

Promoting Security in Common Domains

Over the last several years, it has become apparent that the domains facilitating all international interaction—sea, air, space, and cyberspace—are increasingly congested, contested, and complex. These domains constitute the connective tissue of an ever more interconnected international system. It should, therefore, come as no surprise that the level of activity and investment by both state and non-state actors is rapidly increasing. Satellites are being launched, submarines are being built, long-range aircraft procured, and powerful cyberspace capabilities are being maintained by states that only two decades ago were just beginning to employ rudimentary computer systems. Non-state actors, ranging from pirates off Somalia to cyber “hacktivists” to the growing number of commercial players that own and operate satellites, further complicate this landscape.

The implications of these developments are not fully understood by the U.S. national security community. Yet, there is a broad consensus that they represent both a significant challenge and a major opportunity. Therefore, if the United States is to continue its role in helping create and sustain an international system that promotes peace and prosperity, it must update strategic concepts, adapt instruments of statecraft, and develop innovative approaches to leadership in these critical domains.

Strategic Darwinism: Evolve or Else

The scope and scale of the shifts taking place in these domains are reminiscent of the late Cold War period, when defense officials in the Soviet Union were

Shawn Brimley is a strategist in the Office of the Secretary of Defense. The views expressed here are the author's alone and do not necessarily reflect those of the Department of Defense or the U.S. government.

Copyright © 2010 Center for Strategic and International Studies
The Washington Quarterly • 33:3 pp. 119–132
DOI: 10.1080/0163660X.2010.492725

Report Documentation Page

*Form Approved
OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE JUL 2010	2. REPORT TYPE	3. DATES COVERED 00-00-2010 to 00-00-2010			
4. TITLE AND SUBTITLE Promoting Security in Common Domains		5a. CONTRACT NUMBER			
		5b. GRANT NUMBER			
		5c. PROGRAM ELEMENT NUMBER			
6. AUTHOR(S)		5d. PROJECT NUMBER			
		5e. TASK NUMBER			
		5f. WORK UNIT NUMBER			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Office of the Secretary of Defense, Washington, DC, 20301		8. PERFORMING ORGANIZATION REPORT NUMBER			
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)			
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)			
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 14	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

among the first to truly comprehend what emerging U.S. prowess in long-range and precise weaponry represented—a military-technical revolution that threatened to rapidly erode their perceived military advantages. The reality of U.S. military dominance was on full display during the 1991 Gulf War, when what was then the third largest military in the world was unable to withstand the combined force of stealth aircraft, cruise missiles, special operations forces, and armored divisions—all enabled by advanced sensors and highly networked command and control systems.

Many in the United States triumphantly embraced these developments as evidence of a unique and enduring ability to project and sustain power. Yet, some states—with reason to be concerned about U.S. freedom of action on and in the sea, air, space, and cyberspace—were spurred to embark on a path of military modernization and doctrinal development that, with time, would be able to hold this ability at risk. That time has now arrived. While the United States continues to hold clear advantages in sea, air, space, and cyberspace capabilities, other actors are and will be positioned to credibly contest them in a wide range of contingencies—from insurgencies and state failure, to major conventional

The United States views peace and security within these domains as a common global good.

warfare, to the ever expanding “hybrid” possibilities in between. The challenges posed by this emerging reality should not be overestimated. Yet, they cannot be ignored.

As current conflicts and both unofficial as well as official assessments of the emerging security environment have shown, possible adversaries will employ methods designed to offset U.S. strengths.¹ Potential challengers have powerful incentives to

invest in systems designed to threaten the primary means that the United States utilizes to project power—essentially military bases, sea and air assets, and the networks that support them.² Such systems include but are not limited to: ballistic missiles that can threaten bases and potentially ships; anti-satellite systems; cyber warfare capabilities; long-range aviation forces; anti-ship cruise missiles; and a range of enabling radar and satellite technology. These types of systems would most likely be employed in what the Department of Defense (DOD) terms as an “anti-access” strategy—one designed to blunt or deny U.S. power projection capabilities. Importantly, the acquisition and posture of such systems in sufficient numbers by a potential adversary will add complexity to the decisionmaking calculus of U.S. policymakers charged with considering whether and how to deploy military forces into high-risk environments.

Decisions by a range of actors to make substantial investments in these areas are also enabled by an international system that, through continued market integration and technological openness, has lowered entry barriers, making it cheaper and easier to acquire or develop advanced technology, which in the previous century would have been available to only a few states. These dynamics are most clearly at play in cyberspace, as small groups or individuals can have an outsized impact, but are also present in other domains. For instance, the ability of terrorist groups to acquire sophisticated weaponry via state sponsors or the black market can pose significant threats to modern militaries, as can the ability to easily purchase detailed satellite imagery from commercial providers.³

That a range of state and non-state actors could credibly challenge elements of U.S. ability to project and sustain military power is not surprising. Nor does it necessarily suggest that actors who invest in such capabilities seek either to challenge U.S. leadership or to upend long-standing international diplomatic and governance frameworks concerning their use. Rather, such actors are pursuing their rational self-interest in a world in which dynamics in the sea, air, space, and cyberspace domains are increasingly central to the security and prosperity of all nations.

For a period after the fall of the Berlin Wall, some assumed that U.S. military dominance would dissuade both allies and competitors from making investments in capabilities designed to facilitate long-range power projection. These assumptions have proven false. From the perspective of a rising power like India or China, it makes perfect sense to develop the ability to not only protect critical airspace, coastlines, or space and cyberspace assets, but also to project and sustain power and influence abroad.⁴ Whether it is to protect critical sea lanes, participate in multilateral peacekeeping and antipiracy operations, maintain the ability to credibly project power against possible adversaries, or hold the capabilities of potential rivals at risk, the twenty-first century international system will require great powers to create and maintain these capabilities.

The challenge for the United States is not to oppose these developments, but rather to exercise adroit and prudent statecraft to properly sustain leadership in a world in which these domains become far more complicated than ever before.

Not as New as You Think

The White House, along with the DOD, the Department of State, and the intelligence community, are paying attention to the shifting security environment outlined above. Too often however, domain-centric stovepipes have made it difficult to gain a broader, more strategic view of what changing

dynamics in the sea, air, space, and cyberspace domains portend for the protection and pursuit of U.S. interests.

To properly construct a strategic approach to increasing complexity within the sea, air, space, and cyberspace domains first requires acknowledging their interconnectedness. Modern aircraft and maritime vessels increasingly depend on satellite constellations for navigation, and today's globalized economy would quickly grind to a halt without the Internet. These domains are global by nature, and they are common mediums all international actors use for communication and commerce. In this sense, they can be meaningfully described as the "global commons." The use of this analogy has no formal legal meaning, nor does it imply that these domains necessarily share a common diplomatic or commercial framework. Characterizing any domain as a global common does not suggest that aircraft, satellites, ships, or information networks are not the property of a state or actor. Rather, the term "global commons" illustrates the interconnectedness of

these domains, helping to break down domain-centric concepts and bureaucratic stovepipes. More importantly, it helps to communicate to key U.S. international allies and partners that the United States views peace and security within these domains as a common global good—something that all nations can benefit from equally.⁵ Thus, both Secretary of State Hillary Rodham Clinton and Secretary of Defense Robert M. Gates have employed the term in speeches and official documents.⁶

The strategic imperative is to develop innovative new approaches for the global commons.

Developing a more integrated approach to the global commons is entirely compatible with the long-standing U.S. leadership role in creating and sustaining a healthy international system. In the years following the end of World War II, U.S. strategists grappled with the emergence of both the nuclear age and a powerful Soviet rival with significant air, maritime—and soon space—capabilities. They managed to articulate a strategic approach that lasted for not only the entire Cold War but remains relevant today. National Security Council report 68—the 1950 planning document generally identified as articulating the contours of the U.S. Cold War approach—concluded that a core pillar would be a policy “which we would probably pursue even if there was no Soviet threat . . . it is a policy of attempting to develop a healthy international community.”⁷ Over the course of four decades, the United States pursued a grand strategy that protected U.S. interests by investing in diplomacy, defense, development, and intelligence instruments, promoted an extensive network of alliances and partnerships with states that shared interests with the United States, and pursued strong international norms

and agreements on key global issues that reflected U.S. values. An important element of this strategy included consistent leadership in promoting peace and security in the sea, air, and space domains. These actions helped reinforce an international system whose very architecture promoted vital U.S. interests.

The characteristics of today's international system continue to reflect the interests of the United States and other nations who value robust global communication and commerce underpinned by peaceful cooperation in—and stewardship of—the sea, air, space, and cyberspace domains. The strategic imperative for U.S. policymakers is not only to update the Cold War-era diplomatic and legal frameworks that enabled relative peace and security throughout the global commons, but to develop innovative new approaches to ensure that the architecture of the international system can bear the weight of new challenges—enabling the United States, its allies and partners, and the international community to fully benefit from tomorrow's opportunities.

Space: the High Ground

The need to update and build on Cold War-era approaches is most clear in space. The international norms and agreements that help guide behavior in this domain, such as the 1967 Outer Space Treaty, were forged in a bipolar era wholly different from today's environment and require strengthening as space becomes a much more complex and crowded domain.

The United States remains the most active space-faring nation. In 2009 alone, it conducted 65 commercial and national space launch missions. But the United States is far from the only significant player in space. Today, nine nations or consortia maintain indigenous launch capability and there are over 60 nations or consortia with assets in orbit. In 1980, there were approximately 4,500 objects in orbit, while today there are more than 21,000 of ten cm or more in diameter.⁸ In other words, space is a far more congested environment than many realize.⁹

The problem of space debris illustrates today's more congested environment. The use of space has produced debris that threatens the long-term sustainability of key orbital belts. While the creation of most debris is accidental—such as the February 2009 collision between a Russian Cosmos satellite and a privately-owned Iridium satellite—some result from intentional acts. For example, China's January 2007 test of an anti-satellite missile system created over 2,000 pieces of debris, most of which will circle the planet for decades.¹⁰ The U.S. Space Shuttle has had to maneuver to avoid dangerous debris, and U.S. national security satellites have expended valuable fuel to avoid collisions. The increasing problem of congestion requires updated international guidelines and best practices for monitoring and warning of possible collisions.

The need to update and build on Cold War-era approaches is most clear in space.

Space is also growing more competitive. More than 60 nations or consortia utilize space for civil, commercial, intelligence, and military purposes. European nations are producing advanced capabilities that can be used for civil, commercial, or defense purposes—the emerging Galileo satellite constellation is an example.¹¹

Russia maintains the extensive space infrastructure and remains a key U.S. partner on joint civilian programs such as the International Space Station. China is developing robust capabilities across the spectrum—from satellite constellations to a manned space program with lunar aspirations. In recent years, both Japan and India have enhanced their civilian space capabilities. Last February, Iran launched its first satellite, and in recent years North Korea conducted several failed long range missile tests that it claimed were successful satellite insertions.¹² Moreover, the commercial space industry includes markets for satellites as well as launch capability, the economic value of which is estimated to be several hundred billion dollars.¹³ As the interim Space Posture Review to Congress concluded, the United States no longer enjoys a paramount position in the international marketplace for space capabilities and services.¹⁴

Finally, space has long been used for military purposes, and these dynamics are sure to continue. The United States' space infrastructure allows the U.S. military to strike with precision, to navigate with accuracy, to communicate with certainty, and to see the battlefield with clarity.¹⁵ Other nations are seeking the ability to hold these advantages at a degree of risk. U.S. and allied space assets today are threatened by a range of counterspace capabilities, from spectrum jamming to the physical destruction of satellites. China is far from the only actor seeking to develop the capability to deny or interfere with the space capabilities of others. Iran has repeatedly jammed commercial satellites to censor television news to their public, and other actors have made similar efforts.¹⁶

Given these dynamics, the United States must be prepared to operate in a contested space environment. This not only requires significant improvements in the ability to detect natural or man-made threats to the space-based platforms of the United States and its allies and partners, but it necessitates building improved resiliency into its systems. Across a range of potential contingencies, U.S. armed forces need to be able to both prevail in environments in which a portion of its space infrastructure is temporarily degraded, but deter such situations by reducing vulnerabilities, increasing operational responsiveness, and maintaining the ability to respond appropriately to any attack.

Final Frontier 2.0

No domain holds so much challenge and opportunity as cyberspace. It is hard to overstate the degree of dependence the United States has on the information systems and networks that integrate industry, empower entrepreneurship, and enable the pursuit of U.S. interests at home and abroad.

The United States depends on cyberspace for its prosperity—as President Barack Obama has said, it has “become woven into every aspect of our lives.”¹⁷ Cyberspace is obviously a man-made domain, but it retains many of the basic characteristics of the natural domains of the sea, air, and space—ubiquitous, central to lives and livelihoods, and so vast that establishing total awareness or control is practically impossible. While component parts of information networks and infrastructure are owned by states, businesses, and other actors, the nature of this architecture and the way information moves within it demands a global view. In this important respect, it is useful to conceive of cyberspace as a global domain—like the sea, air, and space domains.

U.S. security is highly dependent on cyberspace. DOD’s information networks provide command and control of U.S. forces, the intelligence and logistics on which they depend, and the weapons technologies that are developed and utilized in the field. As the 2010 Quadrennial Defense Review (QDR) concluded: “In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace.”¹⁸ On any given day, there are up to seven million DOD computer and telecommunications tools in use in 88 countries, using thousands of war-fighting and support applications. As a consequence, U.S. defense networks are scanned millions of times each day.¹⁹ The sophistication and frequency of the threats posed to U.S. defense and other national networks are rapidly increasing as well.

The level of speed, automation, and anonymity that help define the characteristics of cyberspace pose difficult challenges from a defense and intelligence perspective. And while the DOD and intelligence community are generally considered the best prepared for cyber defense, the nature of the domain tends to favor the offense. Therefore, to truly defend and advance U.S. interests, the U.S. approach to cyberspace cannot consist only of static defense. As Deputy Secretary of Defense William Lynn has argued, the United States must “resist the temptation of trying to retreat behind a fortress of firewalls. We can’t afford a digital version of the Maginot Line.”²⁰

Consequently, DOD is adapting to the rapidly evolving cyber environment by developing a set of sophisticated cyber capabilities that it is consolidating in U.S. Cyber Command (USCYBERCOM), which will have the day-to-day

responsibility for operating and defending DOD's information networks.²¹ A key component of USCYBERCOM's mission is to create and sustain a tailored suite of capabilities that can help defend U.S. military networks and, if directed by the president, hold an adversary's network at a degree of risk. DOD is also focusing resources on building a cadre of cyber experts and equipping them with the latest technologies to protect and defend U.S. information networks. Just as the growing importance of space in the middle of the twentieth century demanded significant investments in both capabilities and personnel who could design, build, and field revolutionary new systems, the DOD and its interagency partners are working to ensure the availability of a workforce of highly skilled civilian and military cyber security specialists.

**Advancing U.S.
interests in
cyberspace requires
promoting Internet
freedom.**

Importantly, advancing U.S. interests in cyberspace requires that any military and intelligence capabilities play a supporting role in a positive agenda that champions international norms and agreements to promote free access and prosperity in accordance with U.S. values. Just as the United States supports norms and frameworks in other domains that promote fair access and cooperation, it is beginning to articulate an international agenda that promotes Internet freedom.

As in other domains, a positive agenda requires strong diplomacy reinforced by capable defenses. As Clinton has argued, by articulating and reinforcing U.S. desire for openness and freedom in cyberspace, "we can create norms of behavior among states and encourage respect for the global networked commons."²² For cyberspace in particular, this requires strong interagency and international partnerships that can articulate a cohesive approach and marry such an approach with strategies and policies that reinforce shared interests.

In many ways, however, government actors are far from the only leaders in cyberspace policy and strategy. Google's recent decision to close its Internet search service in China was a significant development that arguably constitutes a turning point in the history of cyberspace—for the first time, a leading corporation forcefully defended Internet freedom in the face of state censorship and withdrew from a large market when it was consistently violated.²³ As has been seen in other key domains, the principles of fair access and freedom of movement undergirded by strong international agreements and frameworks will be a key characteristic of U.S. cyberspace strategy.

Common Seas and Skies

The pace and scope of changes in the air and sea domains remain vital national security concerns. The United States' long-held supremacy in the ability to project and sustain power in these domains continues, but the degree of superiority will inevitably lessen over time as rising powers make significant investments, technology becomes more advanced, and as proliferation of advanced weapon systems accelerates.

Naval dynamics are being strongly influenced by the rising importance of maritime geography. For example, as China and India further integrate into the global economic system, they are becoming more reliant on the security and stability of key sea lines of communication. As Robert Kaplan has outlined, more than 85 percent of the oil and oil products bound for China cross the Indian Ocean and pass through the Strait of Malacca. India depends on the Middle East for 90 percent of its oil imports, and currently operates the world's fifth largest navy.²⁴ These dynamics form the backdrop for an important phase in the geopolitics of Asia—a period where ensuring access to, and the stability of, critical sea lines of communication will pose substantial challenges to U.S. diplomacy and defense planning. Moreover, changing climate conditions in the Arctic will eventually result in large areas of the region being free of ice, and thus useful for commercial shipping during parts of the year. The Arctic is thus an area of increasing international attention by maritime and particularly northern nations.²⁵

This shared need—along with the United States—for secure sea lines of communication offers powerful incentives for cooperation in a wide range of areas, from antipiracy to naval exchanges and perhaps even multilateral exercises and partnerships. These shifting dynamics are well known to naval analysts such as Frank Hoffman, who concludes that if oriented toward openness and stability:

... emerging naval powers could be significant bulwarks supporting the health and success of the international system. However, if geared toward anti-access missions and exclusivity, they could profoundly challenge the U.S. Navy's ability to maintain the openness of the maritime commons.²⁶

As the 2010 QDR described, in addition to counterspace and cyber capabilities, China is deploying significant numbers of medium-range ballistic and cruise missiles, new attack submarines equipped with advanced weapons, increasingly capable long-range air defense systems, and advanced fighter aircraft. These investments appear to be designed, at least in part, to create the ability to temporarily contest or deny freedom of access and movement in the maritime approaches to the mainland. Moreover, China's navy is

developing the capability to deploy surface combatants and submarines at extended distances from the Chinese mainland.²⁷

These investment patterns are not limited to China. Other states are acquiring anti-ship cruise missiles, quiet submarines, advanced mines, and other systems that threaten naval operations. In addition to these weapons, Iran has fielded large numbers of small, fast-attack craft to employ “swarming” tactics designed to overwhelm the defenses of the United States and other nations’ naval vessels.²⁸

Similar dynamics are also influencing investment patterns in global air power. Based on current trends, it is likely that U.S. air forces in future conflicts will encounter integrated air defenses of far greater sophistication and lethality than those fielded by current adversaries. Proliferation of modern surface-to-air missile systems will pose growing challenges for U.S. military operations worldwide. And non-state actors such as Hezbollah have acquired unmanned aerial vehicles and man-portable air defense systems from Iran.²⁹ In particular, the United States and its allies will need to prepare for an environment in which unmanned aerial systems are much more widely available to state and non-state actors. The range, persistence, and autonomy such systems will possess require focused attention by those concerned with the future of global air power.³⁰

To better prepare for a complex future environment in which anti-access capabilities of the kind described above are widely proliferated, Gates has asked the air force and navy to develop a joint air-sea battle concept for defeating adversaries across the range of military operations, including those equipped with sophisticated anti-access and area denial capabilities.³¹ The concept will address how air and naval forces will integrate capabilities across all operational domains—sea, air, land, space, and cyberspace—to counter growing challenges to U.S. freedom of action. As it matures, the concept will not only help guide the development of future capabilities needed for effective military operations, but it is likely to heavily influence how the DOD works with allies and partners in these domains.³²

The Coming Convergence

Spurred by changing dynamics throughout the sea, air, space, and cyberspace, the DOD is assessing how it can help maintain stability in these critical domains while protecting U.S. interests. The department is developing a new National Security Space Strategy, completing a comprehensive internal assessment of cyberspace strategy, and developing an AirSea battle concept. These reviews will help further guide the department as it considers how best to invest in the capabilities and training required for a complex future.

It is particularly important to consider how growing complexity in the sea, air, space, and cyberspace might cause actors in the international system to make widely different judgments concerning both the intentions and capabilities of others. Cold War deterrence dynamics were incredibly complex, and if the forgoing assessment is valid, it seems reasonable to conclude that cross-domain deterrence dynamics will constitute a core analytic issue for the U.S. defense, diplomatic, and intelligence community—particularly as shifts in the actual or perceived balance of power in sea, air, space, and cyberspace become more opaque. For example, it is critical to develop greater insight into the complex issues involving conflict in space and cyberspace (e.g., when attacks in space or cyberspace constitute a use of force inconsistent with UN Charter obligations), and how to control escalation dynamics to avoid such an unfortunate scenario (e.g., when and how conflict in space or cyberspace might result in the use of air, ground, and sea forces).³³

The converging challenges and opportunities presented to the United States by dynamics across these domains cut across all aspects of the U.S. economy, society, and its international relations. While this brief review has focused on the military's role, a comprehensive whole-of-government approach is essential. Moreover, the U.S. government must work increasingly closely with both private sector and international partners. The United States must continue to build and strengthen partnerships and to provide, as much as possible, common approaches to the global commons.

U.S. instruments of statecraft—including diplomacy and development, defense and intelligence—are working hard to update approaches to a security environment that is increasingly complex. Changing dynamics on and in the sea, air, space, and cyberspace will pose some of the most difficult challenges the international community will face this century. Assessing these dynamics, integrating historical lessons, and implementing cohesive strategies will demand focused attention in the government, the private sector, and key research institutions. The United States is at the beginning of a critical and lasting national security imperative—to prepare U.S. institutions and the American people for a set of cross-domain challenges that demand new thinking and innovative approaches.

The United States is at the beginning of a critical and lasting national security imperative.

It is in the U.S. interest to continue to shape the future of the international system, and help maintain peace and security in the common global domains that sustain it. The essence of the U.S. approach to this challenge must draw on

the positive legacy of its leadership during a similar inflection point in the middle of the last century. Reaffirming its leadership, reorienting its national security strategies and programs, and renewing its role as the security and diplomatic partner of choice throughout the global commons will do much to not only sustain, but also to elevate, its role in the decades ahead.

Notes

1. See National Intelligence Council, "Global Trends 2025: A Transformed World," November 2008, http://www.dni.gov/nic/PDF_2025/2025_Global_Trends_Final_Report.pdf and U.S. Joint Forces Command, "Joint Operating Environment 201," February 2010, http://www.dni.gov/nic/PDF_2025/2025_Global_Trends_Final_Report.pdf.
2. See Department of Defense (DOD), "Quadrennial Defense Review," February 2010, pp. 8–9, http://www.defense.gov/QDR/images/QDR_as_of_12Feb10_1000.pdf and Robert M. Gates, speech, U.S. Naval War College, Newport, RI, April 17, 2009, <http://www.defense.gov/speeches/speech.aspx?speechid=1346>.
3. Such dynamics are clearly at play in contemporary conflicts, such as in Afghanistan, Iraq, and the 2006 Lebanon war. High resolution satellite imagery (less than 1 meter resolution) is commercially available.
4. For example, in July 2009, India became the sixth nation to field a nuclear-powered submarine. See Lydia Polgreen, "India Launches Nuclear Submarine," *New York Times*, July 27, 2009, <http://www.nytimes.com/2009/07/27/world/asia/27india.html>. DOD has assessed that while China's emerging military capabilities have allowed it to contribute cooperatively in areas such as peacekeeping, humanitarian assistance and disaster relief, and counter piracy, some of these capabilities, as well as other, more disruptive ones, could allow it to project power to ensure access to resources or enforce claims to disputed territories. See Office of the Secretary of Defense, "Annual Report to Congress: Military Power of the People's Republic of China," 2009, p. 1. http://www.defense.gov/pubs/pdfs/China_Military_Power_Report_2009.pdf.
5. See Joseph Nye, "Recovering American Leadership," *Survival* 50, no. 1 (February–March 2008): 55–68.
6. See Hillary Rodham Clinton, "Remarks on Internet Freedom" (speech, Washington, D.C., January 21, 2010), <http://www.state.gov/secretary/rm/2010/01/135519.htm> (hereinafter Clinton's remarks on Internet freedom) and Gates views on the importance of security in the global commons can be found in both the 2010 Quadrennial Defense Review, p. 8 and the DOD, "National Defense Strategy," June 2008, pp. 6, 16, <http://www.defense.gov/news/2008%20National%20Defense%20Strategy.pdf>.
7. Ernest May, ed., *American Cold War Strategy: Interpreting NSC 68* (New York: St. Martins, 1993), p. 41.
8. Some of the difference can likely be attributed to much better space surveillance capabilities that exist today relative to 1980. Objects in orbit today include over 1,100 active satellites, 10,000 pieces of space debris, 3,700 dead satellites and rocket pieces, and 5,700 unknown objects. There are many more thousands of objects less than ten cm in diameter that can pose threats to spacecraft. See prepared testimony of Lt. Gen. Larry James before the Subcommittee on Strategic Forces, Senate Armed Services Committee, March 10, 2010, <http://armed-services.senate.gov/statemnt/2010/03%20March/James%2003-10-10.pdf>.

9. See Marc Kaufman, "U.S. Finds It's Getting Crowded Out There," *Washington Post*, July 9, 2008, p. A1, <http://www.washingtonpost.com/wp-dyn/content/article/2008/07/08/AR2008070803185.html>.
10. See Joseph Kahn, "China Confirms Test of Anti-Satellite Weapon," *New York Times*, January 23, 2007, <http://www.nytimes.com/2007/01/23/world/asia/23cnd-china.html>.
11. When completed, the Galileo constellation will offer an alternative to the U.S. Global Positioning System (GPS) constellation that broadcasts signals allowing for precision positioning, timing, and navigation.
12. See Nazila Fathi and William Broad, "Iran Launches Satellite as U.S. Takes Wary Note," *New York Times*, February 3, 2009, p. A1, <http://www.nytimes.com/2009/02/04/world/middleeast/04iran.html> and Blaine Harden, "N. Korea Puts Launch in Innocuous Terms," *Washington Post*, February 25, 2009, p. A11, <http://www.washingtonpost.com/wp-dyn/content/article/2009/02/24/AR2009022400324.html>.
13. See Eric Sterner, "Beyond the Stalemate in the Space Commons" in *Contested Commons: The Future of American Power in a Multipolar World*, February 2010, pp. 105–136, http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf.
14. The Interim Space Posture Review, co-authored by the DOD and the Office of Director National Intelligence and provided to Congress, is not publicly releasable. Key themes, however, can be found in the testimony of Principal Deputy Under Secretary of Defense for Policy James N. Miller to the House of Representatives Committee on Armed Services Subcommittee on Strategic Forces on March 16, 2010, http://armedservices.house.gov/pdfs/StratForces031610/Miller_Testimony031610.pdf.
15. See Deputy Secretary of Defense William Lynn, remarks, National Space Symposium, Colorado Springs, Colorado, April 14, 2010, <http://www.defense.gov/speeches/speech.aspx?speechid=1448>. Lynn was paraphrasing comments made by Gen. Robert Kehler, Commander, U.S. Air Force Space Command, at the same symposium on April 13, 2010.
16. See Deputy Assistant Secretary of Defense for Cyber and Space Policy Robert Butler, testimony before the House of Representatives Committee on Armed Services Subcommittee on Strategy Forces, April 21, 2010, http://armedservices.house.gov/pdfs/SF042110/Butler_Testimony042110.pdf.
17. Office of the Press Secretary, The White House, "Securing Our Nation's Cyber Infrastructure," Washington, D.C., May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.
18. Quadrennial Defense Review, p. 37, http://www.defense.gov/QDR/images/QDR_as_of_12Feb10_1000.pdf.
19. See William Lynn, "Protecting the Domain: Cybersecurity as a Defense Priority" (speech, CSIS, Washington, D.C., June 15, 2009), http://csis.org/files/attachments/090615_sf_lynn.pdf.
20. Ibid.
21. USCYBERCOM will be a sub-unified command to U.S. Strategic Command (USSTRATCOM). See the confirmation testimony of Lt. Gen. Keith Alexander (confirmed as the first Commander, U.S. Cyber Command) to the Senate Committee on Armed Services, April 15, 2010, http://armed-services.senate.gov/testimony.cfm?wit_id=9315&id=4505.
22. Clinton's remarks on Internet freedom.
23. See Miguel Heft and David Barbosa, "Google Shuts China Site in Dispute Over Censorship," *New York Times*, March 22, 2010, <http://www.nytimes.com/2010/03/23/technology/23google.html>.

24. See Robert Kaplan, "Center Stage for the 21st Century: Power Plays in the Indian Ocean," *Foreign Affairs* 88, no. 2 (April/May 2009): pp. 16–32; "The Geography of Chinese Power," *Foreign Affairs* 89, no. 3 (May/June 2010): 22–41; James Holmes, Andrew Winner, and Toshi Hoshihara, eds., *Indian Naval Strategy in the 21st Century* (New York: Routledge, 2009), p. 82.
25. See Scott Borgerson, "The Great Game Moves North," *Foreign Affairs Postscripts*, March 25, 2009, <http://www.foreignaffairs.com/articles/64905/scott-g-borgerson/the-great-game-moves-north>.
26. See Frank Hoffman, "The Maritime Commons in the Neo-Mahanian Era," in *Contested Commons: The Future of American Power in a Multipolar World*, February 2010, p. 53, http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf.
27. See Commander U.S. Pacific Command Admiral Robert Willard, testimony to Senate Armed Services Committee, March 24, 2010, <http://armed-services.senate.gov/statemnt/2010/03%20March/Willard%2003-26-10.pdf>; Edward Wong, "Chinese Military Seeks to Extend its Naval Power," *New York Times*, April 24, 2010, p. 1, <http://www.nytimes.com/2010/04/24/world/asia/24navy.html>; Robert Ross, "China's Naval Nationalism: Sources, Prospects, and the U.S. Response," *International Security* 34, no. 2 (Fall 2009): 46–81; Ronald O'Rourke, "China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress," CRS Report for Congress, RL33153, December 23, 2009, <http://www.fas.org/sgp/crs/row/RL33153.pdf>.
28. See Quadrennial Defense Review, p. 32.
29. *Ibid.*
30. For a detailed examination of this issue see Peter Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Press, 2009).
31. See Quadrennial Defense Review, p. 32.
32. For an excellent overview of this issue, see Andrew F. Krepinevich, "Why AirSea Battle?" 2010, http://www.csbaonline.org/4Publications/PubLibrary/R.20100219.Why_AirSea_Battle/R.20100219.Why_AirSea_Battle.pdf and Jan van Tol et al., "Airsea Battle: A Point-of-Departure Operational Concept," 2010, http://www.csbaonline.org/4Publications/PubLibrary/R.20100518.Air_Sea_Battle_A_/R.20100518.Air_Sea_Battle_A_.pdf.
33. See CSIS Commission on Cybersecurity for the 44th Presidency, "Securing Cyberspace for the 44th Presidency," December 2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf and Damon Coletta and Frances Pilch, eds., *Space and Defense Policy* (New York: Routledge, 2009).