic spectrum improves the ability of the U.S. to hold these targets at risk. This includes technologies for advanced sensors, penetrating stealth, survivability to "stand in," and alternatives to GPS navigation.

Third, weapons in flight are under increased risk. The maturation of directed energy and improved capability of ground-based point defenses may cause traditional weapons to come under increased threat. Increasing weapon speed or employing saturation tactics with large "flocks" of weapons improves the probability of weapon arrival. Either approach requires survivability to "stand in" or penetrate, increased payloads, and greater depths of weapons magazines.

Fourth, the threat from "low end" uses of the air domain is growing. The rise of machine learning, object recognition, and improved battery technology may enable small drones or quad copters to contest the air domain at the tree level. This capability may be used to disrupt airfields and to project power locally even in permissive environments. Research into countering machine learning and new capabilities to counter emerging small, swift, and robotic capabilities improves the ability of the U.S. to adjust to this threat.

Conclusion

The ability of military forces to exploit the air domain has revolutionized warfare over the past century. Exploiting the domain to find and hold targets as risk at global ranges remains a

differentiator of U.S. power. Shifting technology, however, threatens to erode this advantage and presents challenges to the U.S. model of power projection. Sustaining that advantage will require more stealth platforms with C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) capabilities and the ability to adapt to unforeseen changes in the air domain, as well as those it supports.

Endnotes

1. U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms*, July 2017, p. 10, http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf (accessed July 26, 2017).
2. North Carolina State University, "Climate Education for K–12: Composition of the Atmosphere," last modified August 9, 2013, http://climate.ncsu.edu/edu/k12/.AtmComposition (accessed July 26, 2017).
3. U.S. Department of the Air Force, *Weather for Aircrews*, Air Force Handbook 11-203, Volume 1, March 1, 1997, p. 9, http://www.dtic.mil/dtic/tr/fulltext/u2/a423996.pdf (accessed July 26, 2017).
4. S. Sanz Fernández de Córdoba, "100km Altitude Boundary for Astronautics," Fédération Aéronautique Internationale, http://www.fai.org/icare-records/100km-altitude-boundary-for-astronautics (accessed July 21, 2017). For a summary of conventions and treaties on air and space boundaries, see Paul Stephen Dempsey, "The Definition and Delimitation of Outer Space," presentation before the U.N. Committee on the Peaceful Uses of Outer Space, Vienna, Austria, March 30, 2017, http://www.unoosa.org/documents/pdf/copuos/lsc/2017/tech-05.pdf (accessed July 26, 2017).
5. The use of an observation balloon in the Battle of Fleurus to report on Austrian movements in 1794 marked the first asymmetric use of the air domain. Countermeasures began as snipers were used in the American Civil War to contest tethered balloon surveillance.
6. See Dave Long, "CBP's Eye in the Sky," U.S. Department of Homeland Security, U.S. Customs and Border Protection, https://www.cbp.gov/frontline/frontline-november-aerostats (accessed July 26, 2017).
7. See Mike Kendrick, "A New Age of Airships Is Ready for Lift-off," *The Telegraph*, March 31, 2016, http://www.telegraph.co.uk/technology/2016/03/31/a-new-age-of-airships-is-ready-for-lift-off/ (accessed July 26, 2017).
8. See Google's Project Loon, designed to deliver Internet using high-altitude balloons, at Project Loon, "What Is Project Loon: Balloon-Powered Internet for Everyone," https://x.company/loon/ (accessed July 26, 2017).
9. For those who are interested in why this is so, see Veritasium, "Why Does a Wing Actually Work?" August 3, 2012, https://www.youtube.com/watch?v=aFO4PBolwFg (accessed July 26, 2017).
10. Rocket-powered missiles fly trajectories that are based on their purpose. Air-to-air, air-to-surface, and surface-to-air missiles and missiles designed for ballistic missile defense fly customized profiles that balance maintaining sensor coverage on the target, preserving energy, and achieving an intercept of their intended target. Surface-to-surface missiles, on the other hand, fly either ballistic or maneuvering profiles. Ballistic profiles, such as those flown by a German V2 or Iraqi SCUD missile of Operation Desert Storm fame, describe a predictable arc based on the equations of motion and may transit space at apogee or the highest point in their arc. Maneuvering profiles, on the other hand, may be employed to fly an unpredictable flight path (such as the boost glide trajectory mentioned earlier), conserve energy, enable sensor coverage for warhead guidance, or defeat defenses. Finally, space-bound missiles transiting the air domain on their way to an orbital speed of 17,000 miles per hour must not go too fast or too low in the atmosphere as side loads due to wind can exceed the vibration or structural limits of a supersonic missile. This region of "maximum dynamic pressure" usually requires rocket designers to throttle down their engines until the missile is past 40,000 feet.
11. U.S. Department of the Navy, Office of Naval Research, "Electromagnetic Railgun," https://www.onr.navy.mil/en/Media-Center/Fact-Sheets/Electromagnetic-Railgun (accessed July 29, 2017); Sam LaGrone, "Pentagon: New Rounds for Old Guns Could Change Missile Defense for Navy, Army," USNI News, updated July 19, 2016, https://news.usni.org/2016/07/18/pentagon-new-rounds-old-guns-change-paradigm-missile-defense-navy-army (accessed July 29, 2017).
12. Kyle Mizokami, "The Army Is Getting a New Long-Range Tactical Missile," *Popular Mechanics*, June 16, 2017, http://www.popularmechanics.com/military/weapons/a26960/army-new-long-range-tactical-missile-deepstrike/ (accessed June 16, 2017).
13. For an example, see Kevin McCaney, "Navy Cranks Up the Power on Laser Weapon," *Defense Systems*, June 28, 2016, https://defensesystems.com/articles/2016/06/28/navy-150-kilowatt-laser-weapon-test.aspx (accessed August 1, 2017).
14. George Seffers, "CHAMP Prepares for Future Flights," *Signal*, February 1, 2016, http://www.afcea.org/content/?q=Article-champ-prepares-future-fights (accessed August 1, 2017).
15. Joe Pappalardo, "Drones Can Now Jam Enemy Radar," *Popular Mechanics*, November 14, 2013, http://www.popularmechanics.com/flight/drones/a9772/drones-can-now-jam-enemy-radar-16157656/ (accessed June 8, 2017).
16. Fact Sheet, "U-2S/TU-2S," U.S. Air Force, September 23, 2015, http://www.af.mil/About-Us/Fact-Sheets/Display/Article/104560/u-2stu-2s/ (accessed August 1, 2017).
17. Paul R. Kucher, "Blackbird Records," SR-71 Online: An Online Aircraft Museum, last modified October 2, 2011, https://www.sr-71.org/blackbird/records.php (accessed August 1, 2017).
18. GlobalSecurity.org, "MiG-25 FOXBAT," last modified February 4, 2016, http://www.globalsecurity.org/military/world/russia/mig-25.htm (accessed August 1, 2017).

19. John Markoff, "Parachutist's Record Fall: Over 25 Miles in 15 Minutes," *The New York Times*, October 24, 2014, https://www.nytimes.com/2014/10/25/science/alan-eustace-jumps-from-stratosphere-breaking-felix-baumgartners-world-record.html (accessed July 24, 2017).
20. Lighter-Than-Air Society, "Japan Sets New Balloon Altitude Record: 53.7 kms," September 22, 2013, http://www.blimpinfo.com/uncategorized/japan-sets-new-balloon-altitude-record/ (accessed July 24, 2017).
21. Fédération Aéronautique Internationale, "FAI Record ID #9881: Altitude Above the Earth's Surface With or Without Maneuvres of the Aerospacecraft," http://www.fai.org/fai-record-file/?recordId=9881 (accessed August 1, 2017).
22. Paige Carter, "Bringing Hypersonic Flight Down to Earth," *Science and Technology Review*, January/February 2000, pp. 20–22, https://str.llnl.gov/str/pdfs/01_00.pdf (accessed June 8, 2017).
23. Bradley Perrett, Bill Sweetman, and Michael Fabey, "U.S. Navy Sees Chinese HGV as Part of Wider Threat," *Aviation Week and Space Technology*, January 27, 2014, http://aviationweek.com/awin/us-navy-sees-chinese-hgv-part-wider-threat (accessed June 8, 2017).
24. Sandrine Ceurstemont, "Plasma Jet Engines That Could Take You from the Ground to Space," *New Scientist*, May 17, 2017, https://www.newscientist.com/article/mg23431264-500-plasma-jet-engines-that-could-take-you-from-the-ground-to-space/ (accessed August 1, 2017).
25. As with the maritime domain, operations within the air domain use nautical miles per hour or "knots" to quantify speed. One nautical mile is equal to one minute of latitude, 6,076 feet, or 1.15 statute miles on a car's odometer. The true speed of sound in knots varies by altitude and pressure. Notwithstanding this, a rule of thumb in aviation is to view the Mach number with the decimal point moved one place to the right as "nautical miles per minute" along the ground, discounting the effect of headwinds or tailwinds. Thus, .82 Mach is roughly 8.2 miles per minute, which equates to 492 knots along the ground with zero wind when multiplied by 60 minutes.
26. The speed record for a turboprop aircraft in level flight is held by the TU-114 at 478 knots or .73 Mach. See Aerospaceweb.org, "Tupolev Tu-114 Rossiya," last modified March 17, 2011, http://www.aerospaceweb.org/aircraft/jetliner/tu114/ (accessed August 1, 2017). Helicopters experience a different problem related to airfoil speed, called dissymmetry of lift. Helicopter blades can experience a condition in which the blade going forward in the direction of flight produces more lift than the blade going opposite the direction of flight. This can place the helicopter out of control when operating at speed unless countermeasures are taken in design.
27. There are claims that the jet-powered ME-262 exceeded the speed of sound in dives during World War II, but experts doubt that this happened. Shock waves prevented the testing of high-speed performance in wind tunnels of the time, and high speed in dives claimed many lives during World War II and in follow-on testing. For more, see PBS, "Faster Than Sound," *NOVA*, October 14, 1997, https://www.youtube.com/watch?v=_WFBe6cDrBg (accessed August 1, 2017).
28. Air entering the intakes of a turbofan engine is slowed by inlet shape, doors, or small flaps on the engine surface. A spinning compressor then sucks in the air and squeezes it, but this compression creates significant heat and pressure. For example, in the latest production F-16s, the air is squeezed 30 times before it is burned. The combustion process increases the temperature of this high-pressure air to nearly 2,750 degrees Fahrenheit before it exits into the afterburner section. This produces about 14,000 pounds of "non-afterburning" thrust, or about 3.5 times the engine's weight. Bumping large amounts of fuel into this hot exhaust and burning it in an afterburner increases thrust to nearly 32,000 pounds—more than seven times the engine's weight. Engines like this deliver tremendous performance across a wide operating envelope, enabling aircraft like the F-16 to fly at supersonic speeds from the surface to 50,000 feet. See General Electric, "F110-GE-129 Turbofan Engines," https://www.geaviation.com/sites/default/files/datasheet-F110-GE-129.pdf (accessed July 24, 2017).
29. As demand for greater range increases, the Air Force Research Laboratory is exploring a "three stream" afterburning turbofan engine that shares some attributes with high-bypass engines for use during subsonic flight and then reverts to a less efficient mode for supersonic flight. This could improve engine fuel efficiency by up to 25 percent, translating to greater range. See Bill Carey, "GE, Pratt & Whitney Win Contracts for Next-Generation Engine," *AINonline*, July 1, 2016, http://www.ainonline.com/aviation-news/defense/2016-07-01/ge-pratt-whitney-win-contracts-next-generation-engine (accessed August 1, 2017).
30. Jesus Diaz, "The Secret Engine Technology That Made the SR-71 the Fastest Plane Ever," SPLOID, December 21, 2014, http://sploid.gizmodo.com/the-secret-engine-technology-that-made-the-sr-71-the-fa-1673510951 (accessed July 29, 2017).
31. Above Mach 3.0, surface heating of the air vehicle becomes an issue, so different materials are needed in the hypersonic regime. Traditionally, titanium has been the metal of choice for handling high temperatures in aviation because it is strong and about half the weight of stainless steel. For example, an SR-71's titanium skin reached 500 degrees Fahrenheit during high-speed flight at Mach 3.0. The material limit of titanium, however, is 800 degrees Fahrenheit. See George Tzong, Richard Jacobs, and Salvatore Liguore, *Air Vehicle Integration and Technology Research (AVIATR), Task Order 0015: Predictive Capability for Hypersonic Structural Response and Life Prediction: Phase 1–Identification of Knowledge Gaps, Volume 1–Nonproprietary Version*, Air Force Research Laboratory, Air Vehicles Directorate, Wright-Patterson Air Force Base, Final Report, September 2010, p. 72, www.dtic.mil/get-tr-doc/pdf?AD=ADA535837 (accessed August 1, 2017).

32. Bill Gertz, "China Successfully Tests Hypersonic Missile," *The Washington Free Beacon*, April 27, 2016, http://freebeacon.com/national-security/china-successfully-tests-hypersonic-missile/ (accessed July 21, 2017).
33. This comparison of weight to thrust is called specific impulse. For a comparison of engine performance, see Dora E. Musielak, Aerospace Engineering Consulting, "Propulsion Comparison," in "Fundamentals of Pulse Detonation Engine (PDE) and Related Propulsion Technology," p. 10, https://info.aiaa.org/tac/PEG/HSABPTC/Public%20Documents/Dora%20Musielak%20Publications/Fundamentals%20of%20PDE%20Propulsion_Musielak.pdf (accessed August 1, 2017).
34. Fact Sheet, "Past Projects: X-43A Hypersonic Flight Program," ed. Yvonne Gibbs, National Aeronautics and Space Administration, last updated May 10, 2017, https://www.nasa.gov/centers/dryden/history/pastprojects/HyperX/index.html (accessed July 29, 2017).
35. Kris Osborn, "The World's New Leader in Super Deadly Hypersonic Weapons: China?" *The National Interest*, February 14, 2017, http://nationalinterest.org/blog/the-buzz/the-worlds-leader-super-deadly-hypersonic-weapons-china-19437 (accessed July 24, 2017).
36. Since Vietnam, most air bases and carrier stations have been within 750 nautical miles of the adversary's capital.
37. Single-place aircraft sustained duty day is 12 hours. Multi-place aircraft sustained duty day is 16 hours. The U.S. Air Force limits pilot flying time to 56 hours per seven consecutive days, 130 hours per 30 consecutive days, and 330 hours per 90 consecutive days.
38. Similarly, though to a lesser extent, Russia has improved its existing stock of sea-launched and air-launched cruise missiles and has developed a pair of new intermediate-range cruise and ballistic missiles in violation of the Intermediate Nuclear Forces Treaty. Moreover, both Russia and China are going to some lengths to demonstrate their respective capabilities, with Russia launching long-range cruise missile attacks across Iraq and into Syria in 2016 and China conducting frequent attacks against scale mockups of U.S. facilities on its ballistic missile ranges in the Gobi Desert. See Michaela Dodge, "Russian Intermediate-Range Nuclear Forces: What They Mean for the United States," Heritage Foundation *Backgrounder* No. 3028, July 30, 2015, http://www.heritage.org/europe/report/russian-intermediate-range-nuclear-forces-what-they-mean-the-united-states. For images of these ranges, see Thomas Shugart, "Has China Been Practicing Preemptive Attacks on U.S. Bases?" War on the Rocks, February 6, 2017, https://warontherocks.com/2017/02/has-china-been-practicing-preemptive-missile-strikes-against-u-s-bases/ (accessed July 28, 2017).
39. Congress appropriated $128 million for a single hardened air refueling hanger on Guam in the National Defense Authorization Act for Fiscal Year 2014, Public Law 113–66. This is about one-half the $246 million sticker price of a new KC-46. During the Cold War, tankers were based away from forward areas, and no attempt was made to shelter them. The increased range of the threat, the distances of the Pacific, and the operational requirements of the F-35 are key differences today. See Alan J. Vick, *Air Base Attacks and Defensive Counters: Historical Lessons and Future Challenges* (Santa Monica, CA: RAND, 2015), http://www.rand.org/content/dam/rand/pubs/research_reports/RR900/RR968/RAND_RR968.pdf (accessed July 29, 2017).

Space 201: Thinking About the Space Domain

Dean Cheng

Over the past three decades, the role of outer space in military operations has risen steadily. From the inception of the space age, America's activities in space have included a large national security component. The development of satellites was not only a matter of national prestige in the ideological competition of the Cold War, but also an effort to monitor military and other developments from the strategic high ground of space. Many of the earliest satellites were engaged in the gathering of intelligence.

Due to their sensitive nature and the advanced technologies associated with them, information derived from reconnaissance satellites (sometimes termed national technical means, or NTM) has generally remained highly classified. Rumors have long abounded regarding the capabilities of American reconnaissance satellites, for example, but little of their actual resolution (what they were able to see on the surface of the planet) was revealed during the Cold War. The end of the Cold War and the subsequent use of satellite imagery in 1991 during the first Gulf War pulled back many of the curtains that had obscured the capabilities and nature of reconnaissance satellites as programs were declassified and images were disseminated more broadly.

Space-based capabilities have also evolved from being oriented primarily toward meeting national security requirements to increasingly being part of global commerce. Where as information from satellites used to be closely held, anyone can now purchase overhead imagery through companies like Digital Globe and Skybox. Similarly, whereas satellite position, navigation, and timing (PNT) used to be employed primarily by military forces to improve weapons accuracy, it is now incorporated as standard equipment in many private cars, and the timing function is employed in myriad activities from precision agriculture to reconciling financial transactions.

It is important to recognize that this massive expansion of the role of space is a relatively recent phenomenon. The space age itself is only a half-century old, having begun on October 4, 1957, with the launch of Sputnik by the USSR.[1] Moreover, because space activities and space-derived information have long been closely held secrets, their full potential for military and civilian applications has yet to be explored. Though information from space systems has been employed in the wars of the past quarter-century, no nations have yet engaged in combat in space. Both the political and technical ramifications of such a conflict are still largely theoretical.

Key Characteristics of Space

Given the growing importance of space in security affairs, it is important to recognize certain key characteristics of the outer space domain.

Characteristic #1: Space is beyond Earth. The outer space region is generally

considered to begin somewhere between 100 kilometers (62 miles) and 100 miles above the surface of the Earth and extends from there. At 100 kilometers, aerodynamic forces have minimal impact on reentry vehicles; at 100 miles, the atmosphere is no longer a meaningful presence. While "space" theoretically encompasses the entire vastness of the cosmos, the militarily significant region of space is that bounded by the Earth–Moon area, as well as certain other locations governed by the Earth–Moon relationship. The latter include the Lagrange points, the five points where the gravitational pulls of the Earth, Moon, and Sun balance each other, thus making it possible for an object placed at one of these points to remain there indefinitely with minimal expenditure of fuel.

Because space is literally beyond the Earth, it is not affected by terrestrial borders as is the case with airspace. Whereas the airspace (physical space within the atmosphere above the boundaries of a nation) is considered the equivalent of sovereign territory, the same does not apply once one enters outer space. Instead, spacecraft of all nations are allowed to transit freely overhead and have no obligation to curtail their activities in doing so. (Realistically, such activities as satellite communications and weather forecasting would be virtually impossible if there were a patchwork of sovereignty governing outer space as there is on Earth.) Ironically, this principle of "open skies" was established when the Soviet Union orbited its Sputnik spacecraft. The Soviets argued that Sputnik did not pass over countries; instead, countries rotated underneath the spacecraft.[2]

Because it is beyond Earth, outer space is also not affected by considerations of terrain. There are no features in space (at least within the Earth–Moon system) that provide concealment or otherwise can mask spacecraft operations. Therefore, there is no real ability for spacecraft to hide.

Counterintuitively, this set of considerations actually makes space situational awareness (SSA) a very complicated affair. Because there is no place for satellites to hide, all orbiting objects can be seen, given a suitable suite of sensors. At the same time, however, this means that one must track several tens of thousands of objects in space, ranging from operational and defunct satellites to spent upper stages of rockets, loose nuts and bolts, and other debris from past space missions. Today, the United States Air Force officially keeps track of over 23,000 objects, which is by no means the totality of objects currently orbiting the Earth.[3] To do so, it makes over 400,000 observations (determining where various objects are located) daily.[4]

Undertaking SSA is essential in part because space objects may be mistaken for missiles; in order to prevent false alarms and possible inadvertent escalation, it is vital to track at least the larger objects in orbit so that we can know what is normally in orbit and therefore what new object might warrant closer scrutiny. Almost as important, tracking current objects in space and determining their orbits is critical to preventing collisions between satellites, preventing collisions between orbiting objects and spacecraft that are being launched, and determining whether space objects' orbits are decaying to the point that those objects may reenter the Earth's atmosphere.

To maintain SSA, the United States (like other nations) employs a variety of means. A vital tool is a network of radars. Some are conventional radars, which can track individual targets. Others are large phased-array radars, which can track multiple objects simultaneously and maintain surveillance over large volumes of space. In addition, there are many telescopes that allow imaging of satellites, which in turn allows analysts to determine the likely functions of a given satellite more precisely. All of these are ground-based systems.

Since 2014, the United States has also deployed a series of satellites that allow it to examine satellites from orbit. The Geosynchronous Space Situational Awareness Program (GSSAP) comprises a number of satellites deployed in geosynchronous orbit.[5] These carry electro-optical sensors that provide analysts with up-close pictures of objects in orbit.

Characteristic #2: Space is a hostile environment. The reaches of outer space are some of the most difficult environments in which machines or people operate. Because spacecraft are operating under near-vacuum conditions, gases that are trapped in the material of a spacecraft may be emitted in a process known as outgassing. These gases, in turn, can condense on the surfaces of a spacecraft, damaging components, clouding lenses and sensors, or otherwise adversely affecting the spacecraft.

Because spacecraft operate beyond the protection of Earth's atmosphere, they are exposed to a variety of forms of radiation, including cosmic rays, solar radiation, and even radiation belts that encircle the Earth (for example, the Van Allen radiation belts). Prolonged exposure to ultraviolet radiation can alter the properties of various materials. Spacecraft are also subjected to wild variations in temperature in ranges of hundreds of degrees. This, in turn, can lead to expansion and contraction of materials and even to cold-welding of parts.

Finally, in addition to being potentially vulnerable to collision with other satellites and any objects in orbit, spacecraft may be hit by micrometeoroids.[6] Everything in space is moving at very high speeds. Space debris, for example, typically moves at about 10 kilometers per second on average, which translates to roughly 22,000 mph.[7] Even grains of sand traveling at such speeds can have an abrasive effect, and larger objects can damage solar panels and instrument packages.

In order to operate in such a hostile environment, spacecraft must be manufactured to very high tolerances. Many are practically hand-made, which makes them very expensive. A commercial communications satellite costs at least $200 million.[8] Military communications satellites such as the Wideband Global Satcom satellite cost upwards of $400 million each.[9] Dedicated reconnaissance satellites (spy satellites) can cost over $1 billion. Reportedly, the overall cost for four new U.S. GOES-R weather satellites will be $11 billion.[10]

The steady increase in the cost of satellites is reflected in the American Global Positioning System (GPS) constellation. When fielding of GPS began in the 1990s, each satellite cost approximately $43 million, and launch costs were about $55 million. In 2013, it was reported that the newest GPS III satellites would cost $500 million each and $300 million per launch.[11]

Given the expense, few states can afford to develop, launch, and operate satellites, much less maintain reserve satellites, either in orbit or on the ground. A satellite that is lost due to a malfunction, collision, or other problems therefore cannot be replaced easily. There will likely be gaps in service or coverage until a replacement satellite can be built and launched. Augmenting a constellation is also not something that can be done either easily or inexpensively.

For these reasons, it is in the interest of satellite operators to have satellites last as long as possible. A satellite will typically carry enough fuel to enable orbital maneuvers. These range from station-keeping in order to stay in the proper orbital track and location to altering the orbit in order to avoid collisions. Activities that adversely affect the life span of a satellite (such as extensive maneuvering) are not undertaken lightly. In particular, changing a satellite's orbital plane (angle relative to the Earth's equator) is very expensive in terms of fuel and is usually avoided.

Characteristic #3: Space is difficult to reach. Not only does it take time to build a satellite; it also takes time and a great deal of infrastructure and related expense to launch it. Various capabilities are necessary to place an object into orbit. One must have a satellite and a launch vehicle. That vehicle is launched from some kind of facility that has a launch pad, a mission-control facility, and surveillance equipment with which to monitor and control the launch. There is usually an assembly or mating facility for placing the satellite payload on the rocket. Finally, other tracking sites are necessary to ensure that the payload has reached the proper orbit, has separated from the launching rocket, and is functioning properly after it has entered orbit.

All of these elements combine to make space operations expensive.[12] Until quite

recently, only major countries could afford space operations, but private companies have entered the market.

The differences among these major space launch providers are the result of a number of factors, the most important of which is reliability of launch. This is no small affair when satellite payloads cost hundreds of millions or even billions of dollars. ULA has perhaps the longest track record of successful launches. SpaceX, a competing private venture, is the newest entrant and therefore does not yet have an established track record, making its reliability more of an unknown.

Types of Orbits[13]

While there is no terrain in space, there are orbital bands that are loosely defined by their altitude above the Earth's surface. There is no clear demarcation among them, but space experts in general talk about three main orbital bands.

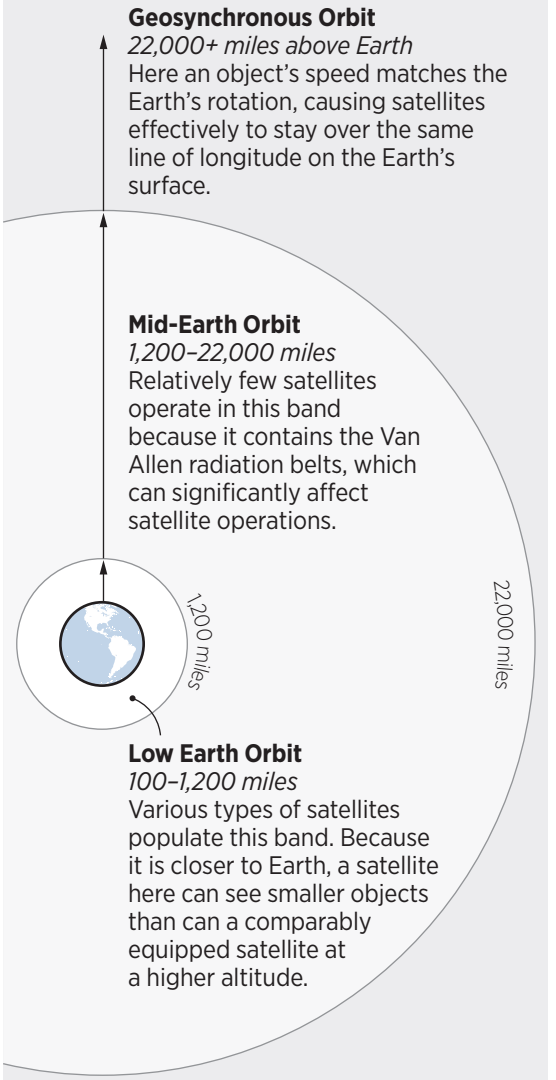
Low Earth Orbit (LEO). This is the part of outer space that begins at about 100 miles above the Earth and extends to 1,200 miles. A variety of satellites populate this band, including various types of reconnaissance and Earth observation satellites, some weather satellites, and various scientific satellites. Because it is closer to Earth, a satellite in LEO can see smaller objects than a comparably equipped satellite at a higher altitude can.

However, satellites in LEO have a more limited field of view. They are essentially viewing a ribbon of the Earth's surface as they orbit around the planet.[14] The closer to Earth, the narrower the ribbon, much as a flashlight's area of illumination shrinks or expands the closer to or farther away it gets from the spot at which it is pointed. Moreover, because of orbital mechanics, an object in LEO cannot hover over a given point unless it uses an enormous amount of fuel to stay in position. Therefore, satellites in this orbital band cannot maintain surveillance over any particular point on Earth. Instead, any individual satellite will pass over a given spot every few hours. Multiple satellites in a constellation can keep a given spot on Earth under constant surveillance—but at the cost of fielding multiple satellites.

Objects in LEO also have a more limited life span. Though they are operating above the bulk of Earth's atmosphere, they nonetheless are still operating within its upper reaches. This imposes atmospheric drag so that their orbit drops (or decays) over time. At 150 km altitude,

FIGURE 3

Types of Earth Orbits



SOURCE: Heritage Foundation research.

heritage.org

a satellite begins to lose altitude within a day; at 400 km, it could remain in orbit for a year before its orbit began to decay appreciably.[15]

Medium Earth Orbit (MEO). This region stretches from 1,200 miles to 22,000 miles above the Earth's surface. Relatively few satellites operate in this band, partly because it also contains the Van Allen radiation belts, which can affect satellite operations significantly. Within this band, however, is an area where a satellite will revolve around the Earth in 12 hours, going over the same spot twice every day. Satellites orbiting at approximately 12,800 miles above the Earth's surface are said to be in semi-synchronous orbit.

Most of the satellites that operate in semi-synchronous orbits are involved with positioning, navigation, and timing. These include the American GPS satellites and their Russian GLONASS, European Galileo, and Chinese Beidou/Compass counterparts.

Geosynchronous Orbit (GEO). The geosynchronous belt is at approximately 22,000 miles above the Earth's surface. At that altitude, an object in orbit is traveling at a speed that matches the Earth's rotation. Consequently, a satellite will effectively stay over the same line of longitude on the Earth's surface, although it may drift north or south in terms of its footprint on Earth. If a satellite is located at the GEO belt at the Earth's equator, however, it will stay over the same location on the ground and is said to be geostationary.

Theoretically, satellites in a geostationary orbit can keep constant watch over one-third of the Earth's surface. Consequently, this orbital band is considered extremely valuable; GEO slots above the equator are occupied by weather satellites, communications satellites, and missile early warning satellites.

In addition to these three orbital bands, there are several other types of orbits that are militarily useful.

Polar and Sun-Synchronous Orbits. Some satellites are launched into low Earth orbits that are at a very high inclination relative to the Earth's equator, essentially traveling from pole to pole. Polar orbiting satellites will typically see the same spot on Earth twice a day, once in daylight and once at night. A particular type of polar orbit is the sun-synchronous orbit. A satellite in such an orbit will always pass over the same spot on Earth at the same time. If it takes images while passing overhead, the fact that the images are taken at the same time every day facilitates the identification of any changes that may have occurred on the ground in the interval between images.

Lagrange Points. At the five Lagrange points, the Earth, Moon, and Sun's gravitational pulls cancel out each other. As a result, an object located at these points will remain in the same location relative to the Earth even as the Earth–Moon system and the satellite itself revolve around the Sun.

Molniya Orbits. Satellites operating in geosynchronous orbit over the equator stay over the same spot, but their ability to view the extreme northern and southern latitudes is very limited. Russian scientists therefore developed the Molniya orbit, where satellites orbit as high as 24,000 miles at their apogee or highest point while dipping as low as 500 miles above the Earth's surface at their lowest point.

Because the Molniya orbit also has a period of 12 hours, the high-altitude portion of the orbit will occur over the same area of Earth twice each day. Moreover, due to the momentum of the satellite, most of the time when it is moving more slowly will be near the top of its orbit. For most satellites in a Molniya orbit, the top of the orbit will be in the Northern Hemisphere, maximizing the opportunity to observe areas of interest in the high northern latitudes.

Major Satellite Missions

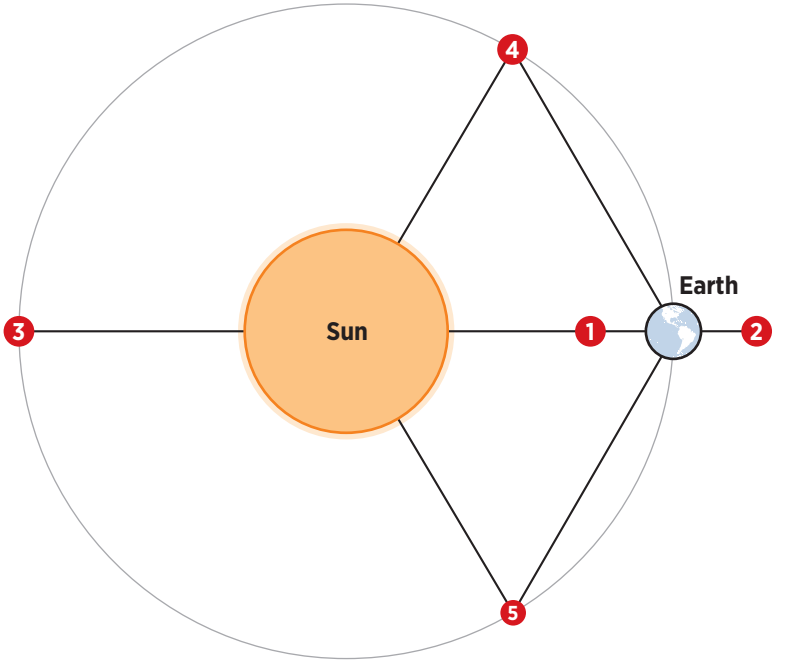
According to the United Nations Office for Outer Space Affairs (UNOOSA), more than 7,600 registered objects (a subset of the more than 23,000 that are tracked) are currently in orbit around the Earth.[16] Of these, only about 1,460 are operational satellites.[17] These satellites are engaged in a number of mission areas.

Intelligence, Surveillance, and Reconnaissance (ISR) Satellites. Satellites tasked

FIGURE 4

Lagrange Points

Lagrange Points are five locations where the gravitational pulls from the Earth, Moon, and Sun cancel each other out. As a result, an object located at any of these points will remain in the same location relative to the Earth, even as the Earth-Moon system and the satellite itself revolve around the Sun.



SOURCE: Heritage Foundation research.

heritage.org

with monitoring developments in other countries have been a mainstay of space capabilities since the dawn of the space age. Both the United States and the Soviet Union sought to develop spy satellites capable of seeing into the other side's hinterlands. These satellites were initially equipped with cameras that dropped film, but those cameras were later replaced with systems that could beam their images back directly to Earth-based stations. Electro-optical satellites are unable to see through fog and clouds, so some satellites carry radars to overcome the effects of obscuring by clouds; these can often produce very high resolution images.

Imaging satellites of various sorts have been supplemented by satellites that can monitor various types of activities in the electromagnetic spectrum. Some listen to radio traffic, collecting communications intelligence (COMINT). Others are able to detect and record electronic signals, collecting electronic intelligence (ELINT). COMINT and ELINT together are referred to as signals intelligence (SIGINT). SIGINT satellites can provide insight into the types of equipment (such as radars) being deployed by countries of interest, with the information collected revealing the wavelengths the equipment houses and what types of units (such as anti-aircraft batteries and anti-ship missile forces) are being deployed.

Most ISR satellites operate in LEO.

Earth Observation and Weather Satellites. Not all information collection is necessarily focused on other countries' military and political forces and behavior. Understanding the local environment can also be important.

Earth observation satellites such as the Landsat series have been collecting information about the land and seas for decades. The resulting data are invaluable for creating maps, as well as for understanding, for example, land use and seasonal changes in ground cover like tree foliage and grasses. For both ISR and Earth observation, data from space sensors are combined with information gathered from aircraft and terrestrial sources to give a comprehensive, layered understanding of any spot or vertical column above the ground on the planet.

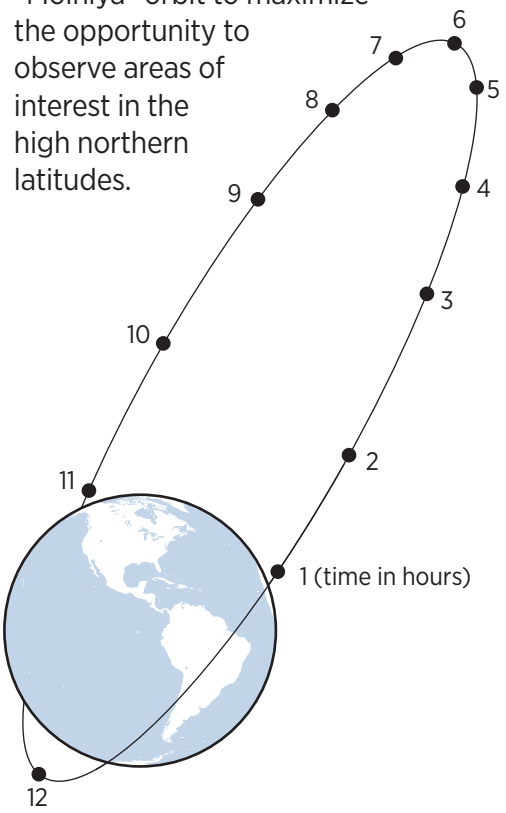
Of particular security importance among the Earth observation satellites are weather

FIGURE 5

Molniya Orbit

500–24,000 miles above Earth's surface

Russian scientists developed the "Molniya" orbit to maximize the opportunity to observe areas of interest in the high northern latitudes.



SOURCE: Heritage Foundation research.

heritage.org

satellites. The ability to forecast weather accurately can have a decisive impact on military operations. Amphibious operations, for example, can be badly disrupted by storms. Similarly, the ability to undertake air operations, whether launched from an aircraft carrier or from a land base, is affected by inclement weather conditions. Aircraft launched from an airbase in the United States may have to fly to a destination thousands of miles away. Knowing weather conditions along the route is essential to safe and effective operations, whether they involve military or civilian aircraft. The better one's understanding of weather information is, the lower the risk that one has to accept to carry out a mission.

Possessing better awareness of weather conditions than is possessed by one's opponent can confer important operational advantages. This was the case in June 1944 when Allied meteorologists, unlike their German counterparts, identified an impending lull in storms that were battering the English Channel. Consequently, the Allies landed on the beaches of Normandy on June 6, while the German high command presumed that storms made such an invasion impossible.

Most Earth observation satellites operate in LEO. Some weather satellites operate in LEO, and others are deployed in GEO.

Communications Satellites. One of the earliest commercial types of satellites was the communications satellite (comsat). Because radio, television, and other communications signals travel in straight lines, their ability to connect users on the ground is often limited by the horizon. Comsats essentially serve as relays for the transmission of these signals; a transmitter sends a signal to the communications satellite in orbit, which then transfers the signal to a ground station that may be well beyond the horizon of the original transmitter. Theoretically, a constellation of three comsats at GEO would be sufficient to provide global coverage. In reality, the availability of transponders (which are the actual relays) limits the ability of any given satellite to provide coverage.

Modern communications satellites are an important link in the movement of voice communications, television signals, and data (including Internet traffic). With the growing popularity of satellite television and its potential for entertainment and distance learning, there is a growing demand for comsat services. In addition, communications satellites are a key enabler for military drone operations. From bases

in the United States, operators can fly drones halfway around the world only because they are able to access comsats that bounce their instruction signals to their drones and relay information gathered by drone aircraft back to controlling or intelligence-processing stations.

Many of the world's communications satellites are run by private companies. Some of the world's largest constellations, for example, are now privately owned by companies such as Intelsat (55 satellites in 2014); Eutelsat (34); and the Canadian company Telesat (10).[18]

Many communications satellites are operated at GEO. However, the Iridium constellation that provides global satellite phone service is largely in LEO. Because of the smaller footprint for satellites operating at that altitude, more are needed to provide global coverage; the Iridium constellation comprises some 66 satellites.

Position, Navigation, and Timing Satellites. Beginning in the 1980s, the United States started to deploy satellites to provide position, navigation, and timing information.

- *Position* provides information about one's location and orientation: "Where am I?"
- *Navigation* provides information linking one's location to a desired destination: "How do I reach my intended location?"
- *Timing* provides precise, accurate time information.[19]

The position and navigation functions are outgrowths of the timing element. Timing functions on the GPS constellation are possible due to the highly accurate atomic clocks that are integrated into each satellite.

Each PNT satellite provides a unique signal indicating which satellite it is and what its orbital parameters are. A receiver (for example, a Garmin receiver in a vehicle) decodes the signal from at least three and usually four satellites to determine its distance from each satellite. This is done by comparing the time stamp signal from each satellite (provided by the onboard atomic clock) with the signals from the others in order to triangulate one's location. The result provides information in three dimensions with accuracy down to a few feet if one is using a cell phone's GPS function to a few inches with dedicated equipment. This is why a navigation application on a phone, in one's car, or aboard a ship far out at sea is able to work.

Because the PNT signal can be reached worldwide and all the clocks in a given constellation are keyed to the same system, the timing function has assumed a growing importance. American military frequency-hopping radios, for example, use the timing signal from GPS to time their jumps from frequency to frequency.

The U.S., Chinese, and European PNT constellations are in MEO, although China's system also includes a component that is based in GEO.

Tracking, Telemetry, and Control

In order to ensure that the various satellites are operating properly, a satellite operator needs a tracking, telemetry, and control (TT&C) network. This network enables the operator to control the satellite's functions.

- *Tracking* refers to the ability to locate a satellite and monitor its orbital condition and situation. This includes the satellite's distance and velocity.
- *Telemetry* is comprised of messages from the satellite that provide the operator with information about how well the satellite is operating. It is typically broken down into information about each of the satellite's subsystems. Telemetry data are distinct from payload data (the missions that the satellite is performing). The former is about the ability of the satellite to perform its mission.
- *Control* refers to the ability of the operator to adjust the satellite's operations. This might involve reorienting onboard instruments such as cameras or the entire satellite (for example, to point the spacecraft's solar panels toward the Sun). It might

involve moving the satellite to a different orbit or requests for more telemetry data.

TT&C networks often include stations in foreign countries and may also incorporate dedicated space support ships.

Space and Future Conflicts

Modern warfare is marked by the centrality of information. The ability to conduct joint air, land, and sea operations rests in part on the ability to create a common situational picture. Modern warfare requires the coordination of forces often separated by vast distances: for example, aerial tankers from one airbase, strategic bombers from another, and carrier air wings operating hundreds of miles from the front lines, along with infantry and armored forces. These forces must be able to communicate among themselves, identifying the location not only of the adversary, but also of one's own forces. All of this relies heavily on the ability to access the strategic high ground of space.

For the United States, this dependence is especially acute because American forces typically operate in an expeditionary mode, far from our own shores. By contrast, an Iran, a China, a North Korea, even a Russia is usually operating far closer to its home territory. Consequently, these states can employ a variety of non-space means, ranging from manned and unmanned aerial vehicles to radar networks, and even human observers on land and sea to provide a constant stream of information. Similarly, they have a range of communications options such as microwave, cell phones, and various types of radio systems to link their forces together—options often not available to U.S. forces because of the distances involved when deploying from home to far-flung theaters of operation.

This asymmetric dependence means that adversaries are incentivized to deny the United States easy access to space, which will affect their own operations far less than those of the U.S. armed forces. Conversely, the United States will have to maintain access to space-based systems for a variety of functions if it is to operate as it has operated in various conflicts since the end of the Cold War.

Counter-space operations, however, will not necessarily be anti-satellite systems shooting down satellites, although a number of nations have tested anti-satellite capabilities in recent years. Because space operations depend on ground-based facilities to control the satellites and obtain data from them, there is a significant terrestrial component to space operations. Similarly, both the systems that control satellites and the data that flow over satellite networks are vulnerable to cyber attacks and data manipulation. A hacked satellite that turns off its camera at key moments is as neutralized as a functioning satellite that is intercepted and destroyed by a co-orbital or ground-based anti-satellite system.

In future conflicts, both the outer space and information space domains will be central battlefields, and operations there will have as much impact as traditional activities in the air, on land, and at sea have had.

Endnotes

1. U.S. Central Intelligence Agency, "The Dawn of the Space Age," *News & Information*, updated February 5, 2013, https://www.cia.gov/news-information/featured-story-archive/2007-featured-story-archive/the-dawn-of-the-space-age.html (accessed May 26, 2017).
2. Philip W. Quigg, "Open Skies and Open Space," *Foreign Affairs*, Vol. 37, No. 1 (October 1958), pp. 95–106, https://www.foreignaffairs.com/articles/space/1958-10-01/open-skies-and-open-space (accessed May 26, 2017).
3. U.S. Strategic Command, "USSTRATCOM Space Control and Space Surveillance," October 17, 2016, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/976414/usstratcom-space-control-and-space-surveillance/ (accessed May 26, 2017).
4. European Space Agency, "Space Debris by the Numbers," information correct as of January 2017, http://www.esa.int/Our_Activities/Operations/Space_Debris/Space_debris_by_the_numbers (accessed June 5, 2017).
5. See "Types of Orbits," p. 70.
6. By the European Space Agency's accounting, there are approximately 750,000 man-made objects between 1cm and 10cm in length orbiting the Earth and over 160 million between 1 mm and 1cm in size, all traveling at extraordinary speeds and able to cause varying amounts of damage to functioning satellites. European Space Agency, "Space Debris by the Numbers."
7. Miria M. Finckenor and Kim K. DeGroh, *A Researcher's Guide to: Space Environmental Effects*, National Aeronautics and Space Administration *International Space Station Researcher's Guide Series*, NP-2015-03-015-JSC, p. 15, https://www.nasa.gov/sites/default/files/files/NP-2015-03-015-JSC_Space_Environment-ISS-Mini-Book-2015-508.pdf (accessed June 5, 2017).
8. Tariq Malik, "Launchpad Explosion Destroys SpaceX Falcon 9 Rocket, Satellite in Florida," Space.com, September 1, 2016, http://www.space.com/33929-spacex-falcon-9-rocket-explodes-on-launch-pad.html (accessed June 5, 2017).
9. Irene Klotz, "New US Military Communications Satellite to Launch Saturday," Space.com, March 17, 2017, http://www.space.com/36100-wgs-9-military-communications-satellite-launches-saturday.html (accessed May 26, 2017).
10. Eric Berger, "America's New, Super Expensive Weather Satellite Launches Saturday," *Ars Technica*, November 18, 2016, https://arstechnica.com/science/2016/11/americas-new-super-expensive-weather-satellite-launches-saturday/ (accessed June 5, 2017).
11. George Leopold, "DARPA Seeks to Bring Satellite Costs Back Down to Earth," Defense Systems, December 13, 2013, https://defensesystems.com/articles/2013/12/13/darpa-space-access.aspx (accessed May 26, 2017).
12. Rich Smith, "How Much Does It Cost to Launch a Satellite?" *The Motley Fool*, June 24, 2016, https://www.fool.com/investing/2016/06/24/how-much-does-it-cost-to-launch-a-satellite.aspx (accessed May 26, 2017).
13. Information in this section is drawn from National Aeronautics and Space Administration, Earth Observatory, "Three Classes of Orbit," https://earthobservatory.nasa.gov/Features/OrbitsCatalog/page2.php (accessed June 5, 2017).
14. James E. Oberg, *Space Power Theory* (Colorado Springs: U.S. Air Force Academy, 1999), p. 39, http://www.au.af.mil/au/awc/space/books/oberg/ (accessed June 5, 2017).
15. Ibid.
16. United Nations, Office of Outer Space Affairs, "Online Index of Objects Launched Into Outer Space," http://www.unoosa.org/oosa/osoindex/search-ng.jspx?lf_id (accessed June 5, 2017).
17. Union of Concerned Scientists, "UCS Satellite Database," November 15, 1974–December 31, 2016, http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.WTWkRk0kv_8 (accessed June 5, 2017).
18. Peter B. de Selding, "The List: 2014 Top Fixed Satellite Service Operators," *Space News*, July 13, 2015, http://spacenews.com/the-list-2014-top-fixed-satellite-service-operators/ (accessed June 5, 2017).
19. U.S. Department of Transportation, "Positioning, Navigation and Timing (PNT) & Spectrum Management," https://www.rita.dot.gov/pnt/about (accessed June 5, 2017).

National Defense and the Cyber Domain

G. Alexander Crowther, PhD

What is "cyberspace," and how does it relate to military affairs? "Cyberspace" is a term that is constantly used but seldom well defined. Its characteristics are poorly understood in the larger public discussion, especially with regard to national security and military matters. This is unfortunate because "cyber" has become profoundly central to nearly everything the military does in defense of U.S. national security interests.

As a domain through which actions can be taken instantaneously, globally, and even anonymously, cyberspace provides opportunities and challenges to countries, groups, and individuals unlike those presented by any other domain or capability. Cyberspace provides someone with the ability to attack anywhere, at any time, with a keystroke. There is no need to deploy a physical force, gain physical access to a region (otherwise done by ship, plane, or overland movement), or be encumbered by mounds of equipment and supplies. An attacker acts in absolute silence, perhaps visible only to the most skilled cyber defender. There is no need to limit one's force to specific ages, physical conditions, or body size, nor is there a need for sprawling bases, expensive facilities (like ports or airfields), square miles of training areas, extensive stockpiles of munitions, or assured access to fuel.

Cyber is generally not affected by environmental concerns or weather conditions. To the extent that cyber operations can be fully automated, they can be undertaken relentlessly, without regard for time, periods of rest, or any other constraint related to the normal use of people and equipment. In short, cyberspace provides a virtually unconstrained sphere through which nearly anyone can act against almost any target without concern for the physical impediments and resources that accompany physical actions.

A wide variety of actors operate in cyberspace. The government of the United States has a variety of responsibilities to the American public, but precisely where the responsibility lies and the extent of that responsibility are currently subjects of debate. Although 90 percent of the Internet traffic in the U.S. is in the private sector,[1] cyberspace is one place for which the U.S. government has acknowledged responsibility. Working mainly through the Department of Defense (DOD), Department of Homeland Security (DHS), and Department of Justice (DOJ):

> The United States will work to promote an **open, interoperable, secure, and reliable** information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation. To achieve that goal, [the U.S.] will build and sustain an environment in which **norms of responsible behavior** guide states' actions, sustain partnerships, and support the rule of law in cyberspace.[2]

Cyberspace

Cyberspace has three layers: the physical network, the logical network, and the cyber persona.

- **The physical network** consists of the hardware, such as cables and your computer, and exists all around the world. Because it exists inside states, states have sovereignty over its components, and they must obey the laws of the states in which they reside.

- **The logical network** is the software that operates the network as well as its manifestations, such as a web page. These electrons that make up the logical network bounce around the globe, following the quickest route from one place to another, and route through hardware that is physically located in states. Some states, such as China and Russia, believe that they have sovereignty over this aspect of the cyber domain as well.

- **The cyber persona** is made up of the people who are operating in cyberspace. Like the physical network, they are present within states and subject to their laws and policies.

Colloquially, these three components are known as hardware, software, and wetware.[3]

The cyber domain has effectively penetrated the world's advanced economies and is making headway in the rest of the world. Many places in Africa, for instance, have skipped over the land line and gone straight to smart phones; currently, approximately 3.74 billion people are connected to the Internet.[4]

This connectivity provides a number of opportunities and challenges. It enables actions by both states and individuals across all of the elements of national power: diplomacy, information, the military, and the economy. It makes diplomatic activity more effective, for example, linking embassies and capitals with almost instant communications and allowing for better research. In addition, the opportunities that cyberspace provides for information are almost unlimited. Humankind creates huge amounts of information annually, and individuals and organizations are constantly digitizing old information, making it available to everyone.

Militarily, cyberspace allows for global command and control of forces and operations and the functioning of a globally distributed logistics system without which modern military operations would be impossible. Intelligence communities, commanders, and warfighters alike benefit from the uninterrupted flow of information. Economically, cyberspace has led to a global boom, from the technology giants Google and Amazon to the individual fisherman in India who can now determine where to obtain the best price for his catch.

In short, with its low barrier to entry, cyberspace has provided advantages across the globe and across the elements of national power. And these advantages grow as access to cyberspace spreads.

At the same time, cyberspace creates challenges. Wikileaks has revealed to the world stolen U.S. diplomatic communications, embarrassing the United States, irritating friends, and empowering enemies. Information is harder and harder to secure and easier and easier to steal. Economically, cyberspace has enabled criminals: Cyber crime cost the U.S. $100 billion and the global economy $400 billion in 2015, and the total is projected to reach $2 trillion by 2019.[5] For the U.S. military, compromise of the U.S. global command and control capability can be turned against the Department of Defense, frustrating or even preventing the execution of military operations.

Vulnerabilities and Actors

The U.S. has begun to confront challenges to its major interests in cyberspace: protection and enhancement of the economy, secure command and control of national defense assets, reliable collection of cyber intelligence, and protection of cyber intelligence and information.[6]

Three major groups threaten U.S. national security: people, states, and non-state actors. People include the general population, leaders, workers in nearly all business sectors, and insider threats. States primarily include Russia,

China, Iran, and North Korea. Non-state actors include proxies, hacktivists, and criminals who sometimes work for themselves but also may work in support of others.

The Human Dimension. Humans are the weakest link in the cybersecurity system.[7] Unlike the physical world, in which potential human activity is limited by geographic and space limitations—Israel, for example, uses a barrier to keep out potential terrorists, and people do not own nuclear weapons or aircraft carriers—barriers to entry for cyber are so low that they have democratized cyber activity. Everyone who has a desktop, laptop, or smart phone is an actor and a potential problem. Because the only thing that organizations do well is what their leaders demand of them, leaders can be a key vulnerability, and thus a "threat" to their organizations, by not emphasizing cybersecurity. Workers using poor cyber hygiene are a threat. Gullible people or people with preconceived but flawed notions of safe cyber practices will fall prey to cyber crime or propaganda. Insiders who do not support their organizations are another threat.

The Population. People are the most vulnerable to cyber operations. Because many people engage in commercial transactions online and use social media daily, they are the most exposed to these varied threats. In general, people usually have not received training or education that would enable them to deal with varied cyber threats. Additionally, most people do not see their information as having value.

Leaders. Research supporting the 2014 Chairman of the Joint Chiefs of Staff war game *Iron Crucible* identified "understanding" as the major challenge in the 21st century.[8] Because most senior leaders typically are not involved in the information business, there is a wide variation in their knowledge of or insistence on best practices in the cyber domain.

The U.S. Office of Personnel Management (OPM) hacks of 2015 are a telling example of poor leadership in this area. Although OPM's Assistant Inspector General for Audits indicated that security shortfalls were well known, having been publicly acknowledged since 2007, the OPM Director did not make cybersecurity a priority. By the time the hacks were identified in 2015, nearly a quarter of OPM's information technology (IT) systems, including several of their most critical and sensitive applications, were operating without a valid cyber-certificate authorization.[9] If the Director had understood the implications of basic security shortfalls, perhaps the theft of sensitive personal information on over 22 million Americans could have been prevented.[10]

Senior officials are often the targets of cyber-attacks because they have access to more information, IT bends the rules for them, and the damage and financial payoff for the attacker can be much bigger.[11] Hence, senior leaders need more training and education to understand how to operate their systems, how to lead and manage cyber systems and workers, and how to decrease their own vulnerability. Senior leaders also need to integrate information activities into their day-to-day operations, whether it is in a business, government, or the military. Only when senior leaders understand the implications of cyberspace will they be able to address vulnerabilities and achieve synergies that cyberspace provides.

Workers. In a phishing quiz, 80 percent of participants misidentified at least one phishing e-mail.[12] Workers are a favorite target because the chance of success goes up when more people are targeted. Roughly 20 percent of trained workers will click on a phishing link[13] even if they have been trained not to do so.

Insider Threats. These involve a variety of motivations and are very difficult to identify ahead of time. Edward Snowden and Bradley Manning are well-known cases in the U.S. The Computer Emergency Response Team (CERT) Insider Threat Center at Carnegie Mellon University maintains a database of more than 1,000 insider threat cases and provides analysis and support to organizations working to prevent insider threats.[14] Another type of insider threat is the "Lone Wolf" or "Wolf Pack." These are individuals or groups that have been radicalized, typically through cognition-shaping cyber operations.

State Threats. Included in this category are threats posed by Russia, China, Iran, and North Korea. States can leverage enormous funding, the ability to organize, and the ability to coordinate actions (multi-domain and multi-tool) at levels far above that of an individual or small group. These state actors challenge the U.S. economy with brazen cyber espionage into critical U.S. companies.

In 2014, for example, a grand jury in the Western District of Pennsylvania indicted five officers from the Chinese People's Liberation Army for cyber espionage in support of state-owned enterprises (SOEs).[15] An array of cyber actors also has challenged the ability of the U.S. to secure its command and control of national security networks reliably and to secure its sensitive and personal information data. In 2015, Russians hacked the Joint Staff,[16] and the OPM discovered a Chinese hack of tens of millions of files containing sensitive personal data.[17] Additionally, the Russians have returned to their Cold War practices of aggressive information operations seeking to undermine developed countries[18] as well as international organizations.[19]

Iran and North Korea are second-tier threats for the United States, and both countries are continuously performing cyber operations against economic and government targets in the U.S. In 2016, the DOJ indicted seven Iranian hackers for operating against a dam and banks in the U.S.,[20] and North Korean hackers have been involved in stealing both money and military designs.[21]

Non-State Actors. This category includes threats from proxies, hacktivists, and criminals. Proxies work on behalf of a government that seeks cyber effects without paying a political price, hoping to achieve plausible deniability by outsourcing such work to individuals. The Russians often use criminals as proxies,[22] and the Chinese use other groups that may or may not be affiliated with each other or other similar criminal entities.

Hacktivists will perform a wide range of operations. Much like the difference between terrorists and freedom fighters, hacktivists attack you while patriots attack people you don't like. Ironically, some groups like Anonymous will attack anyone with whom they disagree, regardless of the target's politics.

Criminals operate across the world. As noted, it is estimated that cyber crime cost the U.S. $100 billion and the global economy $400 billion in 2015 and that the total will rise to $2 trillion by 2019.[23]

All of these actors are aided by the fact that it is very difficult to attribute cyber operations to a specific actor. Cyber actors take very specific steps to prevent attribution, typically by manipulating data to pretend to be someone else. This is one of the largest barriers to cybersecurity as it is difficult to deter an actor whose identity you can't prove.

Nature of Competition in Cyberspace

Competition in cyberspace is fierce and ongoing. States seek to undermine the global order to their own advantage. Individual actors and organizations seek to advance their own political agendas. Criminals seek to make illegal financial gains from cyberspace.

All of these can be inimical to the goals of the United States and its allies and partners. Russia seeks to use cyber-enabled information operations to sow discord inside and among the states that are trying to keep Russia at bay in Europe; China uses cyberspace to steal secrets that it can use for economic gain or to avoid the research and development costs (in time and money) for important military systems; Iran seeks to weaken its opponents around the world; and North Korea maneuvers in cyberspace to avoid international sanctions.

Because of the low barrier to entry into cyberspace and the potential gains to be made, the scale of the challenge is large and growing. The U.S. and its allies and partners need to safeguard their own government spaces, their economic activities, and their citizens. Although the U.S. has strengths including a wide variety of resources and a large, educated workforce, these bad actors use cyberspace to challenge the U.S. at every turn. The U.S. is having a hard

time using traditional strengths (such as military power) against cyber actors.

The U.S. Government in Cyber

Because the U.S. government has a wide variety of resources and the obligation to safeguard the American population, the executive branch performs many cyber activities to mitigate the foregoing threats. The three main U.S. government actors in cyberspace, as noted, are the Departments of Homeland Security, Justice, and Defense.

- **The DHS** coordinates the national protection against, prevention and mitigation of, and recovery from cyber incidents; disseminates domestic cyber threat and vulnerability analysis; protects critical infrastructure; secures federal civilian systems (the .gov domain); and investigates cyber crimes under its jurisdiction.

- **The DOJ** investigates, attributes, disrupts, and prosecutes cyber crimes; is the lead agency for domestic national security operations; conducts domestic collection, analysis, and dissemination of cyber threat intelligence; supports the national protection against, prevention and mitigation of, and recovery from cyber incidents; and coordinates cyber threat investigations.

- **The DOD** is charged with securing the nation's freedom of action in cyberspace and helping to mitigate risks to national security resulting from America's growing dependence on cyberspace. Specific mission sets include directing, securing, and defending DOD Information Network (DODIN) operations (including the .mil domain); maintaining freedom of maneuver in cyberspace; executing full-spectrum military cyberspace operations; providing shared situational awareness of cyberspace operations, including indications and warning; and providing support to civil authorities and international partners.[24]

Deterrence. Ongoing cyber operations against the United States demonstrate that the country has extremely limited capability to deter cyber operations, that the U.S. cyber deterrence threat is not credible, and that U. S. cyber deterrence is failing.[25]

Deterrence is designed to convince others not to perform certain tasks. In this case, it ideally should prevent other actors from performing all four types of cyber operations. One thing that can make cyber deterrence less effective, as noted, is the difficulty involved in attributing an operation to a specific actor. Additionally, second-order and third-order analysis to predict what ancillary actions would follow certain types of cyber-attacks is very difficult to perform in the cyber realm. Incorrect analysis could cause a deterrence operation to trigger a completely opposite reaction and accidentally escalate rather than deter, which causes second thoughts on allowing offensive cyber operations.[26]

The use of cyber capabilities to deter faces two major barriers: For deterrence to work, opponents must believe that they will pay a price for an action, and the target audience needs to understand who is deterring them. This in turn requires a credible threat. Opponents do not currently believe that they will face retaliation in response to their attacks on U.S. assets. Effective cyber retaliation requires that operators perform an attack and leave behind digital "fingerprints" identifying the originator or an explicit message naming the origin of the attack.

But this presents two further problems: Cyber operators do not want to compromise their capabilities by performing an operation that can be traced to them, and it has been difficult to receive clearance to perform offensive cyber operations (OCOs). Any OCO that has major effects can alert an opponent to the presence of intruders, which allows opponents to defend against the intrusion. It can also reveal cyber capabilities, which is anathema to the community that prizes its ability to work in secret. Moreover, it sometimes takes months to penetrate opposition cyber systems. Executing an

attack will announce the operator's presence and "waste" the time required to penetrate and repenetrate target servers.

The Military Cyber Domain

The DOD does not define "domain," but it does define cyberspace as "[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[27] The words "infrastructures and resident data" cover the physical and logical aspects of cyberspace but not the persona aspect. The use of "domain" is meant to indicate that cyberspace is now coequal with the other conventional domains: sea, air, land, and space.[28] This is intended to communicate to leaders within the DOD that they need to pay as much attention to cyber issues as they would pay to air, sea, land, and space issues.

There are four sets of cyberspace activities that pertain to the military: intelligence, information, crime, and military operations.[29] Although the military has equities in all of these areas, it predominates only in the military operations portion. However, there are aspects of intelligence, information, and criminal activities in cyberspace that do involve the military.

In any of these fields, there is a spectrum of activity that ranges from conventional to cyber-enabled to cyber-centric to pure cyber operations.

Normal intelligence operations like stealing secrets and developing sources would have been the traditional approach before the advent of cyberspace. Cyber-enabled intelligence operations would use cyber capabilities in support of these operations, such as analysis of a terrorist network using data that had been gathered by traditional intelligence means. Cyber intelligence operations would be operations that occur entirely in cyberspace, such as the 2012 operation by Chinese hackers that penetrated Indian Navy computers and compromised sensitive information.[30] Purely cyber operations would consist of information and communications technology, network, and defensive cyber operations.

Conventional criminal operations would be old-school crime, such as entering a bank with a pistol and a bag. Cyber-enabled criminal operations would fuse technology and crime, such as ATM-skimming, where criminals use hidden electronics to steal the personal information stored on bank ATM cards and record PIN numbers in order to access victims' accounts.[31] Cyber crime would be a criminal operation that occurs wholly in cyberspace, such as the use of the SWIFT system to steal $81 million from the Bank of Bangladesh.[32]

Conventional information operations would be old-fashioned propaganda or even advertising via printed text, radio waves, or television. The 2016 hack of the Democratic National Committee would be an example of a cyber-enabled information operation.[33] The information was obtained through cyber operations but released through Wikileaks.[34] Cyber information operations would include Daesh recruiting videos, an information operation that takes place entirely in cyberspace.

Military operations can also be cyber-enabled or executed purely in cyberspace. A normal military operation would be the invasion of Iraq. A normal special operation would be the raid to kill Osama bin Laden. An example of a cyber-enabled conventional military operation would be Russian operations in Georgia in 2008 when Russia conducted cyber operations against Georgian targets to degrade Georgian command and control in support of Russian conventional military operations on the ground and in the air.[35] An example of a cyber-enabled special operation would be the Mumbai attack of 2008. Planners used a GoPro camera while walking the route to be used in the attack so everyone could see videos of their routes before the operation. They also used Google Earth during their planning process. The command element monitored Indian social media and traditional media (such as radio and television) to track the response by Indian security forces and steered the ground

force away from reacting Indian forces, enabling the operation to continue much longer than it would have normally.[36]

Cyber military operations include conventional and special operations. A conventional cyber operation would be like "dropping cyber bombs on Daesh." Secretary of Defense Ashton Carter explained at an event at NORTHCOM that "[w]e're using these tools to deny the ability of ISIL leadership to command and finance their forces and control their populations; to identify and locate ISIL cyber actors; and to undermine the ability of ISIL recruiters to inspire or direct Homegrown Violent Extremists."[37] This is a conventional operation in that it does not require special techniques or unique modes of employment in a covert nature.

A cyber special operation would be the Stuxnet attacks on Iran. This operation meets many of the criteria for a special operation as defined in the DOD's Joint Publication 3-05, *Special Operations*.[38] It required unique modes of employment, tactics, techniques, procedures, and equipment. It was conducted in a hostile, denied, or politically and/or diplomatically sensitive environment and was characterized by a clandestine or covert nature (no one has yet proved who conducted the operation) and low visibility.

Criminal operations do not usually pertain to militaries in the conventional sense. In cyberspace, however, there are crimes that involve members of the DOD, as well as crimes that involve the Defense Industrial Base. Additionally, members of the DOD participate in several types of activities that pertain to cyber crime and cyber-enabled crime, including cyber security and critical infrastructure protection, law enforcement and counterintelligence, document and media exploitation, and counterterrorism.[39]

Each of these provides examples of how the military would be involved in four areas: crime, intelligence, information operations, and military operations. Although military forces are involved in these areas, they are not involved in all operations in these areas (the DOJ handles most cyber crime). This, then, is the circumscribed area that can be called the military cyber domain. These distinct categories are changing and becoming more integrated with cyber activities. As cyber capabilities expand, more military operations will be enabled by them; eventually all military operations will be enabled by cyber capabilities.

Military Cyber Operations

There are four main types of cyber operations: shaping cognition; cyber surveillance and reconnaissance (CSR); operational preparation of the environment (OPE); and cyberspace attacks. They can be either defensive or offensive in nature. Defensive cyber operations (DCOs) comprise the vast majority of U.S. government (and military) activities. Offensive cyber operations (OCOs) are rarer for the United States. None of these activities is unique to cyberspace. All military operations require reconnaissance and preparation, and shaping cognition through information (for example, through advertising) is ubiquitous in modern society.

Opponents perform shaping-cognition intelligence operations against the United States on a minute-by-minute basis and perform OPE regularly. Large-scale, destructive cyberspace attacks are rare but have the potential to be catastrophic in their effects.

Shaping cognition is using information to cause people to think in a certain way. This can be benign like Facebook or malign like cyber crime. It is perhaps the most significant opportunity and challenge for cyber today. Due to the pervasive nature of information in the 21st century, everyone who connects to the Internet can shape the thoughts of others. Radicalization by state and non-state actors is a significant challenge, especially lone-wolf or wolf-pack radicalization. The Islamic State has successful influence operations running globally 24 hours a day. The fact that volunteers have been to ISIS territory from around the world indicates how successful these operations are. Other actors target populations of other countries (to radicalize); government

employees (to create an insider threat); and businesses (to coerce or blackmail them into behavior that the initiator desires). Governments consequently struggle to cope with widespread cognition shaping.

CSR is data gathering. Google gathers data every time one accesses the Internet. States gather data on people in other countries or on their own citizens. States such as China gather economic data and pass it on to their state-owned enterprises who use it to obtain a competitive advantage in the marketplace. Criminals gather data to better execute their criminal activities. Today, everyone is a data-gatherer.

OPE is specific preparation of the environment for follow-on operations by installing "back doors" in targeted computer systems so that they can return at a later time to execute an attack or devising specially designed software that will allow them to achieve an effect, such as opening the gates on a dam. Among recent examples, as noted, are the seven Iranians who were indicted for hacking into banks and a dam in New York.[40]

OCOs are a means by which to achieve an end, another tool that provides additional capabilities to the President and battlefield commanders and relevant forces.

Cyber operations are limited only by the imagination and capability of the attackers, yet there are only two types of cyber-attacks: syntactic and semantic.[41] Syntactic operations involve the actual coding used in a piece of cyber programming (the syntax of the coding), and semantic operations seek to shape thoughts using language or semantics. As an example, a phishing operation begins as a semantic operation, asking the target to "click on this link," and then, once the link is activated, changes to a syntactic attack by which the malicious code enters the target's system and changes the syntax of the code in the targeted platform. Shaping the thoughts of others may be the more important of these two types of attack.

A cyberspace attack produces two forms of effect: manipulation and denial. Manipulation means controlling or changing the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives. Denial attempts to degrade, disrupt, or destroy. Degrading limits the capacity of a target, and disruption completely but temporarily prevents access to a target.[42] Destruction eliminates the target altogether.

Cyber operations are changing the characteristics of warfare. Although the nature of war is constant, the characteristics of warfare can change whenever a new weapon or tactical approach is introduced. Operations in cyberspace now allow for more information to be acquired and shared and better command and control to be exercised on the battlefield, theoretically decreasing the "fog of war" by adding fidelity to the commander's understanding of the battlespace. It allows for more accurate and effective use of the people and logistics capabilities involved, putting the right person or widget at the right place at the right time. It also allows for a significant improvement in the ability to shape cognition.

While it allows all of these to assist friendly forces, however, it also allows our opponents to do the same. They will have a better understanding of—and consequently an opportunity to copy or defeat—our technologies and capabilities. They will be able to access our command and control and logistics networks, potentially modifying orders so that forces or spare parts end up in the wrong place. They also will be able to use patterns in the movement of information to improve their own intelligence, identifying our units and their capabilities.

These capabilities require the U.S. government generally, as well as the U.S. military specifically, to modify its practices. Leaders and organizations need to do a better job of selecting and utilizing new technology. Laws and policies need to be updated to leverage the new technology. Older leaders need to understand how younger followers perceive and use technology.

Implications for Operations. Cyberspace permeates all aspects of our daily lives and therefore all operations whether military,

governmental, or commercial. Cyber operations, including information operations, will require attention from leaders from the tactical level to the strategic level.

At the tactical or local level, cyber operations will provide information to the warfighter that previously did not exist or was available only to national-level leaders. Soldiers will carry smart phones, which will require command attention and supervision to prevent the unintentional compromise of militarily relevant information. Units will have access to huge amounts of information, including the position of every friendly vehicle, soldier, airframe, and ship as well as any enemy forces that have been identified. This information will make our forces much more effective and efficient if properly utilized.

At the same time, our opponents will use their similar capabilities as effectively as they can to accomplish their own objectives in keeping with their own integrated information warfare doctrine. It will be difficult for U.S., allied, and partner units to control their own information while exploiting their opponent's information. Units will have to perform DCOs at all levels. Failing to do so will likely result in operational paralysis when their command and control assets are degraded or destroyed. They also will have access to limited OCOs if their particular mission warrants access to that level of support.

Automation and information flows will make day-to-day operations easier. However, while attention to sound DCOs and skillful execution of OCOs will lead to military success, failure in each case will present exploitable opportunities to an enemy.

Implications for the Services. As occurred when airplanes, tanks, and automatic weapons were introduced to war, forces will need to reorganize to integrate robust cyber and particularly information capabilities. Specifically, the services will have to:

- **Modify** training and equipping to ensure that units practice DCO at all times and will have to stand up additional OCO capabilities as their use becomes more widespread.

- Because cyber operations happen at nearly instantaneous speed and in a wide variety of locations simultaneously, **modify** their doctrine to allow for greater authority to execute cyber operations at much lower and more local levels in order for units to continue to function when command and control are degraded and operate effectively at the speed of information.

- **Purchase** more modern information technology equipment and software, which are inherently more secure.

- **Provide** universal, entertaining, iterative cyber hygiene training to the entire force. Properly equipped and trained units will be able to be much more effective and efficient in information-age combat. According to the Australian Signals Directorate, 85 percent of cyber problems can be mitigated with proper cyber hygiene.[43] This will be expensive in the short term, but once it is fully integrated into the force, it will act as a force multiplier.

U.S. Military Cyber

The Office of the Secretary of Defense articulates three primary cyber missions: "**defend DoD networks, systems, and information**; **defend the nation against cyberattacks of significant consequence**; and **support military operational and contingency plans**."[44]

Because the DOD is a very large, bureaucratic organization that operates around the world, it is proving difficult for it to fully embrace cyberspace operations. First, there are DOD legacy structures. Services such as the Army provide trained and equipped forces, while Combatant Commands (CCMDs) like U.S. European Command (EUCOM) and U.S. Pacific Command (PACOM) use those forces for missions. This means that the DOD, the largest organization in the world, must

simultaneously defend every military system that is linked in any way to or affected by "cyber" used by DOD, the Joint Staff, the three military departments, and four services that collectively employ almost 3 million people, more than 450,000 of whom work overseas, both afloat and ashore.

The department's responsibilities also include several hundred thousand individual buildings and structures located at more than 5,000 different locations or sites worldwide.[45] Each person in the DOD needs to communicate and pass information on a daily basis. Many have multiple computers and devices that they operate on different networks. All of this must be secure and reliable, from the Nuclear Command and Control System down to tactical radios that connect soldiers in the field.

Adding further complication, each service is responsible for its own procurement of computers, devices, and components and has its own procedures for doing so.[46] Each service defends itself, at least in part, and the DOD maintains separate organizations to defend the larger organization and defense agencies apart from the individual services and operational commands, all of which makes training and equipping for operations in cyberspace very bureaucratic and cumbersome. This is exacerbated by the overall defensive tone of the three mission sets: The DOD mainly defends their networks and provides defensive assistance to other agencies as required, a set of tasks that must be attended to every second of the day.

The DOD also performs offensive missions when directed to do so by the President. This is a very circumscribed set of missions, for several reasons. First, much as the entire U.S. Marine Corps would be swallowed by a megacity like Lagos, Nigeria, DOD offensive cyber assets would be overwhelmed by being everywhere and helping everyone. Additionally, many aspects of ongoing cyberspace activity do not pertain to the DOD at all. Just as most aviation activity does not concern the Air Force and most maritime activity does not involve the Navy, most cyber activity does not concern the Defense Department. An example would be an individual using PayPal to make a purchase from the web-retailer Amazon.

Operations in cyberspace as a military domain must therefore be a circumscribed mission set. Nevertheless, militarily relevant information, intelligence, criminal, and military-specific activities occur all over the Internet, so the military must be able to maneuver throughout all of cyberspace.

The Services and Cyber. The service chiefs provide cyber operations capabilities for deployment/support to Combatant Commands as directed by the Secretary of Defense.[47] In addition to joint strategy and doctrine, each service has its own doctrine to deal with cyber issues. This is not just because each service has its own history and culture. Cyber defense of ground forces is different from protecting platform-centric operations like those conducted by the Navy and Air Force. The Army must protect ground units, the Navy must protect groups of ships operating at sea across the globe, and the Air Force must protect individual flying platforms. At the same time, each service must protect its own infrastructure.

Therefore, under their Title 10 role as force providers to the combatant commanders, the services recruit, train, educate, and retain their own military cyber forces. There are four service component commands under U.S. Cyber Command (USCYBERCOM): U.S. Army Cyber Command, U.S. Fleet Cyber Command/U.S. 10th Fleet, 24th Air Force, and U.S. Marine Corps Forces Cyber Command.[48] These service-specific units have several functions: They operate and defend their portion of the DODIN; perform full-spectrum cyber operations, meaning offensive and defensive; provide for cyber training and education; and undertake cyber research and capabilities development for their respective services.

Combatant Commands are responsible for geographic areas (such as European Command) or functional areas (such as Special Operations Command or U.S. Transportation Command) and provide operations

instructions and command and control functions to the armed forces. They have a significant impact on how the service component cyber commands are organized, trained, and resourced—areas over which Congress has constitutional authority.[49] CCMDs share cyber information largely through USCYBERCOM and their own joint cyber centers, but various personnel also meet periodically to share information in collaboration sessions.[50]

USCYBERCOM was formed in 2010. It is a subunified command under U.S. Strategic Command (STRATCOM). Congress and the Obama and Trump Administrations have examined the propriety of dividing the two and promoting CYBERCOM to a full Combatant Command. This would allow CYBERCOM to work directly with other commands without having to work through an extra layer of command at STRATCOM. CYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to direct the operations and defense of specified units and the DODIN. When so directed, it also prepares to conduct full-spectrum military cyberspace operations to enable actions in all domains, ensure U.S. and allied freedom of action in cyberspace and deny the same to adversaries,[51] and counter efforts by opponents to interfere with CCMD operations.

USCYBERCOM's main instrument of power is the Cyber National Mission Force, which conducts cyberspace operations to disrupt and deny adversary attacks against national critical infrastructure. It is the U.S. military's first joint tactical command with a dedicated mission focused on cyberspace operations. It planned to create 133 cyber mission teams by the end of fiscal year 2016;[52] the current plan is for all the teams to be fully functional by 2018.[53] The force eventually will consist of 13 National Mission Teams (NMTs), which are designed to defend the United States and its interests against cyberattacks of significant consequence; 68 Cyber Protection Teams (CPTs), which defend priority DOD networks and systems against priority threats; 27 Combat Mission Teams (CMTs), which aid Combatant Commands by generating integrated cyberspace effects in support of operational plans and contingency operations; and 25 Cyber Support Teams (CSTs), which provide analytic and planning support to the National Mission and Combat Mission teams.[54]

Put another way, National Mission Teams perform strategic operations, and CMTs conduct cyberspace operations in support of CCMDs. CPTs protect the DODIN, the services, and the CCMDs. CSTs support NMTs and CMTs.

This number of teams and their organizational distribution together ensure that the U.S. military meets the need to conduct offensive and defensive cyber operations around the clock in multiple commands and in multiple areas around the world, something quite unlike conventional military forces outside of active combat engagements. Once the Cyber Mission Force is fully established in 2018, the DOD no doubt will reassess its requirements and modify the force as needed based on experience.

Conclusion

The United States is challenged by a wide variety of state and non-state actors in cyberspace, which is already huge and constantly growing. Additionally, the U.S. has certain societal vulnerabilities at home that make facing these challenges more difficult. The Department of Defense, Department of Homeland Security, and Department of Justice have to operate in this environment as the U.S. government's three principal actors, which also seek partnerships with the private sector that operates almost all of the Internet.

The U.S. government seeks to protect the United States through protection and deterrence. Because of the size and complexity of cyberspace as well as domestic legal and cultural constructs in the United States, the DOD must circumscribe the scope of its operations in cyberspace, operating in the military cyber domain as required in the criminal, informational, intelligence, and operational fields. The DOD must defend itself, assist the President in

other areas when directed to do so, and conduct defensive and offensive cyber operations as an integrated part of normal military operations.

In order to conduct these operations, the department has organized cyber forces in each of the services under the command of the Commander, United States Cyber Command, who has the task of training, educating, and building a world-class cyber force while simultaneously conducting cyber operations 24 hours a day around the globe. Conceptually, the DOD has recognized cyber as a domain, making it equal to sea, air, land, and space. "Cyber" promises to provide significant gains in the efficiency and effectiveness of U.S. military units through the full integration of conventional operations, cyber capabilities, and operations in the information environment.

Although military leaders understand the importance of cyber and information, not all understand the scope of the opportunities and challenges that cyber provides. The military services will have to expend more resources on training and equipping not only cyber forces, but all forces that will be serving in an environment where they are under continuous cyber-attack. Defensive cyber operations will protect forces from cyber-attacks while offensive cyber operations enable other conventional and special operations as an integrated whole. The U.S. is ahead of almost all other states in cyber capability, but it must continue to invest time and effort in order to maintain that lead.

Endnotes

1. Author's interview with Brigadier General Greg Touhill, U.S. Air Force (Ret.), March 27, 2015.
2. See *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, The White House, May 2011, p. 8, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed July 5, 2017). Emphasis in original. Until the Trump Administration develops strategies, we must rely on Obama-era documentation.
3. The Merriam-Webster Dictionary defines wetware as "the human brain or a human being considered especially with respect to human logical and computational capabilities." See "wetware," Merriam-Webster.com, https://www.merriam-webster.com/dictionary/wetware (accessed August 14, 2017).
4. Internet World Stats, "Usage and Population Statistics: World Internet Users and 2017 Population Stats," March 31, 2017–Update, http://www.internetworldstats.com/stats.htm (accessed August 14, 2017).
5. Steve Morgan, "Cyber Crime Costs Projected to Reach $2 Trillion by 2019," *Forbes*, January 17, 2016, https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#3f772b113a91 (accessed June 26, 2017).
6. Among the most recent laws is the Cybersecurity Information Sharing Act of 2015, incorporated into the Consolidated Appropriations Act of 2016, Public Law 114-113, 114th Cong., which was signed into law by President Barack Obama on December 18, 2015. See Brad S. Karp, "Federal Guidance on the Cybersecurity Information Sharing Act of 2015," Harvard Law School Forum on Corporate Governance and Financial Regulation, March 3, 2016, https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ (accessed July 5, 2017). Policies include a variety of executive orders, and important strategies include the May 2011 White House *International Strategy for Cyberspace* (see note 2, *supra*) and U.S. Department of Defense, *The DoD Cyber Strategy*, April 2015, https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (accessed July 5, 2017).
7. Joanna Belbey, "The Weakest Link in Cybersecurity," *Forbes*, February 27, 2015, http://www.forbes.com/sites/joannabelbey/2015/02/27/the-weakest-link-in-cybersecurity/#38c0d3377410 (accessed June 26, 2017).
8. Brigadier General Jon T. Thomas, Deputy Director, Future Joint Force Development, Joint Staff, J7, "Joint Force Development: Moving from Concept to Reality," 2013, p. 10, http://www.dtic.mil/ndia/2013/expwar/WThomas.pdf (accessed July 11, 2017); "Q&A with Rear Adm. Kevin Scott," *CHIPS Magazine*, October–December 2015, http://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=6918 (accessed July 11, 2017); and U.S. Department of Defense, *Department of Defense Fiscal Year (FY) 2017 President's Budget Submission*, The Joint Staff, *Defense-Wide Justification Book Volume 5 of 5, Research, Development, Test & Evaluation, Defense-Wide*, February 2016, pp. 75–77, http://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2017/budget_justification/pdfs/03_RDT_and_E/RDTE_MasterJustificationBook_Joint_Staff_PB_2017.pdf (accessed July 1, 2017).
9. Eleven out of 47 systems were operating without a valid cyber-certificate authorization. See Evan Perez and Tom LoBianco, "OPM Inspector General Questioned Over Hacking Report," CNN, updated June 17, 2015, http://www.cnn.com/2015/06/16/politics/opm-hack-ig-testimony/index.html (accessed June 26, 2017).
10. Ellen Nakashima, "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *The Washington Post*, July 9, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say (accessed June 26, 2017).
11. Kaspersky Lab, "Top 10 Tips for Educating Employees About Cybersecurity," 2015, http://go.kaspersky.com/rs/kaspersky1/images/Top_10_Tips_For_Educating_Employees_About_Cybersecurity_eBook.pdf?mkt_tok=3RkMMJWWfF9wsRonuKXNcO%2FhmjTEU5z16OgIWa%2BzIMI%2F0ER3fOvrPUfGjI4ITMZjI%2BSLDwEYGJlv6SgFQrDHMalq1LgPXxE%3D (accessed July 5, 2017).
12. News release, "McAfee Labs Report Highlights Success of Phishing Attacks with 80 Percent of Business Users Unable to Detect Scams," McAfee, September 4, 2014, http://www.mcafee.com/us/about/news/2014/q3/20140904-01.aspx (accessed June 26, 2017).
13. Susan Richardson, "Leaky End Users Star in DBIR 2016," Data on the Edge, May 23, 2016, http://blog.code42.com/leaky-end-users-star-in-dbir-2016/ (accessed June 26, 2017).
14. Computer Emergency Response Team, "CERT Insider Threat Center," Carnegie Mellon University, Software Engineering Institute, 2017, http://www.cert.org/insider-threat/cert-insider-threat-center.cfm (accessed June 26, 2017).
15. News release, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Department of Justice, May 19, 2014, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (accessed July 5, 2017).
16. Kevin McCaney, "Report: US Suspects Russia in 'Most Sophisticated' Joint Staff Hack," Defense Systems, August 6, 2015, https://defensesystems.com/articles/2015/08/06/joint-staff-email-hack-most-sophisticated.aspx (accessed June 26, 2017).

17. Dominic Rushe, "OPM Hack: China Blamed for Massive Breach of US Government Data," *The Guardian*, June 5, 2015, https://www.theguardian.com/technology/2015/jun/04/us-government-massive-data-breach-employee-records-security-clearances (accessed June 26, 2017).
18. News release, "Joint Statement from the Department of Homeland Security and the Office of the Director of National Intelligence on Election Security," U.S. Department of Homeland Security, October 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national (accessed June 26, 2017).
19. Anthony Cuthbertson, "Russian Cyber Attacks Aim to 'Destabilize' the West and NATO," *Newsweek*, February 3, 2017, http://www.newsweek.com/russian-cyber-attacks-hacking-nato-fallon-putin-destabilize-west-552050 (accessed June 26, 2017).
20. Ellen Nakashima and Matt Zapotosky, "U.S. Charges Iran-Linked Hackers with Targeting Banks, N.Y. Dam," *The Washington Post*, March 24, 2016, https://www.washingtonpost.com/world/national-security/justice-department-to-unseal-indictment-against-hackers-linked-to-iranian-goverment/2016/03/24/9b3797d2-f17b-11e5-a61f-e9c95c06edca_story.html?utm_term=.b0f47016466d (accessed June 26, 2017).
21. Reuters, "North Korean Hackers Were Behind a Recent Major Cyber Attack," *Fortune*, March 15, 2017, http://fortune.com/2017/03/15/north-korea-hackers-cyber-attack/ (accessed June 26, 2017), and Sean Lyngaas, "North Korean Hackers Steal F-15 Design," *FCW: The Business of Federal Technology*, June 13, 2016, https://fcw.com/articles/2016/06/13/north-korea-f15-lyngaas.aspx (accessed June 26, 2017).
22. Timothy Maurer, "Cyber Proxies and the Crisis in Ukraine," Chapter 9 in *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed. Kenneth Geers (Talinn, Estonia: NATO CCD COE Publications, 2015), pp. 79–86, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Maurer_09.pdf (accessed June 26, 2017).
23. Morgan, "Cyber Crime Costs Projected to Reach $2 Trillion by 2019."
24. G. Alexander Crowther and Shaheen Ghori, "Detangling the Web: A Screenshot of U.S. Government Cyber Activity," *Joint Force Quarterly*, Issue 78 (3rd Quarter 2015), pp. 75–83, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-78/jfq-78.pdf (accessed June 26, 2017).
25. Clorinda Trujillo, "The Limits of Cyberspace Deterrence," *Joint Force Quarterly*, Issue 75 (4th Quarter 2014), pp. 43–52, http://ndupress.ndu.edu/Media/News/News-Article-View/Article/577560/jfq-75-the-limits-of-cyberspace-deterrence/ (accessed June 26, 2017); Gerry Smith, "Stuxnet: U.S. Can Launch Cyberattacks But Not Defend Against Them, Experts Say," *Huffington Post*, June 1, 2012, http://www.huffingtonpost.com/2012/06/01/stuxnet-us-cyberattack_n_1562983.html (accessed June 26, 2017); and Jared Serbu, "Foreign Cyber Weapons 'Far Exceed' US Ability to Defend Critical Infrastructure, Defense Panel Says," Federal News Radio, March 7, 2017, https://federalnewsradio.com/dod-reporters-notebook-jared-serbu/2017/03/foreign-cyber-weapons-far-exceed-u-s-ability-defend-critical-infrastructure-defense-panel-says/ (accessed July 6, 2017).
26. This is not unique to cyber operations; it pertains to all such actions in all domains. An air strike intended to do one thing may generate a response that no one anticipated.
27. "Cyberspace," in U.S. Department of Defense, *DOD Dictionary of Military and Associated Terms*, June 2017, p. 60, http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf (accessed July 6, 2017).
28. David Aucsmith, "Cyberspace Is a Domain of War," War in Cyberspace, May 26, 2012, https://cyberbelli.com/2012/05/26/cyberspace-is-a-domain-of-war/ (accessed July 6, 2017). For another point of view, see Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society*, Vol. 8, Issue 2 (2012), pp. 321–336, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/4.Libicki.pdf (accessed June 26, 2017).
29. Military operations as used here include military or paramilitary operations that other security forces (such as the Italian Carabinieri) or intelligence forces (such as the CIA) could perform but are mainly military in nature.
30. Manoj Kumar, "Indian Navy Raises Army for Cyber Front: Recruiting Cadets Against Chinese Hackers," *International Business Times*, July 13, 2012, http://www.ibtimes.co.in/indian-navy-raises-army-for-cyber-front-recruiting-cadets-against-chinese-hackers-362686 (accessed June 26, 2017).
31. Wesley Fenlon, "How Does ATM Skimming Work?" HowStuffWorks, November 8, 2010, http://money.howstuffworks.com/atm-skimming.htm (accessed July 6, 2017).
32. Kim Zetter, "That Insane, $81M Bangladesh Bank Heist? Here's What We Know," *Wired*, May 17, 2016, https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/ (accessed June 26, 2017).
33. Spencer Ackerman and Sam Thielman, "US Officially Accuses Russia of Hacking DNC and Interfering with Election," *The Guardian*, October 8, 2016, https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election (accessed June 26, 2017).

34. Tom Hamburger and Karen Tumulty, "WikiLeaks Releases Thousands of Documents About Clinton and Internal Deliberations," *The Washington Post,* July 22, 2016, https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/?utm_term=.c84944ed0527 (accessed June 26, 2017).
35. Andreas Hagen, "The Russo–Georgian War 2008: The Role of the Cyber Attacks in the Conflict," AFCEA Cyber Conflict Case Studies Essay Contest, Second Place Entry, May 24, 2012, http://www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf (accessed June 26, 2017).
36. Angel Rabasa, Robert D. Blackwill, Peter Chalk, Kim Cragin, C. Christine Fair, Brian A. Jackson, Brian Michael Jenkins, Seth G. Jones, Nathaniel Shestak, and Ashley J. Tellis, *The Lessons of Mumbai*, RAND Corporation, 2009, http://www.rand.org/pubs/occasional_papers/OP249.html (accessed July 6, 2017).
37. Colin Clark, "Carter Details Cyber, Intel Strikes Against Daesh at NORTHCOM Ceremony," *Breaking Defense*, May 13, 2016, http://breakingdefense.com/2016/05/carter-details-cyber-intel-strikes-against-daesh-at-northcom-ceremony/ (accessed June 26, 2017).
38. U.S. Department of Defense, Joint Chiefs of Staff, *Special Operations*, Joint Publication 3-05, July 16, 2014, p. I-1, http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf (accessed June 26, 2017).
39. U.S. Department of Defense, "Fact Sheet: DoD Cyber Crime Center (DC3)," http://www.dc3.mil/ (accessed July 6, 2017).
40. Nakashima and Zapotosky, "U.S. Charges Iran-Linked Hackers with Targeting Banks, N.Y. Dam."
41. Paul Thompson, "Semantic Hacking and Intelligence and Security Informatics," Conference Paper, International Conference on Intelligence and Security Informatics, Institute for Security Technology Studies, Dartmouth College, May 27, 2003, https://link.springer.com/chapter/10.1007/3-540-44853-5_40 (accessed June 26, 2017).
42. U.S. Department of Defense, Joint Chiefs of Staff, *Cyberspace Operations*, Joint Publication 3-12 (R), February 5, 2013, p. II-5, http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (accessed June 26, 2017).
43. Australian Government, Department of Defence, Australian Signals Directorate, "Strategies to Mitigate Cyber Security Incidents," February 2017, https://www.asd.gov.au/infosec/mitigationstrategies.htm (accessed July 5, 2017).
44. U.S. Department of Defense, *The DoD Cyber Strategy*, p. 3. Emphasis in original.
45. U.S. Department of Defense, "DOD 101: Overview of the Department of Defense," https://www.defense.gov/About/DoD-101/ (accessed June 26, 2017).
46. "The Defense Department procurement process can be confusing and complicated. There are a variety of contract types—each with its own pluses and minuses. The regulations can be daunting since they seem to be the size of the tax code. The competition for contracts can be fierce. There is a lot of paperwork." Michael Bame, "Overview of the DoD Procurement Process," ThoughtCo., updated August 10, 2016, https://www.thoughtco.com/overview-dod-procurement-process-1052245 (accessed June 26, 2017).
47. U.S. Department of Defense, Joint Chiefs of Staff, *Cyberspace Operations*, p. ix.
48. U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (accessed July 5, 2017).
49. Andrew Feickert, "The Unified Command Plan and Combatant Commanders: Background and Issues for Congress," Congressional Research Service *Report for Congress*, January 3, 2013, http://fas.org/sgp/crs/natsec/R42077.pdf (accessed July 5, 2017).
50. Rita Boland, "Command's Cybersecurity Crosses Domains, Directorates," *Signal*, June 1, 2013, www.acyberstrategufcea.org/content/?q=command%E2%80%99s-cybersecurity%E2%80%A8-crosses-domains-directorates (accessed June 26, 2017).
51. U.S. Strategic Command, "U.S. Cyber Command (USCYBERCOM)," September 30, 2016, http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom/ (accessed June 26, 2017).
52. Crowther and Ghori, "Detangling the Web."
53. U.S. Department of Defense, *The DoD Cyber Strategy*.
54. Ibid.