spotlight on security

Security Challenges in the 21st Century Global Commons

By Tara Murphy

National defense is no longer ensured only through maintaining the sanctity of one's borders, but is also highly dependent upon the ability to navigate safely through the global commons. These commons—sea, air, space, and cyberspace—enable militaries to protect national territory and interests, as well as facilitate the passage of goods, people, communication, and data upon which every member of the international community depends. Yet, a number of emerging trends are threatening this freedom of action. The effect is that as the United States and other nations increasingly rely upon the commons in a globalized world, challenges to freedom and stability within these commons are simultaneously growing.

In today's global community, a state cannot consider its security solely a function of the areas directly surrounding it; rather, the security of one is tightly linked to the security of all. National defense is not ensured only through maintaining the sanctity of one's borders, but is also highly dependent upon the ability to navigate safely through the global commons. These

---

Tara Murphy is a fellow with the Defense and National Security Group at the Center for Strategic and International Studies (CSIS), where she has developed an analytic framework of the broad range of issues related to U.S. nuclear weapons policy and nonproliferation for the *Towards a Comprehensive Framework for Integrating Nuclear Issues* project, and been a contributing author to two CSIS reports, *Transforming NATO (…again): A Primer for the NATO Summit in Riga 2006* (CSIS, 2006), and *A Collection of Papers from the 2006 PONI Conference Series* (CSIS, 2007). Previously, Ms. Murphy was Project Coordinator of the Project on Nuclear Issues at CSIS, and a non-resident fellow at the Center for the Study of the Presidency, where she authored a paper, "Widening the Divide: The Role of Leadership in the Transatlantic Rift" (CSP, 2004). Ms. Murphy holds an M.A. in Security Studies from Georgetown University and a B.S. *magna cum laude* in International Affairs with a minor in French from the Georgia Institute of Technology.

commons—comprised of the domains of sea, air, space, and cyberspace—enable militaries to protect national territory and interests, as well as facilitate the passage of goods, people, communication, and data upon which every member of the international community depends.

The sea provides passageway to 45,000 merchant ships worldwide and over 90 percent of global trade.[1] Each year, 2.2 billion passengers, 40 percent of international tourists, and 44 million tons of freight travel by air. The global economic impact of air transport in 2007 was estimated to be $3.5 trillion, or 7.5 percent of global GDP.[2] Additionally, the economic worth of the communications, imagery, and positioning data gained from satellites in space was $257 billion in 2008, and each day, financial traders in New York City transfer more than $4 trillion, or approximately 25 percent of annual U.S. GDP, via the Internet.[3] As the 2010 U.S. Department of Defense's *Quadrennial Defense Review Report* states, "Global security and prosperity are contingent on the free flow of goods shipped by air or sea, as well as information transmitted under the ocean or through space."[4] Access to the global commons enables these flows, in turn promoting both international stability and prosperity.

Indeed, global commerce, travel, and information have greatly contributed to the growing wealth of nations and to the stability of the post-Cold War international system. The world's seas, air, space, and—more recently—cyberspace also play critical roles in states' national defense and their ability to conduct military operations worldwide. The United States relies on freedom to operate in the commons in order to protect the U.S. homeland and its vital national interests. Yet as the global commons grows, the number of emerging trends that threaten this freedom of action also increases.

As these trends continue and use of the commons becomes more contested, the United States will find it increasingly difficult to achieve its stated strategic objectives. While there is wide discussion on the implications of these challenges on U.S. freedom of operation within each of the separate domains, holistic analysis of the global commons from a strategic perspective is lacking.[5] The fundamental interdependency of these four domains transcends their unique attributes and creates specific opportunities for U.S. and international leaders to improve their security. For this reason, it is worth examining the 21st century's challenges within the global commons side by side. Doing so highlights the opportunity for the United States to lead the international community in taking steps to counter these challenges—namely, by addressing the threats, strengthening governance, and promoting stability within the commons. This, in turn, will ensure that the global commons continue to serve as the foundation of the global economy and the facilitator of international security.

Global Commons Overview

The global commons are those areas that are not under the control of a particular state, but are open for use by states, organizations, and individuals worldwide. They have been described by leaders in the Department of Defense (DoD) as the "fabric or connective tissue of the international system,"[6] and include the sea, air, space, and cyberspace domains.[7] Because these areas exist beyond the sovereign bounds of any nation, governance must be achieved through international treaty or agreement.

The global commons are those areas that are not under the control of a particular state, but are open for use by states, organizations, and individuals worldwide.

The foundation for international cooperation and regulation of the maritime domain is strong and is based in the United Nations Convention on the Law of the Sea (UNCLOS). UNCLOS is a comprehensive international legal framework that defines states' territorial boundaries into and above waterways, identifies states' rights to resources in their territorial waters, and regulates behavior on the seas. The United States signed the UNCLOS treaty in 1994 and continues to adhere to all of its provisions, but has yet to ratify the agreement.[8] The institutional frameworks that provide for governance of airspace are similarly well developed. International treaties define a state's sovereign airspace as 60,000 feet above its geographic boundaries and twelve miles from its coastline. Although there is no single global regime for the regulation of airspace access and over-flight rights, extensive international and bilateral agreements exist to address these issues and regulate the skies for commercial use.[9] Long-standing presence in the seas and air has allowed states ample time to develop these regulatory frameworks that ensure standards of use and responsibility for maintaining security within these domains.

By contrast, space and cyberspace have notably less mature governance regimes. The launch of the Soviet satellite, Sputnik I, into geosynchronous orbit in 1957 unveiled space as a new frontier.[10] So far, international efforts have prevented the weaponization of outer space. The 1967 Outer Space Treaty continues to serve as the primary regulatory structure that establishes space as a global commons and defines states' right to access and use space for peaceful purposes.[11] Although past arms control agreements have addressed space use, they are dated and no other institutionalized

agreements that deal with space issues exist. Largely anarchic, cyberspace lacks any type of formal governance regime. Regulation of cyberspace is complicated by several factors, particularly the private sector's high level of ownership. Although some agreements on standards and regulations have been reached, the burden of responsibility to provide cyber-security falls primarily on individual users. As both the newest and arguably most unique members of the global commons, the space and cyberspace domains present governance challenges that call for continued effort, creative thought, and public–private sector cooperation. If those objectives can be attained, the possibility of extending the type of institutionalized cooperation that governs the seas and air into space and cyberspace is promising.

Issues related to governance and the sharing of communal resources have dominated much of the academic study of the global commons. Perhaps the most frequently cited analysis of this type is Garrett Hardin's 1968 article, "The Tragedy of the Commons."[12] Hardin's conclusion, "Freedom in a commons brings ruin to all," summarizes his argument that self-interest propels an individual to seek to maximize his gain earned from a shared resource because the detriment to the resource that results is shared among all members of the community.[13] Studies of individuals' and communities' behavior in a global commons are ongoing, as issues such as pollution, global climate change, and resource scarcity continue to shape the 21st century.[14]

The term "commons" was originally coined by Alfred Thayer Mahan in his study entitled, *The Influence of Sea Power Upon History 1660–1783*.[15] Mahan revolutionized the concept of commerce in warfare through his analysis of hegemonic control of the seas. He states, "The first and most obvious light in which the sea presents itself from the political and social point of view is that of a great highway; or better, perhaps, of a wide common, over which men may pass in all directions."[16] Mahan drew attention to the economic benefits gained from such a passageway through the creation of trade routes and the consequent power projection capabilities a state could reap by dominating seaborne commerce.

In 2003, Barry Posen wrote a seminal piece on the defense and security benefits of unchallenged freedom of operation in the commons entitled, "Command of the Commons: The Military Foundation of U.S. Hegemony."[17] Posen argues that dominance in these shared domains serves as the foundation of the leadership role that the United States holds in the international system. He states, "Command of the commons is the key enabler of the U.S. global power position. It allows the United States to exploit more fully other sources of power, including its own economic and military might as well as the economic and military might of its allies."[18] Posen's work on this topic

brought to the forefront the role that the global commons play as a key enabler of U.S. defense and national security strategies.

Back then, the United States may have felt that it was unrivaled in terms of its ability to exploit the global commons for its own purposes and benefit; today, however, things have changed. The United States' access to the commons, as well as its ability to operate safely within these domains, is increasingly challenged by a broad range of actors. This competition is consequently threatening the United States' and other states' use of the commons for military, economic, and commercial purposes. This ever more apparent trend is evidence of the shifting role of the global commons in defense strategy and tactics; where it once facilitated military operations, it now serves as a means for adversaries to deny U.S. freedom of action and force the United States to engage on the enemy's terms. The United States, therefore, would directly gain from improving security within the global commons, as well as reap the larger benefits that such heightened stability would bestow upon the entire international community.

Strategic Significance of the Global Commons

In the face of the global commons' shifting role, U.S. leaders and policy analysts are reiterating the importance of these domains in international security and U.S. defense. Specifically, political and military leadership is increasingly highlighting the challenges that the United States and the world face within the global commons. In a 2008 speech to the Air War College, Secretary of Defense Robert Gates commented, "Protecting the 21st century's 'global commons'—in particular, space and cyberspace—has been identified and adopted as a key task."[19] In 2009, Under Secretary of Defense for Policy Michèle Flournoy stated, "we also see in some cases the rising tensions in the global commons…and we have a strong economic interest and security interest in keeping those global commons open and free from threat."[20] In a February 2010 briefing with the Chairman of the Joint Chiefs of Staff Admiral Michael Mullen, Secretary Gates emphasized the issue again, saying,

> The Department's leadership now recognizes that we must prepare for a much broader range of security challenges on the horizon. They range from the use of sophisticated, new technologies to deny our forces access to the global commons of sea, air, space, and cyberspace to the threat posed by non-state groups developing more cunning and destructive means to attack and terrorize.[21]

The strategic importance of the global commons to U.S. national defense and international security warrants this high level of attention. As challenges

within these domains continue to emerge, they will demand creative solutions—particularly in the relatively new, man-made domain of cyberspace—and will require international engagement to implement these solutions. The United States has the capacity to lead in this regard and should prioritize developing technology and policy countermeasures to the challenges emerging in the sea, air, space, and cyberspace domains.

Since World War II, the United States has leveraged its political and economic leadership as well as its military strength to lead the way in developing an international system that fosters stability. Relatively unfettered access to the global commons has enabled the United States to move toward an open, globalized economy and closer partnerships with friends and allies. More precisely, the commons have provided for freedom of action for the U.S. military; access to physical infrastructure (such as military bases and logistics centers); availability of timely, highly accurate information and the ability to communicate it quickly; global economic interdependence; and the explosion of international travel. It is these elements, important to every nation around the world, that are increasingly threatened by a number of challenges emerging in the 21st century global commons.

The DoD Capstone Concept for Joint Operations identifies perhaps the greatest challenge to U.S. operations in the global commons in the near future:

> Diminished access will complicate the maintenance of forward presence, a critical aspect of past and current U.S. military strategy, necessitating new approaches to responding quickly to developments around the world as well as more robust exploitation of existing U.S. advantages to operate at sea and in the air, space, and cyberspace.[22]

The development and proliferation of anti-access/area-denial (A2/AD) technologies to an increasing number of states, including potential U.S. adversaries, presents U.S. leaders with what military strategist Andrew Krepinevich calls, "a strategic choice of the first magnitude."[23] Namely, U.S. leaders must decide to either change the way the United States does business or surrender the ability to project power worldwide. These power projection capabilities underpin the openness of the global commons. Krepinevich argues, "While generally underappreciated, the U.S. military's role as the steward of the global commons—the world's oceans in particular—has enabled the free movement of goods around the world, facilitating both general peace and prosperity."[24] Thus, challenges to U.S. power projection capabilities in the maritime, air, space, and cyberspace domains directly threaten the openness of the global commons.

Challenges in the Maritime Commons

One of the dominant ways in which the United States has projected global power is through its naval forces and forward bases; the maritime domain, however, is becoming increasingly contested through the rise of new naval powers, development and proliferation of A2/AD capabilities, and piracy. Forces ranging from globalization to regional-power competition are motivating a number of states around the world to invest in maritime capabilities. Following the 1996 Taiwan Strait crisis, during which the United States moved two aircraft carriers to the Strait as a show of force after Chinese aggression, the Chinese People's Liberation Army (PLA) has prioritized the development of a blue-water navy that rivals the United States'. Additionally, countries including Japan, South Korea, India, and Russia are investing in their naval capabilities.[25]

Ensuring the security of the maritime commons against piracy is another motivating factor of such endeavors.[26] China, for instance, has shown some signs of beneficent intentions by increasing its role in international counter-piracy missions. In 2008, the PLA Navy (PLAN) sent warships to join U.S. naval operators patrolling the Somali Coast. More recently, Beijing has expressed interest in leading some of the planning of such missions.[27] Unfortunately, these positive steps are tempered by concerning Chinese actions with respect to the seas. Specifically, China's assertion of exclusionary rights in its exclusive economic zone (EEZ)—in opposition to UNCLOS treaty provisions and its territorial claims in the South China Sea—heighten suspicion of Chinese intentions in the region.[28] If other states follow suit to prevent safe, unrestricted passage of sea vessels through their EEZ (200 miles from the coastline into a bordering body of water), the openness of the commons is directly challenged and could have devastating economic results.

The development and proliferation of A2/AD capabilities and other advanced military technologies to an increasing number of states presents another important challenge to U.S. power projection capabilities and security within the maritime domain. A number of states are developing sophisticated anti-ship cruise missiles and quiet diesel–electric submarines with wake-homing torpedoes that challenge the U.S. ability to operate in blue water. Furthermore, advanced military technology is enabling states with relatively weaker navies to make unexpected leaps in the development of precision-guided munitions.[29] Thus, the fact that technology is saturating the international market and is increasingly available to a wide variety of actors is empowering potential U.S. adversaries with military capabilities that place them on par with some U.S. military forces.

Potential U.S. adversaries that stand out in their development of such capabilities are China and Iran. Both states continue to make nontrivial investments in A2/AD technology in order to deny the United States use of forward bases and the ability to conduct maritime operations in their respective regions. The Chinese have and continue to develop land-based anti-ship ballistic missiles (ASBMs), anti-ship cruise missiles (ASCMs), air-launched cruise missiles, diesel–electric submarines, and maritime intelligence, surveillance, and reconnaissance capabilities. In a conflict with the United States, these weapons would be brought to bear against U.S. forward based forces at Kadena Air Base on Okinawa as well as the future Andersen Air Base on Guam.[30] Denying the United States the ability to access these bases, particularly if combined with the ability to strike U.S. Navy aircraft carriers with ASBMs, could cripple U.S. military operations in the region.

Similarly, Iran sees the necessity of negating key U.S. advantages in the global commons as critical to success in any military engagement with the United States. Consequently, Iran is working to modernize and augment its arsenal of A2/AD capabilities and refine its methods to debilitate U.S. forces in the Persian Gulf. Iran has a significant mine-laying capability, which presents a threat to larger commercial and military vessels navigating the narrow passageways of the Gulf and the Strait of Hormuz. These anti-ship mines could effectively slow the ships to make them easy targets for attack by land- and sea-based weaponry. The Iranian navy also fields small surface combatants armed with ASCMs and small boats loaded with small arms ranging from man-portable surface-to-air missiles to heavy machine guns and rifles.[31] These capabilities, particularly mines, can present a significant threat to a modern fleet in the shallow, narrow, semi-enclosed waters of the Persian Gulf. Indeed, Iranian leaders can rely upon relatively low-tech weaponry to combat more advanced U.S. forces, especially if they can maintain the element of surprise. However, the presence of anti-ship mines and small boats that may conduct suicide attacks are not only of concern to the United States. Over 90 percent of Persian Gulf oil passes through the Strait of Hormuz,[32] making it a strategic chokepoint whose disruption would have severe consequences for the global economy. Even absent a crisis, this increasing militarization of a waterway that is so critical to global resource distribution is a concern for the international community and a threat to maritime security.

Further jeopardizing this stability are ongoing acts of piracy; in particular, there has been a dramatic uptick in recent pirate attacks and hijackings in the Gulf of Aden and the Horn of Africa. Pirate attacks in the region increased 200 percent from 2007 to 2008. According to the Piracy Reporting Center of

the International Maritime Bureau, there were 214 pirate attacks, resulting in 47 hijackings, in the Gulf of Aden and off the coast of Somalia in 2009.[33] Early this year, the Combined Maritime Forces (CMF) stood up the Combined Task Force 151 specifically for counter-piracy missions. More than twenty nations have contributed assets to the CMF for maritime security operations, including combating the threat piracy poses to commercial and military vessels at sea, and this presence appears to be reducing the number of pirate attacks in the region.[34] There have also been signs, however, of pirates moving to the southern and eastern coasts of Somalia. At this time, piracy is not widespread enough to effectively close the global waterways. However, its persistence even in the face of joint operations, such as those CMF is performing, signifies that piracy presents an explicit threat to commercial trading vessels that could become a more serious challenge if efforts to combat piracy are not ongoing. Piracy exemplifies the broader trend of the empowerment of smaller states and non-state actors in littoral and blue-water operations. In combination with the proliferation of advanced technologies such as long-range, precision-guided missiles, these trends portend a higher degree of danger in the seas unless steps are taken to ensure global security and openness.

Challenges in the Air Commons

The 2009 Christmas Day bombing attempt on a Northwest Airlines flight to Detroit was the third known attempt at air terrorism since the attacks of September 11, 2001. Umar Farouk Abdulmutallab of Nigeria is alleged to have smuggled the explosive material onto the plane and started a fire. The U.S. Embassy in London issued Abdulmutallab a tourist visa in 2008, unaware that his name was on a National Counterterrorism Center (NCTC) terrorism watch list, the Terrorist Identities Datamart Environment (TIDE). Despite the fact that Abdulmutallab's father notified U.S. Department of State officials of his son's extremist views, the suspected bomber's name was never moved from TIDE to the FBI's Terrorist Screening Data Base (TSDB), from which no-fly lists are created.[35] Instances of terrorism on airlines are devastating to an industry already suffering from the current economic crisis. Since 2008, air travel has declined 20 percent.[36] This trend is likely to continue if passengers are afraid to fly or are deterred by intrusive—albeit necessary—security procedures at airports, a possibility that is likely to heighten with the introduction of x-ray screening mechanisms. Although these relatively rare terrorist events are not apt to spell the downfall of the commercial airline industry, threats of suicide bombings, hijackings, attacks on airports, and even surface-to-air attacks continue to lessen public faith in the security of air travel. Citizens worldwide will continue to call upon their governments to reach a balance of ensuring travelers' safety

with appropriate security precautions that protect privacy and cultural sensibilities to the greatest extent possible.

Challenges to openness of the air commons are more directly threatened by the continued proliferation of A2/AD technology and advanced military technology. Chinese advances in these capabilities pose a serious potential threat to U.S. freedom of action in the skies. In the case of a China–U.S. conflict, the PLA would likely aim to render U.S. airbases in the region ineffective, disable land-based aircraft, and deny the United States use of the airspace above Taiwan and the Taiwan Strait. The Chinese are very close to—if not already in possession of—the military capabilities required to achieve these objectives. They would most likely use ballistic missiles, surface-to-air missiles (SAMs), and land-based interceptor aircraft.[37] Against these capabilities, the United States would have difficulty maintaining air superiority. Additionally, U.S. allies who provide support to the forward bases that will be targets of Chinese aggression could possibly withdraw their support during a crisis because of their vulnerability.

Indeed, disputes over access to bases and over-flight rights are challenging the openness of the air commons. Forward-based, overseas military presence is a major element of U.S. military strategy and has enabled U.S. post-Cold War military operations in Iraq, the Balkans, Afghanistan, and elsewhere. Forward bases, however, may be becoming less of an asset and more of a liability as potential U.S. adversaries continue to develop the capabilities needed to strike U.S. allies that host these bases and forward-deployed U.S. forces. A 2006 report from RAND's Project Air Force explains, "…basing and access are likely to become increasingly problematic as host countries fall under credible threat of attack."[38] China is fielding the types of military capabilities that will threaten U.S. reliance on forward bases and access, including short- and medium-range ballistic missiles, a modernized bomber fleet, and strike aircraft.[39] As in the maritime domain, the openness of the air commons is increasingly threatened by the rise of non-state actors and the spread of advanced technologies. Individual and group terrorist attacks on airliners, as well as the promulgation of weaponry and know-how that can limit U.S. power projection capabilities and operations, are global phenomena. Dealing with each in a way that promotes international security will require global solutions. For example, on the terrorist front, global cooperation between the United States and China is needed to ensure mutual maritime security.

Challenges in the Space Commons

The fragility of the space commons is the preeminent challenge to its continued openness. The accidental collision of objects in space or an intentional attack

of a state's space capabilities through the use of an anti-satellite (ASAT) weapon can have highly destructive effects, regardless of the size of the debris with which the satellite collides or ASAT weapon that attacks it. Indeed, the potential for destruction in space is such that if an object the size of a marble strikes a satellite orbiting the Earth, it does so with the equivalent energy of a one-ton object dropped from a five-story building.[40] Increasing congestion only increases the likelihood of such collisions taking place. It is estimated that there are over 18,000 manmade objects in space, including approximately 1,300 active satellites operated by over 40 countries, 10 of which are capable of launching satellites.[41] The sheer volume of objects requires improved space situational awareness to preserve the openness of the domain.

The fragility of the space commons is the preeminent challenge to its continued openness.

In addition, several recent events have spurred the United States to take action to increase the ability of satellites to "see" the area around them. The Chinese use of an ASAT weapon to destroy a weather satellite in 2007 created a larger debris field than any other human event in space.[42] The February 2009 collision of an Iridium communications satellite and an inactive Russian satellite further intensified debris concerns. It is possible that, unless the issue is addressed, debris creation could eventually render space useless. To guard against this possibility, the U.S. Air Force is investing in a number of programs that improve the ability to detect objects around and approaching satellites.[43] The United States currently monitors satellites for risk of collision in space and notifies commercial satellite operators or other governments when there is risk of collision with another satellite or debris.[44] Such efforts, in addition to continued advancements in sensor technology, are critical steps to improving space situational awareness and reducing the probability that new and dangerous debris is created.

The vulnerability of satellites is an especially grievous problem in light of the significant functions this technology performs. Satellites have revolutionized the way that the world transmits and receives information, and they play a critical role in both the commercial and military spheres. Satellites were initially valued for the strategic information they provided to military affairs; today, they are used to provide tactical- and operational-level information to troops on the ground.[45] Satellites provide targeting, reconnaissance, and communications information for offensive and defensive military actions; but they also provide these critical data for humanitarian assistance and disaster relief missions. Satellite images proved invaluable tools to the

responders of the 2008 earthquake in China, 2004 tsunami in Southeast Asia, and countless other relief efforts.[46]

This across-the-board reliance on satellites largely underpins global concerns over ASAT capabilities. On January 11, 2007, China successfully destroyed an inoperative weather satellite using ASAT technology, and they are continuing development of kinetic ASAT capabilities, as well as ground-based ASAT laser systems.[47] This research, in combination with their investments in an expansive space exploration program, could lead to technology that is capable of destroying mid-Earth orbit satellites, including U.S. global positioning satellites.[48] Although their lack of transparency is concerning, China is not the only state in pursuit of advanced space technology. Lasers and jammers that disrupt satellite operations present another serious concern. Instances of past interference include Iraq's jamming of U.S. precision-guided munitions in 2003 and Brazilian interference with transponders on a U.S. Navy satellite in 2008. Iran and Turkey have both jammed satellites to prevent the broadcast of programming from political opposition groups. Iran again jammed satellites during the protests following the 2009 presidential elections, when it blocked out the Voice of America broadcasting.[49] It is clear that a number of challenges to openness in the space domain exist, and that number is on the rise. Further, the lack of an effective, up-to-date governance regime is perpetuating those concerns. For example, China in 2007 and the United States in 2008 violated an informal twenty-two year moratorium on ASAT testing; absent a larger, more formal international legal framework, these activities will continue with little or no consequence for transgressors. Until such steps are taken, issues related to the threat of attack against space assets and the risk of damage to assets from accidental collision will persist; in either case, the extreme result could be an obsolete space domain.

Cyberspace is the most unique domain of the global commons: it is man-made; it facilitates the transfer of information and data rather than people, vessels, and goods; and it is in large part owned by the private sector.

Challenges in the Cyber Commons

During his first year in office, President Barack Obama drew a significant amount of attention to the cyber domain and the need to improve security within it. He identified this digital commons as a "strategic national asset" and stated that, "Protecting this infrastructure

will be a national priority."[50] It will also be a formidable challenge. Cyberspace is the most unique domain of the global commons: it is man-made; it facilitates the transfer of information and data rather than people, vessels, and goods; and it is in large part owned by the private sector. The issue of ownership, in particular, will complicate governance and necessitates a high level of public and private sector cooperation.

Equally pressing to cyber-security is the issue of attribution. The difficulty of pinpointing the source of an attack in the cyber domain has serious implications for deterrence and reprisal. In order to successfully deter an adversary or launch retaliatory attacks, a state must be able to identify the aggressor. Cyber-identification is complicated and the techniques used are underdeveloped, particularly against such methods such as a "false flag" attack, which allows a perpetrator to disguise the origin of an attack. U.S. leaders rightly fear that in this type of opaque and poorly understood environment, any retaliatory steps taken might not be against the true source of the initial attack. Such issues were raised during a cyber wargame with U.S. military leaders in early January 2010. Results of the wargame were void of good news; instead, it was reported that "the enemy had all the advantages: stealth, anonymity, and unpredictability."[51] Priority should be placed on developing new technologies to strengthen attribution of actions in cyberspace. At the same time, U.S. leaders should work with the private sector and international allies to identify norms of behavior and consequences that work to strengthen deterrence of cyber attacks.

What is more, the infrastructure of cyber networks is perhaps the greatest vulnerability for the United States and other developed nations. Deputy Secretary of Defense William Lynn underscored this vulnerability at a recent discussion on cybersecurity: "With 15,000 networks and 7 million computing devices used by our Department, we have formally recognized cyberspace for what it is—a domain similar to land, sea, air and space. A domain that we must depend upon and protect."[52] Lynn pointed out that more than one hundred foreign intelligence agencies have tried to access U.S. networks, and Secretary Gates has admitted that the United States is under virtually constant cyber attack.[53] The threat, however, goes beyond the Defense Department. Critical infrastructure systems, including power grids and transportation systems, are run from a cyber platform. Depending on the scale of the attack, the potential economic, social, and military effects could be profound. Even more threatening is the case where an adversary who launches a series of attacks against the networks that facilitate everyday life, an event that could cause catastrophic physical damage and loss of life.

States such as Russia and China are developing offensive cyber warfare capabilities that could achieve such disruptions, and whose secondary and tertiary effects could lead to significant civilian and military casualties. Russia demonstrated these capabilities in attacks against Estonia in 2007 and against Georgia during the South Ossetia War in 2008. The recent attacks on Google evidence China's wide range of cyber capabilities, as well. Chinese military analysts say that in the case of China–U.S. conflict, the Chinese would use cyber attacks to disable U.S. battle networks at the early onset of the conflict.[54] Successful attacks of this type could effectively achieve a wide range of devastating effects, from disruption of logistics to hijacking of precision-guided munitions. The challenges for achieving security in the cyber domain are significant, and they are complicated by concerns over privacy and individuals' rights. A difficult but necessary task of government is to reconcile the two in order to strengthen cybersecurity; in this effort, the innovation and talent of the commercial sector should be leveraged. Cyber networks facilitate much of the world's activity; protecting these networks, improving their resiliency in case of attack, and developing better methods for identifying attackers should, as the president says, be a highest priority.

Conclusion

The Obama administration is taking important steps to remediate challenges to U.S. power projection capabilities worldwide, and to reverse trends that threaten the openness of the global commons. These initiatives are powerful moves toward the protection of four domains that facilitate the activities of countries all over the world. In pursuing such a path, the President has also reasserted America's position as a leading guardian of international stability and economic interconnectedness. Bipartisan support from Congress and co-operation from U.S. allies abroad are necessary for continued success in these areas, and these groups should bolster their contributions to these efforts.

Twenty-first century global challenges demand global solutions that harness innovation to develop countermeasures and collaboration—between private and public sectors, and among global state and non-state actors—to ensure these threats are adequately addressed. International efforts to modernize and strengthen governance regimes are an important additional step, as international legal frameworks and norms put pressure on states to act in ways that support the global good. By working toward these goals in concert with other nations, U.S. leaders can help ensure the continued openness of the global commons, the literal and virtual foundations upon which international security is pursued, achieved, and protected. Y

–Jason Warner served as the lead editor of this article.

NOTES

[1] Ninety percent of global trade was valued at $14 trillion in 2008. International Maritime Organization, "International Shipping: Carrier of World Trade," 2005, http://www.imo.org/includes/blastDataonly.asp/data_id%3D18900/IntShippingFlyerfinal.pdf (accessed February 26, 2010).

[2] IATA, "Fact Sheet: Economic & Social Benefits of Air Travel," February 2010, http://www.iata.org/pressroom/facts_figures/fact_sheets/economic_social_benefits.htm (accessed February 26, 2010).

[3] Abraham M. Denmark and James Mulvenon, *Contested Commons: The Future of American Power in a Multipolar World* (Washington, DC: Center for a New American Security, 2010), 5.

[4] U.S. Department of Defense, *Quadrennial Defense Review Report*, February 2010, 8.

[5] A recently published study from the Center for a New American Security, *Contested Commons: The Future of American Power in a Multipolar World* (2010), is a notable exception and demonstrates that this type of analysis is newly emerging.

[6] Michèle Flournoy and Shawn Brimley, "The Contested Commons," *Proceedings Magazine* 135, 7 (2009), http://www.usni.org/magazines/proceedings/story.asp?STORY_ID=1950

[7] Some experts argue that the Arctic should be considered the fifth commons as a result of the opening of new sea lanes as Arctic ice melts, and the consequent territorial claims of various states. The United States Department of Defense continues to classify the Arctic as primarily a maritime domain, and the area is not dealt with as a separate commons in this paper. For more information on the changing face of the Arctic and states' territorial ambitions in the region, see Richard A. Kerr, "A Warmer Arctic Means Change for All," *Science* 30 (2002): 1490–1493; Roderick Kefferputz and Claude Weinber, "Safeguarding Arctic Resources," *EuropeanVoice.com*, August 1, 2009, http://www.europeanvoice.com/article/imported/safeguarding-arctic-resources/63567.aspx (accessed February 26, 2010); and Dina Fine Maron, "Canada Will Use Robot Subs to Map Arctic Sea Floor, Boost Territorial Claims," *New York Times*, February 10, 2010, http://www.nytimes.com/gwire/2010/02/10/10greenwire-canada-will-use-robot-subs-to-map-arctic-sea-f-45098.html (accessed February 27, 2010).

[8] Marjorie Ann Browne, "IB95010: The Law of the Sea Convention and U.S. Policy," *CRS Issue Brief for Congress*, February 14, 2001, http://www.cnie.org/nle/crsreports/marine/mar-16.cfm (accessed February 21, 2010).

[9] Denmark and Mulvenon, 15. For example, U.S. airspace and air approaches are guarded, patrolled, and monitored by the United States and Canadian bi-national organization, North American Aerospace Defense Command (NORAD). For more information on NORAD, see http://www.norad.mil/about/index.html

[10] Steve Garber, "Sputnik and the Dawn of the Space Age," NASA History Division, October 10, 2007, http://history.nasa.gov/sputnik

[11] Peter L. Hays and Charles D. Lutes, "Towards a theory of space power," *Space Policy* 23 (2007): 209.

[12] Garrett Hardin, "The Tragedy of the Commons," *Science*, December 13, 1968, 1243–1248.

[13] Ibid, 1244.

[14] Elinor Ostrom of Indiana University is also widely known for her academic study of the commons, for which she won the 2009 Nobel Prize in Economics. To hear Michele Norris' interview of Ostrom on NPR's *All Things Considered*, visit http://www.npr.org/templates/story/story.php?storyId= 113735444 (accessed February 27, 2010).

[15] A.T. Mahan, *The Influence of Sea Power Upon History 1660–1783* (1890; reprinted, New York: Dover Publications, Inc., 1987).

[16] Ibid, 25.

[17] Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* 28 (2003): 5–46.

[18] Ibid, 8.

[19] Robert Gates, Remarks to Air War College, Montgomery, AL, April 21, 2008.

[20] Center for Strategic and International Studies, "Rebalancing the Force: Major Issues for QDR 2010," April 27, 2009, transcript by Federal News Service, Washington, DC.

[21] U.S. Department of Defense, Office of the Assistant Secretary of Defense (Public Affairs), "DoD News Briefing with Secretary Gates and Adm. Mullen from the Pentagon," February 1, 2010, http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4549 (accessed February 27, 2010).

[22] U.S. Department of Defense, Capstone *Concept for Joint Operations Version 3.0*, January 15, 2009, 6.

[23] Andrew F. Krepinevich, *Why AirSea Battle?* (Washington, DC: Center for Strategic and Budgetary Assessments, 2010), 7.

[24] Ibid, 7.

[25] Denmark and Mulvenon, 21.

[26] Ibid, 21.

[27] David Axe, "War is Boring: Mixed Signals from China Point to Security Dilemma," *World Politics Review*, http://www.worldpoliticsreview.com/article.aspx?id=5132 (accessed February 17, 2010).

[28] Vaudine England, "Who's right in South China Sea spat?" BBC News, March 13, 2009, http://news.bbc.co.uk/2/hi/7941425.stm; and "South China Sea," GlobalSecurity.org, April 18, 2010, http://www.globalsecurity.org/military/world/war/south-china-sea.htm

[29] James Kraska, "How the United States Lost the Naval War of 2015," *Orbis* 54 (2010): 35–45.

[30] Krepinevich, 25.

[31] Ibid, 29.

[32] Caitlin Talmadge, "Closing Time: Assessing the Iranian Threat to the Strait of Hormuz," *International Security* 33 (Summer 2008): 82.

[33] Mark McDonald, "Record Number of Somali Pirate Attacks in 2009," *New York Times*, December 30, 2009, http://www.nytimes.com/2009/12/30/world/africa/30piracy.html (accessed February 26, 2010).

[34] Commander, Combined Maritime Forces Public Affairs, "New Counter-Piracy Task Force Established," January 8, 2009, http://www.navy.mil/Search/display.asp?story_id=41687 (accessed February 25, 2010).

[35] Dan Eggen, Karen DeYoung and Spencer S. Hsu, "Plane suspect was listed in terror database after father alerted U.S. officials," *The Washington Post*, December 27, 2009, A01.

[36] Micheline Maynard and Liz Robbins, "New Restrictions Quickly Added for Air Passengers," *New York Times*, December 27, 2009, http://www.nytimes.com/2009/12/27/us/27security.html (accessed February 27, 2010).

[37] Krepinevich, 23.

[38] David A. Shlapak, "Shaping the Future Air Force," *RAND Project Air Force Technical Report* (Arlington, VA: RAND Corporation, 2006): 8.

[39] Krepinevich, 17.

[40] Michael Krepon and Samuel Black, Space Security or Anti-satellite Weapons? (Washington, DC: The Henry L. Stimson Center, 2009), 16.

[41] Dana J. Johnson, "Policies for a Contested Space Environment," Remarks made at the Henry B. Gonzales Convention Center, San Antonio, Texas, January 14, 2010, http://spacepolicyonline.com/pages/images/stories/Johnson_-_AETC_Symposium_Remarks_14_Jan_2010_FINAL.pdf (accessed February 25, 2010); and Krepon and Black, p. 4.

[42] Bates Gill and Martin Kleiber, "China's Space Odyssey," *Foreign Affairs* 86 (2007): 2–6.

[43] Samuel Black and Victoria Samson, Space Security Programs of Interest in the Fiscal Year (FY) 2011 Department of Defense Budget Proposal, http://www.stimson.org/space/pdf/Space_Security_Programs_in_FY11_Budget.pdf ; and Amy Butler, "2011 Funding Request Includes New Sat System," *Aviation Week*, February 11, 2010, http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=defense&id=news/awst/2010/02/08/AW_02_08_2010_p27-202005.xml&headline=2011%20Funding%20Request%20Includes%20New%20Sat%20System

[44] Johnson.

[45] Peter L. Hays and Charles D. Lutes, "Towards a theory of space power," *Space Policy* 23 (2007): 207.

[46] Krepon and Black, p. 10–11.

[47] According to GlobalSecurity.org, a medium range ballistic missile launched a kinetic kill vehicle to destroy the missile. See, "Chinese Anti-Satellite [ASAT] Capabilities," *GlobalSecurity.org*, January 26, 2009, http://www.globalsecurity.org/space/world/china/asat.htm (accessed February 1, 2010).

[48] Krepinevich, 15.

[49] Denmark and Mulvenon, 29.

[50] Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure, The White House, Washington, DC, May 29, 2009.

[51] John Markoff, David E. Sanger, and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *New York Times*, January 25, 2010, http://www.nytimes.com/2010/01/26/world/26cyber.html

[52] William Lynn III, Cyber Threat: Most Perilous Challenge, remarks delivered at a roundtable on cybersecurity, Sydney, February 13, 2010.

[53] "Gates: Cyber Attacks a Constant Threat," *CBS News*, April 21, 2009, http://www.cbsnews.com/stories/2009/04/21/tech/main4959079.shtml (accessed February 28, 2010).

[54] Krepinevich, 16.