JANUARY
2010

Contested Commons: *The Future of American Power in a Multipolar World*

Edited by Abraham M. Denmark and Dr. James Mulvenon
Contributing Authors: Abraham M. Denmark, Dr. James Mulvenon, Frank Hoffman, Lt Col Kelly Martin (USAF), Oliver Fritz, Eric Sterner, Dr. Greg Rattray, Chris Evans, Jason Healey, Robert D. Kaplan

Center for a
New American
Security

Acknowledgments

We would first like to thank our co-contributors Chris Evans, Oliver Fritz, Jason Healey, Frank Hoffman, Robert Kaplan, Lt Col Kelly Martin (USAF), Dr. Greg Rattray, and Eric Sterner for their insights and hard work in developing contributions that directly informed our understanding of the Global Commons. In addition to producing great papers on their specific areas of expertise, their knowledge and advice were essential to the development of the opening chapter.

We would also like to thank the experts at the Center for a New American Security for their helpful comments and excellent suggestions throughout the research and writing of this report. We are especially indebted to CNAS Director of Studies Dr. Kristin Lord for her excellent suggestions and feedback, and to CNAS Senior Military Fellows COL Ross Brown (USA), CDR Herbert Carmen (USN), and Lt Col Jeffery Goodes (USMC) for their key insights and analytic support. Research Associate Brian Burton, Research Assistants Zachary Hosford, William Rogers, and Michael Zubrow, and Joseph S. Nye, Jr. National Security Interns Michael McCarthy, Amanda Hahnel, and Jennifer Bernal-Garcia all provided exceptional support and feedback. Liz Fontaine's creativity, patience, and assistance in the publication process were indispensable.

Over the course of the past several years we have had the good fortune to meet and interact with many capable and impressive national security and defense policy experts at various conferences, seminars, and meetings in Washington and around the world. We only hope that we can offer to them the level of hospitality and openness that they have extended to us as CNAS continues its work in national security and defense policy. We would like to thank and acknowledge the friends, experts, and government officials, both former and current, who offered their valuable insights and critiques as part of the Commons Working Groups listed at the end of this report. We would like to especially thank Shawn Brimley, Dr. Patrick Cronin, Dr. Thomas Ehrhard, and Dr. Thomas Mahnken for their support throughout the development of this report. Of course, we alone are responsible for any errors or omissions.

Cover Image

Cover Illustration by Liz Fontaine, CNAS.

TABLE OF CONTENTS

JANUARY 2010

Contested Commons:

The Future of American Power in a Multipolar World

Edited by Abraham M. Denmark and Dr. James Mulvenon

Contributing Authors: Abraham M. Denmark, Dr. James Mulvenon, Frank Hoffman, Lt Col Kelly Martin (USAF), Oliver Fritz, Eric Sterner, Dr. Greg Rattray, Chris Evans, Jason Healey, Robert D. Kaplan

About the Authors

Abraham M. Denmark is a Fellow at the Center for a New American Security.

Chris Evans is a Senior Consultant at Delta Risk Consulting.

Robert D. Kaplan, a National Correspondent for The Atlantic and a Senior Fellow at the Center for a New American Security, is writing a book on the Indian Ocean.

Jason Healey is the Washington D.C. Office Director for Delta Risk Consulting.

Frank Hoffman wrote his chapter when he was a Fellow at the Foreign Policy Research Institute and the Potomac Institute for Policy Studies. He now works for the Department of the Navy.

Oliver Fritz is the Assistant Director of Strategic Planning at Headquarters, U.S. Air Force.

Lt Col Kelly Martin (USAF) is a Senior Military Fellow at the Center for a New American Security.

Dr. James Mulvenon is Vice-President of Defense Group Inc.'s Intelligence Division and Director of DGI's Center for Intelligence Research and Analysis.

Dr. Greg Rattray is a Partner at Delta Risk Consulting, is Chief Internet Security Advisor at the Internet Corporation for Assigned Names and Numbers (ICANN), and is a member of the Cyber Conflict Studies Association Board.

Eric Sterner is a Fellow at the George C. Marshall Institute.

CHAPTER I:
CONTESTED COMMONS: THE FUTURE OF AMERICAN POWER IN A MULTIPOLAR WORLD

By Abraham M. Denmark and Dr. James Mulvenon

JANUARY 2010

Contested Commons:

The Future of American Power in a Multipolar World

Our overall policy at the present time may be described as one designed to foster a world environment in which the American system can survive and flourish.

— NSC 68: U.S. Objectives and Programs for National Security, April 14, 1950

CONTESTED COMMONS: THE FUTURE OF AMERICAN POWER IN A MULTIPOLAR WORLD

By Abraham M. Denmark
and Dr. James Mulvenon

Executive Summary

The United States has been the primary guarantor of the global commons since the end of World War II. The U.S. Navy and Coast Guard have dissuaded naval aggression and fought piracy around the world, ensuring unprecedented freedom of the seas. The United States led the creation of international agreements on air transportation, enabling the creation of a global air industry. America also forged an international consensus on the openness of space, ensuring all countries with the means to do so can utilize orbital space for scientific, commercial and military purposes. Lastly, research funded by the U.S. government led to the creation of a decentralized network of connections now called the Internet, which connects physically dispersed markets, capital and people.

The United States derives great benefit from open access to these global commons, but so too does the world at large. Indeed, dependable access to the commons is the backbone of the international economy and political order, benefiting the global community in ways that few appreciate or realize. Today, over 90 percent of global trade, worth over 14 trillion dollars in 2008, travels by sea.[1] Civil air transportation carries 2.2 billion passengers annually and 35 percent of all international trade, by value.[2] Governments, militaries and corporations around the world rely on space for communications, imagery, and accurate positioning services, making space a 257 billion dollars industry in 2008.[3] Financial traders in New York City use the Internet to transfer 4 trillion dollars, greater than 25 percent of America's annual GDP, every day.[4]

For the past 60 years, and especially since the end of the Cold War, America's nearly unchallenged military advantage in the global commons has guaranteed their openness and stability. Yet, this dominance is increasingly challenged. New powers are rising, with some adopting potentially hostile strategies and doctrine. Meanwhile, globalization and technological innovation are lowering the threshold for states and non-state actors to acquire asymmetric anti-access capabilities, such as advanced anti-ship cruise missiles, anti-satellite weapons, and cyber warfare capabilities. The decentralization of military power and expanded access to technologies once reserved for superpowers will necessarily contest America's 60-year-old dominance over the global commons and its ability to maintain their openness.

While disturbing on their own, these trends are developing concurrently with America's growing reliance on the commons. Militarily, the United States increasingly relies on the commons to enable many aspects of its operations, from logistics, to command and control, to extended power projection. Economically, the United States depends on the global commons to provide essential services to its citizens, connect its markets to suppliers and customers overseas, and manage billions of dollars of financial transactions.

As threats mount, it is in the interest of the international community to reaffirm its commitment to preserving the openness of the global commons. American military primacy will not dissuade rising powers from acquiring capabilities designed to contest U.S. power on the sea, in the air, in space and in cyberspace. Thus, while the United States should continue to develop military capabilities to ensure it can counter anti-access threats posed by state and non-state actors in the global commons, it must recognize that it cannot and should not protect the commons alone.

This report advocates a new strategy that is firmly grounded in the American traditions of maintaining openness, building institutions and empowering friends and allies. As part of this strategy, the United States should use all elements of national power, and work with its friends and allies, to ensure that responsible states continue to enjoy the ability to operate within the global commons. This renewed commitment to defending the global commons will require not only changes in American policy and posture, but also a coordinated set of international agreements, foreign military and civilian capacity building initiatives, and a network of subnational norms and agreements that support openness and stability while confronting disruption and exclusivity.

Specifically, as part of this strategy, the United States should renew its commitment to the global commons by pursuing three mutually supporting objectives:

- **Build global regimes:** America should work with the international community, including allies, friends, and potential adversaries, to develop international agreements and regimes that preserve the openness of the global commons.
- **Engage pivotal actors:** The United States should identify and build capacities of states and non-state actors that have the will and ability to responsibly protect and sustain the openness of the global commons.
- **Re-shape American hard power to defend the contested commons:** The Pentagon should develop capabilities to defend and sustain the global commons, preserve its military freedom of action in commons that are contested, and cultivate capabilities that will enable effective military operations when a commons is unusable or inaccessible.

Introduction

Dependable access to the commons is the backbone of the international economy and political order, benefiting the global community in ways that few appreciate or realize. Over 90 percent of global trade, worth over 14 trillion dollars in 2008, travels by sea.[5] Every year, 2.2 billion passengers and 35 percent of the world's manufactured exports by value travel through the air.[6] Governments, militaries, and corporations around the world rely on space for communications, imagery, and accurate positioning services, making space a 257 billion dollars industry in 2008 alone.[7] Financial traders in New York City use the Internet to transfer 4 trillion dollars, greater than 25 percent of America's annual GDP, every day.[8] Moreover, any computer in the world with access to the Internet can access and transmit information to any place in the world within seconds, allowing unprecedented connectivity for global social networks, commercial enterprises and militaries.

While the liberalization of global trade laws is a major cause of today's active and robust global market, a fundamental physical openness is also essential. Goods manufactured overseas have to be shipped in large containers on huge cargo ships over vast oceans. The orders for the goods and requisite parts assembled in a factory must be transmitted over networks that constitute the Internet. The container ships carrying goods use satellites to navigate and communicate. These capabilities do not happen by accident—they are the result of decades of effort by governments and private corporations to build a "system of systems" that allows for global commerce. These systems exist within and between the global commons: the high seas, air, space and cyberspace.

The interconnectedness and interdependence brought by the globalized economy contributes significantly to stability and prosperity, allowing people, ideas and capital to freely crisscross the world with little regard for international borders. Globalization has lifted millions out of poverty and given emerging regional powers new influence over their own destinies. Indeed, the 2008 *U.S. National Defense Strategy* claimed that "global prosperity is contingent on the free flow of ideas, goods, and services."[9] Clearly, if the United States and the international community want to sustain this level of globalization, the openness of the global commons must be maintained.

Contemporary American strategists recognize the commons, individually and as a group, as central to American national security interests. The United States regularly updates naval, air and space strategies to detail how the U.S. military should think about each commons. Moreover, President Barack Obama has identified cyberspace as a national security priority, bringing it into the fold as a recognized strategic commons. Taken together, the global commons form "the connective tissue of the international system and of our global society."[10] Secretary of Defense Robert Gates described the American approach toward the global commons as:

> Opening doors, protecting and preserving common spaces on the high seas, in space, and more and more in the cyber world. This presence has offered other nations the crucial element of choice and enabled their entry into a globalized international society. … We stand for openness, and against exclusivity, and in favor of common use of common spaces in responsible ways that sustain and drive forward our mutual prosperity.[11]

Since the end of World War II, the openness and stability of the global commons have been protected by U.S. military dominance and sustained by U.S. political and economic leadership. The U.S. Navy and Coast Guard have dissuaded naval aggression and fought piracy around the world, ensuring unprecedented freedom of the seas. America also forged an international consensus

Since the end of World War II, the openness and stability of the global commons have been protected by U.S. military dominance and sustained by U.S. political and economic leadership.

on the openness of space, ensuring that all countries with the means to do so can utilize space for scientific, commercial and military purposes. The United States drove the creation of international agreements on air transportation, enabling the creation of a global air industry. Lastly, research funded by the U.S. government created a decentralized network of connections now called the Internet, which facilitates the free flow of ideas and connects physically dispersed markets, capital and people. In all these domains, the United States supported political and economic leadership with uncontested military dominance.

The prevailing American approach to the global commons was described and eloquently advocated in Barry Posen's influential 2003 article, "Command of the Commons." Posen argues that command of sea, air and space "provides the United States with more useful military potential for a hegemonic foreign policy than any other offshore power ever had."[12] He paints a picture of American military dominance that was sweeping and uncontested:

> Command of the commons is the military foundation of U.S. political preeminence. It is the key enabler of the hegemonic foreign policy that the United States has pursued since the end of the Cold War. The military capabilities required to secure command of the commons are the U.S. strong suit. They leverage science, technology, and economic resources. They rely on highly trained, highly skilled, and increasingly highly paid military personnel. On the whole, the U.S. military advantage at sea, in the air, and in space will be very difficult to challenge—let alone overcome. Command is further secured by the worldwide U.S. base structure and the ability of U.S. diplomacy to leverage other sources of U.S. power to secure additional bases and over-flight rights as needed."[13]

As a result of this unfettered access to the commons, the U.S. military has dominated all dimensions of conflict. Geography made the United States a natural sea power, and successful exploitation of air, space and U.S. technological prowess made the United States a power in the cyber commons as well. The commons, in turn, serve as a key enabler of the U.S. military and its ability to project power globally. The American military demonstrated its conventional military dominance in the 1991 Persian Gulf War, the 1994 air war over Yugoslavia, the 2001 invasion of Afghanistan, and the 2003 invasion of Iraq. The utilization of satellites and advanced communications technologies empowered the U.S. military to operate with overwhelming speed, coordination, efficiency and destructiveness. For example, as former Secretary of the Air Force Michael Wynne explained, "In World War II, it took 1,500 B-17s dropping 9,000 bombs to destroy a given target. Today, one B-2 can strike and destroy 80 different targets on a single mission using weapons guided by space-based USAF global positioning system signals."[14]

Yet, this dominance is becoming increasingly contested, with significant consequences for the world's access to the commons and the power of the American military. While Posen was correct to argue that American primacy is rooted in its continued access to the commons, some emerging trends suggest that cracks may be appearing in the U.S. military's capacity to maintain command of the commons.

The free flow of capital has facilitated the emergence of a multipolar world, giving rise to new centers of power. While the consequent reduction in poverty has generally been a positive development and a long-sought American objective, some of these new powers have used their newfound wealth to acquire and develop high-end anti-access capabilities that could undermine the openness and stability of the global commons. Globalization and technological advancements have also lowered the threshold for poor states and non-state actors to acquire disruptive military technologies. Some developing nations and non-state actors have acquired and developed advanced military technologies, such as anti-ship cruise missiles and cyber warfare units.

These threats to America's role in the commons coincide with the rise of other challenges that will tax the U.S. military. In fact, some states are developing anti-access military capabilities and exclusionary policies that threaten the very international system that has made them stable and prosperous. Pentagon assessments suggest the United States in the coming decades will confront a greater number of threats, across a broader spectrum of warfare, in a more geographically diverse and challenging number of hotspots, than it has in the past.[15] In addition, the United States will need to maintain existing military commitments to deter and defend attacks on U.S. interests and allies.

At the same time, America's allies are showing less willingness to employ military force. While some states have joined in operations to preserve the maritime commons, many others free ride on American power.

These troubling trends are occurring within the context of an ongoing reduction in the size of America's forward-stationed military forces in Europe, Asia and the Middle East. In 2004, the Department of Defense's Global Posture Review recommended a 35 percent reduction in forward-stationed military personnel, and a 30 percent cut of U.S. military facilities abroad. There are several reasons for these shifts (e.g., changing threats, ongoing operations, technological improvements), not the least of which is a degree of reluctance to permanently station U.S. forces in other nations, particularly in the Middle East and East Asia. While the United States is attempting to revise many of its alliances into broader agreements focused on multilateral and global missions, the declining presence of U.S. military bases abroad will force American military power to become more reliant on an expeditionary, rather than a forward-stationed, posture. In other words, just as the global commons are becoming more contested, the U.S. military will rely increasingly on the global commons for extended power projection.

Taken as a whole, the future security environment will test American leadership.

Taken as a whole, the future security environment will test American leadership. Protecting open access to the global commons will be in high demand, but the capacity of the U.S. military to protect the commons will be challenged by new commitments and an increasingly diverse set of military threats. The status quo, in which the United States is the sole guarantor of the openness of the global commons and other states free ride, is unsustainable.

The status quo, in which the United States is the sole guarantor of the openness of the global commons and other states free ride, is unsustainable.

If states and non-state actors are able to disrupt the commons, the existing international political and economic order will be fundamentally undermined. However, the United States has a unique opportunity to shape the world's approach to the commons. If a larger number of existing and emerging powers can be persuaded to promote the openness and stability of the commons, the international political and economic order will be strengthened.

Despite the emergence of an increasingly complex set of military threats, it is important to remember that it is not America's *absolute* level of power and influence that is falling, but its *relative* power compared to other emerging states.[16] While its dominance may be contested in the coming decades, America's ability to lead remains. The key for the United States will be to recognize both its capabilities and its limitations, and to act now to shape the future security environment in ways that will protect key U.S. interests, as well as interests shared with the international community.

PROTECTING THE CONTESTED GLOBAL COMMONS

Going forward, the United States should develop political and military strategies that take these new realities into account and preserve the openness and stability of the global commons in an age of multipolarity. This report advocates a broad and multi-pronged strategy to preserve the openness of the four global commons: maritime, air, space and cyberspace. This strategy should employ all elements of national power, including diplomacy, strategic public engagement, and economic incentives and disincentives. Military power will continue to play an essential role because militaries worldwide can sustain the commons by promoting access, or they can destroy them by enforcing exclusivity or rendering a commons unusable. The U.S. military, for its part, should be prepared to sustain and defend the global commons.

This strategy should be firmly founded in the best traditions of American institution-building and with the recognition that the United States can no longer protect the commons alone. Specifically, the United States should develop and enable an international order which, in turn, nurtures a loose set of international agreements and regimes among responsible and like-minded states that effectively preserves the openness and stability of the global commons. Although America's "unipolar moment" may be fading and its military dominance becoming increasingly contested, the need for American leadership is as strong as ever.

To support this strategy, the United States should re-commit to three traditional pillars of American foreign policy: preserving American leadership, projecting American power as necessary, and promoting alliances and partnerships.

Preserving American Leadership: American leadership in the coming decades will depend on Washington's ability to adapt to an era in which American military primacy throughout the global commons will be contested. Rising and revanchist powers are investing heavily in naval, air, space and cyber power; non-state actors are also gaining access to advanced anti-access military capabilities. The United States must be prepared to lead in a world in which its dominance is also contested politically in a world where other powers demand influence on and within the world's common spaces.

Projecting American Power: American power faces a critical paradox: the United States requires the ability to project military power anywhere, but the use of forward bases in the key regions in the world come at considerable strategic cost.[17] Thus, throughout the world — from the Middle East to Africa to East and South Asia — the United States needs to retain the ability to persistently project power without provoking resentment. It is therefore vital that America develop flexible basing and access options that do not require large and politically costly forward bases, but can support sea-based power projection. As Robert Kaplan notes, "Carrier strike groups, floating in international waters only a few miles offshore, require no visas or exit strategies."[18] Further, as cyber power emerges as a form of warfare, options to project power from cyberspace with a minimal overseas footprint could develop.

Promoting Alliances and Partnerships: Working with and through allies and partners will be key to America's ability to develop an effective international community that can share the responsibility of maintaining the global commons with the United States. These partnerships reinforce America's position as a global leader.[19] The 2007 maritime strategy recognizes this fact, and identifies the imperative for the Navy, Marine Corps and Coast Guard to "foster and sustain cooperative relationships with more international partners."[20] Such an approach can and should be pursued in all commons.

ABOUT THIS REPORT

To inform this report, the Center for a New American Security (CNAS) commissioned four papers designed to explore specific aspects of the contested commons. Each paper was reviewed by a separate commons working group, which was composed of leading experts from academia, the government, the military and the private sector (see the Appendix: Contested Commons Working Groups). In addition, CNAS Senior Fellow Robert D. Kaplan contributed a case study on the future maritime security environment in the Indian Ocean to illustrate how one area of the global commons could become contested. These papers directly informed this chapter, which presents a comprehensive assessment of the global commons, the threats to American interests in those commons, and strategies to address them.

Overview of the Global Commons

There are four major global commons: maritime, air, space and cyberspace. Each commons is fundamentally different from the others. However, this report examines them together as a global commons because they share four broad characteristics:

1. They are not owned or controlled by any single entity.

2. Their utility as a whole is greater than if broken down into smaller parts.

3. States and non-state actors with the requisite technological capabilities are able to access and use them for economic, political, scientific and cultural purposes.

4. States and non-state actors with the requisite technological capabilities are able to use them as a medium for military movement and as a theater for military conflict.

Academics have long studied "the commons," though primarily as shared properties or resources that pose challenges for societal resource management. While that examination can be traced back to commentary by the likes of Thucydides and Aristotle,[21] contemporary academic investigation of the commons was catalyzed by a seminal 1968 article, "The Tragedy of the Commons," by the ecologist Garrett Hardin.[22] Hardin described a hypothetical common pasture in which local herdsmen graze their cattle. Although each herdsman relies on the pasture to sustain his cattle, Hardin argues that each herdsman is individually motivated by self-interest to increase the size of his herd. This action, repeated by every herdsman with the means, quickly leads to overgrazing and the destruction of the pasture. Thus, to quote Hardin's bleak conclusion, "Freedom in a commons brings ruin to all."[23]

To overcome the tragedy of the commons, theorists point to several potential means of governance:

- Hardin proposed the establishment of control by a central authority and/or commercialization of common property, either of which could overrule the self-interest of individuals.
- American economist Mancur Olson proposed that smaller groups are more capable of cooperation than larger groups, as it is easier to share values and responsibilities with a smaller set of actors.[24]
- International relations theorist Robert Keohane argued that a "hegemonic" power can establish international regimes that facilitate international cooperation, but these regimes can remain effective after periods of hegemony have ended.[25]
- Elinor Ostrom, who received the 2009 Nobel Prize for Economics for her work on the commons, argues that self-governing institutions, properly constructed, can play a lead role in maintaining resources.[26] For Ostrom, a key to lasting governance of the commons is the ability to deny benefits of the commons to states that violate its rules and norms.

These perspectives suggest that the United States, as the "hegemonic power," has an opportunity to develop international institutions that last beyond its "hegemonic period." By engaging a set of like-minded states and non-state actors with the ability or potential to substantially contribute to the health and success of the global commons (referred to in this study as "pivotal actors"), the United States could build and lead an international effort to protect the global commons. Moreover, by firmly opposing efforts by those who would undermine the openness and stability of the global commons, the United States and its partners will give challengers new incentives to contribute to the health and openness of the global commons.

THE STRATEGIC GLOBAL COMMONS

Parallel to this academic focus on the commons, strategists have pointed to the commons as the primary channels through which commerce, militaries, people and ideas travel. The concept was probably first coined in 1890 by the famed naval strategist Alfred Thayer Mahan, in his influential work *The Influence of Sea Power Upon History, 1660 – 1783*:

> 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, but on which some well-worn paths show that controlling reasons have led them to choose certain lines of travel rather than others. These lines of travel are called trade routes; and the reasons which have determined them are to be sought in the history of the world [emphasis added].[27]

As technologies advanced, new commons have become accessible. The birth of the airplane made it possible for people and goods to travel across continents and over oceans in a matter of hours, with the effect of bringing the most far-flung parts of the world closer together in terms of time, if not space. The advent of high-thrust rocketry during and after World War II allowed for the use of space for several applications, including international communications at the speed of light and ever-present satellite observation. Most recently, the digital revolution spurred the development of the Internet, enabling the transfer of vast amounts of information across the Earth in a matter of seconds.

Table 1

MILITARY COMPARISONS OF THE GLOBAL COMMONS[28]

	MARITIME	AIR	SPACE	CYBER
Strategic Advantages	Enables global power projection	Allows direct strikes against enemy forces and centers of gravity	Creates a new high ground; enables global imaging and communications	Enables fast transfer of information; finely coordinated military operations; force multiplier, especially for non-state actors
Speed and Scope of Operations	Slow transit over long distances; enables global strikes	Fast, global transit. Scope dependent on sortie rates close to targets	Allows for continuous global operations; detailed C3ISR; precision strike	Extremely fast global operations; automation of command and control
Examples of Key Features	Sea lanes, straits, canals, sea ports	Airports, air ceilings, English language commercial standard, basing and over-flight access	Orbit slots, Lagrangian points, space ports	**Physical:** submarine cables and their landing stations, Internet exchange points, corporate data centers, infrastructure nodes; **Logical:** TCP/IP standard, highly-connected web nodes

The global commons all have distinct military applications and implications, in addition to their importance to the global economy (Table 1).

The maritime, air, and space commons are based (to varying degrees) on a conceptual foundation that facilitates international cooperation by defense and commercial establishments, as well as a set of global regimes that regulate behavior within, and open access to, the commons. The maritime and air commons are the most mature, with robust intellectual and institutional frameworks. The space commons is less mature, with governance that is limited and dated. The cyber commons is largely anarchic, with an amalgamation of multilateral, national, and non-state agreements that have all had limited success in governance and regulation.

The characteristics of each of the commons should not obscure their fundamental similarities. Indeed, their fundamental interdependence is what binds them. In many ways, the global commons only functions effectively because each aspect is utilized simultaneously. To provide just one example, American aircraft carriers — the most potent symbol of American military power — sail on the high seas, use satellites for communications and positioning, use the air for combat and patrol, and

The characteristics of each of the commons should not obscure their fundamental similarities.

leverage cyberspace to transfer data quickly inside the ship and to ground stations around the world. Just one ship, therefore, uses all of the commons in one voyage.

The following sections summarize key characteristics of each of the global commons, with particular attention to the strategic importance of each.

THE MARITIME COMMONS[i]

The maritime commons includes 139 million square miles of ocean, ports and the littoral corridors that connect widely dispersed markets and manufacturers around the globe. Goods produced in Asian or American factories, or oil extracted from Middle Eastern oil fields, require the openness of this commons in order to deliver their goods to customers around the world. With 90 percent of global commerce traveling by sea, and many countries (for example, China and Japan) relying on maritime shipping for critical energy supplies, the openness of the maritime commons is essential to a healthy international economic system and is vital to the national security interests of the United States and its allies. As articulated in the United States' 2005 *National Strategy for Maritime Security,* "The right of vessels to travel freely in international waters, engage in innocent and transit passage, and have access to ports is an essential element of national security. The free, continuing, unthreatened intercourse of nations is an essential global freedom and helps ensure the smooth operation of the world's economy."[29]

The maritime commons has been central to trade and military power since antiquity. Mahan emphasized the close link between maritime power and economic development, and the application of sea power to sustain geopolitical influence. He recognized that whoever controlled the commons had great leverage and could exploit it to preserve the peace and exert influence. Another leading naval theorist, Julian S. Corbett, focused on the importance of sea lines of communication, and described a strategy now known as *sea control.*[30] The openness of the maritime commons today depends to some degree on the security of key ports of entry and vulnerable straits. About 75 percent of the world's maritime commerce passes through a handful of international straits and canals, which function as choke points.[31]

The importance of the openness of the maritime commons has been enshrined in a series of international agreements, most notably, the UN Convention on the Law of the Sea (UNCLOS). This agreement defines acceptable claims of sovereignty in the oceans, identifies the rights and responsibilities of coastal states, and preserves the rights of states to operate peacefully within international waters. Other agreements detail accepted rules of behavior and standardize forms of communication at sea. To date, UNCLOS has been a tremendous success of international institution building — 158 countries, and the European Union, have joined the Convention. Although the United States signed UNCLOS in 1994, the agreement has not yet been ratified by the Senate. Nevertheless, the United States operates according to its main provisions and regards it as customary international law.

THE AIR COMMONS[ii]

Open access to the air is a foundation of the global economy. The air commons see more than 2.2 billion passengers annually.[32] In 2006, air transport facilitated the movement of 35 percent by value

[i] The views expressed in this section are derived from Frank Hoffman, "The Maritime Commons in the neo-Mahanian Era," *Contested Commons: The Future of American Power in a Multipolar World* (January 2010) 49 – 75.

[ii] The views expressed in this section are derived from Lt Col Kelly Martin and Oliver Fritz, "Sustaining the Air Commons," *Contested Commons: The Future of American Power in a Multipolar World* (January 2010) 77 – 103.

(3.5 trillion dollars) of the world's manufactured exports, as well as over 40 percent of the world's international tourists, which accounts for 3.4 percent of global GDP. The air transport industry directly employs 5.5 million people and indirectly brings about 32 million jobs worldwide.[33]

Since World War I, air power has been a fundamental aspect of military power. Air power allows a military to overcome geographic obstacles on the battlefield, at speeds that minimize the distance between the air bases and the battlefield, given sufficient air-refueling capabilities. The scope and speed of air power allows countries to influence a conflict at the strategic and tactical levels from positions around the world. Contemporary American theorists on air power emphasize the importance of it in influencing an enemy's leadership and in striking the enemy's military.[34] While a decades-old debate about the ability of air power to influence events on the ground continues to rage, the U.S. military views air superiority as critical enough to warrant the expenditure of billions of dollars.

The air commons today represents a "mature" commons. Use of the air for commercial purposes is managed effectively by a series of international organizations and bilateral agreements, all of which are largely unseen by the casual traveler. States exercise unquestioned authority over their airspace up to 60,000 feet in their geographic borders, plus 12 miles out from their coastlines. Despite a successful set of international standards and bilateral access agreements, a single international agreement on access and over-flight continues to elude the international community. International air travel agreements today remain almost entirely bilateral, leading to inconsistencies and inefficiencies in the system. That being said, access is generally open, and limitations on access usually result more from internal challenges than external threats.

In many ways, the global commons only functions effectively because each aspect is utilized simultaneously.

The U.S. military has embraced a strategy of preserving the military advantages necessary to maintain air superiority during conflict. Secretary of Defense Gates claimed that by 2020, "The United States is projected to have nearly 2,500 manned combat aircraft of all kinds. Of those, nearly 1,100 will be the most advanced fifth-generation F-35s and F-22s. China, by contrast, is projected to have no fifth-generation aircraft by 2020. And by 2025, the gap only widens."[35]

THE SPACE COMMONS[iii]

Satellite-based positioning information, overhead imagery and communications facilitate global coordination of commercial, scientific and military activities with a degree of speed and precision that would be impossible without the use of outer space. In general, space can be understood as a utility that lies at the heart of other international activities. For example, signals from the Global Positioning Satellite (GPS) system not only help users navigate the surface of the planet, but they also can help to precisely time financial transactions around the world. Militarily, space provides the "strategic high ground" from which global communications and remote sensing can be quickly transmitted to militaries around the world. A military that can effectively use space has a tremendous advantage in terms of speed of communications, breadth of surveillance and intelligence, and accuracy of positioning and timing.

[iii] The views expressed in this section are derived from Eric Sterner, "Beyond the Stalemate in the Space Commons," *Contested Commons: The Future of American Power in a Multipolar World* (January 2010) 105 – 135.

Space's *militarization*—its use as a medium to support military operations—has existed for more than four decades. Since the height of the Cold War, satellites have monitored nuclear tests and other military activities and facilitated global communications, mapping, and other activities with both military and scientific purposes. Yet space has yet to be *weaponized*, in that it is not yet a theater for warfare or for the placement of arms, and it remains a global commons open to any actor with the means to access it.[36]

To a large degree, this openness can be credited to a robust set of international agreements that effectively codify space as a global commons. When space first became accessible to humanity in the 1950s, the United States proposed an agreement establishing orbits as common spaces beyond traditional conceptions of sovereignty. The Soviet Union initially disagreed, arguing that its sovereign claim over its territorial air space extended to orbit and beyond. Once Moscow saw the benefit of sending satellites into orbit to spy on the West, its conceptions of its sovereign interests changed, and the USSR agreed to establish space as, in effect, a global commons. Although several arms-control agreements helped to solidify space as a commons, the most comprehensive existing international agreement on the use of space is the 1967 Outer Space Treaty. It defines space as an area beyond claims of state sovereignty, but it has a limited focus on military matters—beyond banning weapons of mass destruction in orbit or on any celestial body, and prohibiting the use of celestial bodies for military bases or the testing of weapons.

U.S. policy has consistently embraced space as a global commons "by all nations for peaceful purposes and for the benefit of all humanity."[37] Yet the United States has also defended space as a legitimate medium for defense and intelligence activities. The 2006 National Space Policy reinforced an American commitment to the "exploration and use of outer space by all nations for peaceful purposes, and for the benefit of all humanity," rejected claims of national sovereignty, and reaffirmed the "rights of passage through and operations in space without interference." On the issue of military objectives, it was quite clear, asserting:

> The United States considers space capabilities—including the ground and space segments and supporting links—vital to its national interests. Consistent with this policy, the United States will: preserve its rights, capabilities, and freedom of action in space; dissuade or deter others from either impeding those rights or developing the capabilities intended to do so; take those actions necessary to protect its space capabilities; respond to interference; and deny, if necessary, adversaries the use of space capabilities hostile to U.S. national interests.[38]

THE CYBER COMMONS[iv]

Cyber space is now an integral part of modern life. People interact, cooperate, and compete through a series of networked linkages that span the world. This unique system has evolved into a global commons. Through a combination of simple web-based communications and more complex infrastructure networks, the cyber commons enables private and public institutions to provide essential services such as energy, food, and water. Banks and asset traders use the Internet to shift billions of dollars within seconds. Modern militaries—especially the U.S. military—employ the cyber commons as a key enabler of military operations, using both commercial and private networks for everything from command and control to logistics support.

As the newest and least-understood global commons, a more robust discussion on the nature of the cyber commons is necessary. Its speed

[iv] The views expressed in this section are derived from Dr. Greg Rattray, Chris Evans and Jason Healey, "American Security in the Cyber Commons," *Contested Commons: The Future of American Power in a Multipolar World* (January 2010) 137-176.

and scope creates advantages and challenges. Communications across cyberspace can happen near instantaneously, and vast amounts of data can rapidly transit vast distances, often unimpeded by physical barriers and political boundaries. However, dependence on the use of cyberspace creates vulnerabilities and weaknesses that could be exploited by adversaries.

To date, the United States and the international community have had little success in governing the cyber commons. In many respects, governance in cyberspace resembles the American Wild West of the 1870s and 1880s, with limited governmental authority and engagement. Users — whether organizations or individuals — must typically provide for their own security. Much of cyberspace operates outside the strict controls of any hierarchical organizations. No one individual or entity is in charge. Internet traffic is routed through peer arrangements between Internet Service Providers (ISPs), without central authority or control. The resolution of domain names fundamental to web browsing and e-mail is strictly based on an agreed set of protocols, loosely coordinated by a nongovernmental organization referred to as the Internet Corporation for Assigned Names and Numbers (ICANN).

Further challenging any effort to govern or control the cyber commons is the complexity of its ownership — the physical infrastructure of the cyber commons is largely owned and controlled by the private sector. States do not, and cannot, command the cyber commons to the same degree as the sea or air, or even to the extent that they controlled communications technologies in the past. Today, there are myriad providers of devices, connectivity and services in loosely woven networks with open standards. Many governments, especially in the western world, have a limited ability to control cyber activities that originate within their borders. To date, the American approach to cyberspace has been supportive of a cyber commons that is open and market-based.

This condition of anarchy is not absolute. Economic imperatives and the desire to widen and standardize communication networks have led to the creation of relatively public and transparent nongovernmental operations of the Internet Engineering Task Force (IETF), ICANN, and other organizations for standardization, governance and regulation of cyberspace. States and other organizations can also establish boundaries by making choices in how to employ hardware, software and standards. To date, America has supported a cyber commons that is open and market-based.

The United States has also come to realize the strategic value of the cyber commons. Late in the Bush administration, in 2008, a Comprehensive National Cyber Security Initiative was formulated and launched, codified in NSPD-54/HSPD-23. Early in the Obama administration, a White House-led review of cyberspace policy identified cyberspace as a "national asset" and committed the United States to a concerted effort to secure its infrastructure from attack. A few months later, the U.S. military established Cyber Command, charged with protecting networks and conducting offensive cyber warfare. Beyond the Department of Defense, national cyber security efforts have included the National Security Agency, the Department of Justice and the Department of Homeland Security.

Challenges to the Global Commons

In the coming decades, the United States will face a more diverse set of threats, from a broader array of actors, than ever before. As new powers rise and globalization lowers the threshold for less-advanced nations and non-state actors to acquire cheap yet advanced military technologies, the openness of the global commons, and America's traditional military dominance therein, will become increasingly contested.

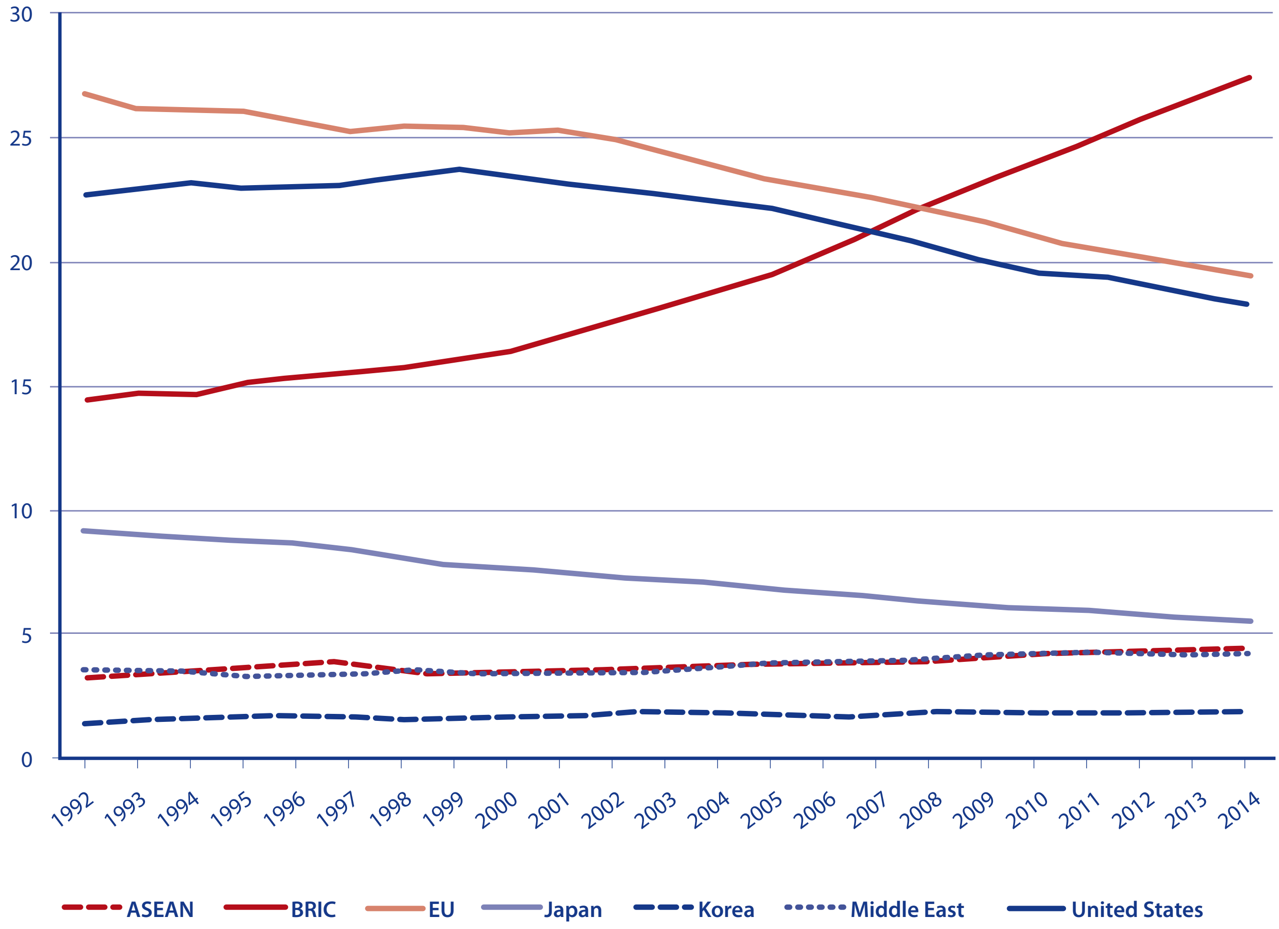
THE COMING MULTIPOLARITY

There is an emerging consensus that the dynamics of the international system are gradually but fundamentally evolving.[39] Since the end of the Cold War, globalization has connected previously separated nations and markets, leading to an unprecedented creation of global prosperity and the rise of new economic powers such as China, India, and others. Since 1999, the United States' share of global GDP has declined, while that of Brazil, Russia, India, and China (BRIC) has increased (see Figure 1). By 2014, the International Monetary Fund predicts that BRIC countries will represent more than 27 percent of global GDP, and the United States and the EU will represent less than 20 percent each.[40]

In his book *The Post-American World*, Fareed Zakaria eloquently described the "rise of the rest" as a broad trend of economic growth throughout the developing world:

> In 2006 and 2007, 124 countries grew their economies at over 4 percent a year. That includes more than 30 countries in Africa. Over the last two decades, lands outside the industrialized West have been growing at rates that were once unthinkable. While there have been booms and busts, the overall trend has been unambiguously upward. Antoine van Agtmael, the fund manager who coined the term "emerging markets," has identified the 25 companies most likely to be the world's next great multinationals. His

Figure 1: Percentage of World GDP (1992 – 2014).[41] 2007 – 2014 data is projected.



> list includes four companies each from Brazil, Mexico, South Korea, and Taiwan; three from India, two from China, and one each from Argentina, Chile, Malaysia, and South Africa. This is something much broader than the much-ballyhooed rise of China or even Asia. It is the rise of the rest — the rest of the world.[42]

Despite an emerging consensus that international power dynamics are changing, there is little agreement as to what the future world will look like. Indeed, America's leading strategic thinkers demonstrate uncertainty about the security environment. Some, like Council on Foreign Relations President Richard Haass, foresee a world in which American power is in relative decline and states themselves are forced to share power with non-state groups and empowered individuals.[43] Princeton University's Dr. G. John Ikenberry argues that Americans continue to live "in an extraordinarily benign security environment."[44] The Carnegie Endowment's Robert Kagan argues that "nationalism in all its forms is back … and so is international competition for power, influence, honor, and status."[45]

Regardless of the specific form one believes the future world will take, it is clear that the international system of the new millennium is evolving toward, or returning to, a more complex environment.[46] As new powers rise, they may develop interests and perspectives on the global commons that differ from those of the United States. Moreover, in a multipolar world, the United States will be increasingly forced to consider the preferences of other powers.

THE GLOBALIZATION OF THREATS

This shift in relative economic and political power is driving a change in the global balance of military power. A combination of economic growth and a relatively stable and benign security environment has allowed state and non-state actors to enhance their military capabilities. While several states are building traditional complements of blue-water navies, more modern land armies, and advanced air forces, certain actors are focusing their military modernization efforts on capabilities tailored to undermine traditional U.S. military advantages.

For the first time since the end of the Cold War, challengers seek to prevent the use of the commons to extend American military dominance.

For the first time since the end of the Cold War, challengers seek to prevent the use of the commons to extend American military dominance. After careful analysis of American war-fighting practices in the 1991 Persian Gulf War and subsequent wars in Yugoslavia, Afghanistan, and Iraq, potential adversaries recognize that, in all of these wars, the U.S. military depended on its access to, and use of, the global commons. This dependence on the commons is a vulnerability that, if exploited, could render the U.S. military less potent and easier to deter or defeat. Specifically, potential adversaries have identified the U.S. military's reliance on long logistics chains and regional bases, on space-based communications and imagery, and on digitized communications networks as key vulnerabilities whose loss would significantly undermine America's ability to fight.

To take advantage of American vulnerabilities, adversaries are developing two general types of capabilities:

- Low-End Distributed Threats: Capabilities and tactics generally utilized by insurgencies and guerilla movements, in which the adversary denies the dominant power a direct confrontation.

- High-End Asymmetric Threats: Capabilities and tactics tailored to undercut the traditional military advantages and enabling capabilities of the dominant power.

In each case, America's potential adversaries hope to avoid military confrontation where America is strongest and focus on areas where the United States is vulnerable — often within the global commons.

Another troubling component is what some American strategists have identified as the emergence of "hybrid warfare," in which an adversary combines the structure and tactics of insurgencies with high-end technologies that are employed to target and undercut traditional advantages of a conventional, modern military force. In the summer 2006 war in Lebanon, Hezbollah utilized advanced battlefield tactics and weaponry, including the successful use of an advanced ground-to-ship missile and anti-tank weapons, along with unconventional command and control and suicide bombers.[47] The Israeli experience in Lebanon has become a textbook case of the kind of hybrid warfare that some defense analysts believe will be a defining feature of the future security environment.[48]

THE CONTESTED COMMONS

Rising powers and broader access to potent new technologies give potential adversaries the ability to contest the openness of the global commons, with profound consequences for the maintenance of American military dominance and the persistence of an open international system. This section will detail threats and vulnerabilities in the maritime, air, space and cyber commons and how those vulnerabilities could challenge the U.S. military and the openness of the global commons in the coming decades.

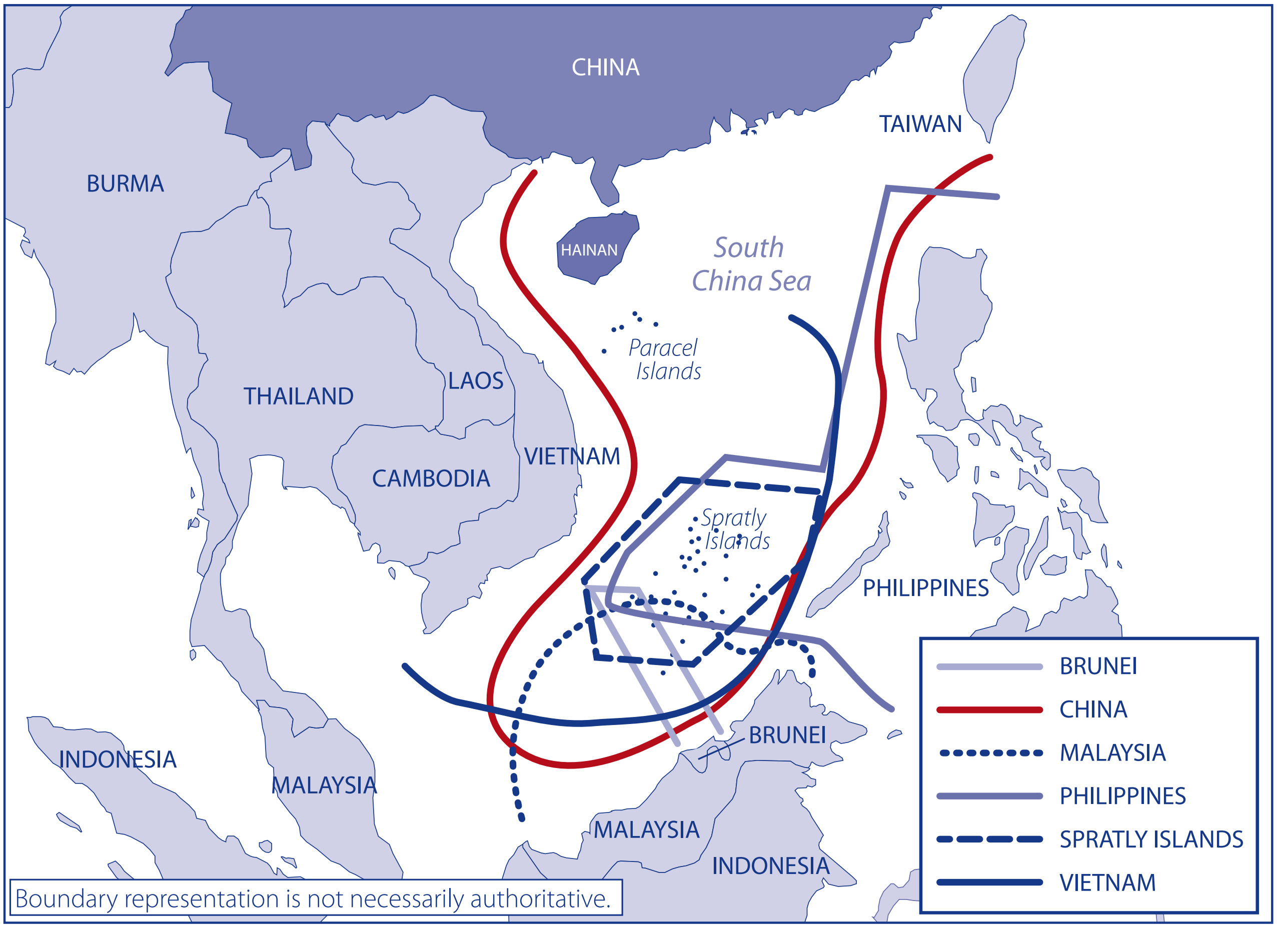
Maritime

As the oldest and best understood commons, the maritime domain possesses elements of all attributes needed to support its openness and stability. There is a well-recognized norm and tradition supporting the freedom of the seas, and international law protecting the openness of the maritime commons is robust and widely recognized. However, diplomatic challenges to the existing legal regime are emerging. Moreover, the rise of new and revanchist naval powers, the development of non-state and hybrid maritime threats, and the effects of global climate change threaten to undermine the mix of international law and American dominance that has preserved the maritime commons since the end of World War II.

Shrinking Diplomatic Space: While international acceptance of UNCLOS is a boon for the openness of the commons, codification does not mean that all states agree on the interpretation of the Convention, as illustrated by several competing claims of sovereignty in the South China Sea. Six countries claim all or part of the South China Sea and have attempted to use UNCLOS to justify their claims. Several of the disputing countries, China being the most egregious example, have attempted to exaggerate UNCLOS's meanings to extended territorial borders (Figure 2). In the case of China, it claims territorial borders more than a thousand miles from the Chinese mainland.

As defined in UNCLOS, a state maintains sovereign control of coastal waters out to 12 miles beyond its beach, and the sole right to extract resources as much as to 200 miles from its shores. The area between 12 and 200 miles is known as the Exclusive Economic Zone (EEZ). As stated in UNCLOS, the EEZ remains an international waterway through which warships may make innocent passage. Yet China claims that states must first obtain permission from Beijing before transiting its EEZ, in direct contradiction to the letter of UNCLOS and the spirit of traditional laws of the

Figure 2: Conflicting Claims in the South China Sea.[49]



Boundary representation is not necessarily authoritative.

sea. Similar reading of international law by Beijing has already contributed to tension with the United States, as the 2001 EP-3E incident and the 2009 USS *Impeccable* encounter demonstrated.

The implications of this interpretation are profound. If states are able to determine who is able to sail in what have traditionally been international waters and exclude whatever maritime traffic at will, the openness of the maritime commons would be challenged. Navies would be forced to request permission before sailing through what would normally be international waters, in effect extending sovereign claims 200 miles beyond the coastline. The openness of the maritime commons demands freedom of navigation within EEZs, and restrictive interpretations of UNCLOS would fundamentally undermine that openness.

Rising Naval Powers: Advanced naval capabilities, and weapons that could be used to deny access to the maritime commons, are spreading to new state actors. Rising powers such as China, India, Russia, Japan and South Korea continue to invest heavily in naval capabilities, portending a future with many blue-water navies on the high seas. These rising maritime forces have already achieved startling successes, including improvements in submarine capabilities, surface fleets, and, in the case of China, ballistic missiles designed to attack major ships at sea.

The rise of new and revanchist naval powers, some with unclear intentions regarding longstanding norms and regimes, raises serious questions about the future of the maritime commons.

A key variable is how these new capabilities are used. As discussed above, the preservation of a globalized economic system and the openness of the global commons should be in the interest of the international community. Some resurgent naval powers, such as South Korea and India, are clearly developing naval capabilities in order to protect the openness of the commons. They speak of their burgeoning naval powers as important contributors to the international system, and they envision employing them in counter-piracy and other operations. Other states, such as Russia and China, are much more circumspect about the purposes envisioned for their growing navies. China's counter-piracy operations off the coast of Somalia are encouraging, however, China's insistence on an exclusionary definition of its rights over EEZs, its behavior toward foreign vessels in the international waters of the South China Sea, and its development of anti-ship ballistic missiles, suggest a different vision of the maritime commons.

The rise of new and revanchist naval powers, some with unclear intentions regarding longstanding norms and regimes, raises serious questions about the future of the maritime commons. Such powers will test the ability of the United States and its allies to maintain open access to the world's oceans. In addition, with some projecting a mid-term future of several blue-water navies, America's ability to sustain maritime dominance is open to question.[50]

Threats from Maritime Armed Groups: Other threats to the maritime commons originate from non-state actors, referred to in this study as Maritime Armed Groups (MAG). Increases in the incidence of piracy, and rare but notable acts of maritime terrorism and insurgency from the sea, have garnered more attention in recent years.[51] Although worldwide rates of piracy have actually fallen since the early 2000s, the average annual rate of pirate acts remains about 300 per year.[52] While piracy tends to occur in narrow straits, the Gulf of Aden and the Horn of Africa have recently emerged as a new hotspot for pirates, accounting for 37 percent of pirate attacks in 2008.[53]

In addition to piracy, maritime terrorism—though rare—has succeeded in the past. Al Qaeda's successful attack on the USS *Cole* in Aden in October 2000 is the most well-known example. Others include al Qaeda's somewhat successful October 2002 attack on the oil tanker MV *Limburg*, which was rammed by a small suicide boat in the Arabian Sea off of Yemen. Nigeria's insurgent group, the Movement for the Emancipation of the Niger Delta (MEND) has proven to be effective at mounting riverine and littoral operations, having attacked oil facilities 75 nautical miles from the coast. These attacks slowed energy shipments from West Africa, which is the source of about 15 percent of American oil imports. Before its defeat, the Tamil Tigers, or LTTE, in Sri Lanka possessed a substantial navy, which attacked targets in the brown, green, and even blue waters around the island.

At this time, threats posed by MAGs do not present significant threats to the maritime commons. While these threats will spur some tactical adjustments, they do not yet have the ability to threaten the global commons with any degree of scope or persistence. Yet, the potential exists for these groups to escalate and coordinate their actions to threaten the maritime commons.

Hybrid Maritime Threats: State and non-state actors have the ability to bring hybrid warfare to the maritime commons. The war between Hezbollah and Israel in summer 2006 saw Hezbollah's successful incorporation of a maritime dimension. Hezbollah fighters used an Iranian-supplied anti-ship cruise missile, probably a Chinese variant of the C-802 *Silkworm*, to strike an Israeli corvette that was not aware of the need to activate its missile defense system. While terrorist groups like Hezbollah have yet to develop the ability to sustain threats against the maritime commons or press them beyond the littoral waters of the Middle East, their ability to acquire and successfully employ advanced anti-access capabilities is an example of a lowering threshold for the acquisition of disruptive technologies, and may be a harbinger of future developments.

With its ability to use a small fleet of frigates and fast patrol craft, along with submarines, mines, and advanced anti-ship cruise missiles, Iran also represents a hybrid threat. Iran's coastline and 17 islands in the Persian Gulf are a strategic choke point in the maritime commons and a potential challenge to the U.S. military. Iranian military doctrine suggests that it will employ asymmetric tactics that exploit the constricted geographic character of the gulf and the advanced systems that it has acquired.[54]

Air

Like the maritime domain, the air commons is fairly mature, with robust international governance and a strong tradition of international cooperation supporting freedom of the skies. However, the persistent threat of terrorism, and the proliferation of advanced surface-to-air and surface-to-surface missiles, could undermine the openness of the air commons in the coming decades. Moreover, the U.S. military's ability to access the air globally will be challenged by reliance on basing agreements and over-flight rights, dependence on the space and cyber commons, and a lack of a central authority to respond to challenges and threats to the air commons.

Terrorist Threats: If terrorists successfully demonstrate that air travel is unsafe, the free flow of air travel between states could be constrained. Air hijackings have been a problem since the 1930s, but the perceived threat posed by hijackings has grown exponentially in the wake of September 11. Bombings, as conducted by Libyan nationals over Lockerbie and as conceived by the al Qaeda "Bojinka" plot in 1995, also remain a significant threat. Additionally, airports have presented attractive targets to terrorists, as demonstrated in airport attacks in London, Rome and Vienna. Surface-to-air threats from terrorists also exist, as demonstrated by a 2002 attempt to shoot down a chartered Boeing 757 airliner, owned by Israel-based Arkia Airlines, with shoulder-launched Strela-2 (SA-7) surface-to-air missiles as it took off from Moi International Airport in Mombasa, Kenya.

Terrorism is a significant threat to air travel, but it does not yet pose a systemic threat to the air commons. Popular confidence in the safety of air travel has been shaken in the wake of major terrorist attacks, but it has always returned after a period of months. Unless terrorists could demonstrate the ability to persistently threaten commercial aircraft across a broad geographic scope, it is unlikely that terrorism would fundamentally threaten the openness of the air commons.

Advanced Air-to-Air Systems: Advanced combat aircraft have proliferated in recent years, largely because of Russian exports and China's increased role in cooperative research and development. The family of fighters that evolved from the Russian Su-27 represents a potent technical competitor to

Emerging Maritime Commons in the Arctic

As worldwide temperatures increase and the polar ice caps shrink, maritime shipping lanes are emerging, and previously unreachable resources are becoming accessible. In 2005, the Northeast Passage opened along the Eurasian border for the first time in recorded human history. The Northwest Passage along Canada opened up for the first time in 2007. The melting of polar ice has not only opened new shipping routes of potential significance, but it has also made significant resources more accessible. Some estimates suggest that as much as 25 percent of the Earth's untapped energy resources could be found in the Arctic.[55] These new opportunities are challenging the long-held international moratorium on competition in the Arctic Circle. As Frank Hoffman quips, "The only thing in the Arctic melting faster than the northern ice cap is the international comity."[56]

This new competition for the Arctic maritime commons was cast into stark relief by the August 2007 planting of a titanium Russia flag, on the seabed 4,200 meters (14,000 feet) below the North Pole, by Russian mini-subs to further Moscow's claims to the Arctic.[57] Moscow argued before a UN commission as early as 2001 that waters off its northern coast were, an extension of its maritime territory, and Prime Minister Vladimir Putin has already described the urgent need for Russia to secure its "strategic, economic, scientific and defense interests" in the Arctic.[58] Several countries with territories bordering the Arctic—including Russia, the United States, Canada and Denmark—have launched competing claims to the region. The competition has intensified as melting polar ice caps have opened the possibility of new shipping routes in the region.

For its part, the United States is far behind Russia in its capability to operate on the ocean surface in the Arctic. Russia is expanding its fleet of large icebreakers to about 14, including the world's largest, the nuclear *50 Years of Victory*. At the same time, the United States has two heavy icebreakers, with one currently out of service.[59] While the United States today contracts ice breaking services to Russia, this disparity is diminishing U.S. capacity to defend its access to the Arctic just as its strategic significance is on the rise. In September 2008, the Russian national security council began drafting new policy to formalize its claims of sovereignty in areas previously recognized as beyond claims of sovereignty.[60]

the current U.S. F/A-18E/F, F-16, F-15 and F-15E aircraft. The well-publicized “Cope India” exercises in 2004 and 2005 included media reports that U.S. forces were frequently “shot down” during exercises with the Indian Air Force, and that the U.S. Air Force was surprised at the technical improvements made to the Indian MiG-21s and Su-30s as well as the quality of the pilots.[61]

In addition to exporting fighter aircraft, Russia and China are developing “fifth-generation” fighter aircraft and cooperating heavily in research with other countries. Russia has long been developing the PAK-FA program with MiG and Sukhoi design teams. In November 2009, India and Russia announced an expansion of their cooperative work on the PAK-FA, and industry sources believe 2017 to be the target date for an Indian prototype.[62] Currently an importer and license producer of Su-30 aircraft, China is clearly moving toward an indigenously developed next generation of combat aircraft.[63] There have been other indications that China may instead focus expanding the capabilities of the J-10 fighter, with potential sales to Pakistan.[64]

Advanced Surface-to-Air Systems: Russia’s development and proliferation of advanced surface-to-air-missiles—coined “double digit” SAMs because of their North Atlantic Treaty Organization (NATO) code names—threatens American air dominance. As a system, these weapons are focused on countering U.S. control of the air through increased lethality, the defeat of stealth, and the targeting of standoff command, control and refueling assets. Russian SA-20 deployments reportedly caused NATO to decide against sending airborne warning and control system (AWACS) craft during the conflict with Georgia in 2008, demonstrating Western concerns about the capabilities of the SA-20.[65]

Double-digit SAMs have become a major proliferation concern. China reportedly possesses 16 SA-20 battalions and an equivalent number of shorter-range, but still lethal, SA-10 systems.[66] Around the globe, other reported customers of the SA-10 and SA-20 include Iran, Libya, Algeria, Venezuela and Vietnam.[67] In addition, China is developing an indigenous variant of the SA-10, the HQ-9, which is now available for export—repeating the trend seen with combat aircraft.[68]

These systems could threaten America’s most advanced fighters and bombers as well as American military operations in the air, and they could fall into the hands of terrorists if transferred to state sponsors of terrorism or states with internal security problems. If so, the openness of the air commons could be significantly challenged by states or non-state actors, with profound implications for international commerce and American military operations.

Precision surface-to-surface weapons: A military’s ability to use the air as a theater for operations depends on the use of bases, either on land or at sea, where aircraft can land, refuel, rearm, repair and take off. The utility of short-range military aircraft is also directly associated with the ability to launch aircraft rapidly in close proximity to its targets (sortie rates). To address these requirements, the United States since the end of World War II has established a network of bases around the world, bringing much of the world into reach of American air power.

Yet the development and proliferation of long-range precision weapons, primarily short- and medium-range ballistic missiles, are increasingly threatening the security of these bases and thus the reach of short-range American air power. China, Iran, North Korea, India and Pakistan have developed medium-range ballistic missiles (MRBM) and/or intermediate-range ballistic missiles (IRBM), though India and Pakistan target theirs largely at one another. The threat of MRBMs and IRBMs to American bases in East Asia is similar to the one posed to Taiwan's air bases by short-range ballistic missiles (SRBMs) from China. A 2009 report by RAND Corp. concluded, "The threat to Taiwan from Chinese ballistic missiles is serious and increasing. … Although literally thousands of missiles might be needed to completely and permanently shut down Taiwan's air bases, about 60–200 submunition-equipped SRBMs aimed at operating surfaces would seem to suffice to temporarily close most of Taiwan's fighter bases."[69]

The development of highly precise ballistic missiles, and an accompanying Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) network, may also threaten sea bases. China's development of an anti-ship ballistic missile (ASBM), based on an MRBM airframe, poses a significant threat to naval operations in the western Pacific. China's ability to bypass America's robust air-defense capability and strike ships at sea with ballistic missiles could severely limit American naval power projection capabilities, and thus its ability to maintain the openness of the maritime and air commons.

The proliferation of highly-accurate ballistic missiles capable of striking American bases at sea or on land could undermine American power projection, and the U.S. military's ability to protect the air and maritime commons. Without the use of land and sea bases, the U.S. military would not be able to sustain large forces at sea for extended periods of time, thus leaving the air and maritime commons open for disruption or domination.

Reliance on Access to Bases and Over-flight Agreements: While aircraft carriers allow the United States military to project air power far from regional bases, extended global power projection cannot be sustained without access to resources stored on land. American forward land bases have become hubs for the protection of the air and maritime commons. However, the United States made the decision in the years after World War II that bases would be maintained with the consent of the host nation. While most of these bases were originally established to contain the expansion of Communism, they now serve as way stations for humanitarian assistance and disaster relief, for the protection of the commons, and for the projection of American military power.

A host nation's support for these bases is not a given and has, at times, been revoked or revised in reaction to the local government's displeasure with the actions of the United States and/or U.S. military personnel. For example, the Subic Bay Naval Base in the Philippines was the largest U.S. naval base in the Pacific Ocean until it was closed in 1992 over disagreements between the two governments. Moreover, crimes and accidents committed by U.S. military personnel, and the sheer presence of U.S. military personnel in forward bases can create resentment in local populations, as seen occasionally in Japan, South Korea and Germany.

Yet forward bases are not the only element of air power that depend on foreign cooperation. The United States must also seek permission if any plane, be it military or commercial, flies within a country's sovereign air space (up to 60,000 feet). The U.S. military has often been forced to alter its war plans because of an inability to gain over-flight permission.[70] Thus, the U.S. military's ability to access the air and maritime commons is inextricably interwoven with diplomatic and economic influence around the world.

Reliance on Cyber and Space: In the past decade, commercial airlines utilized advanced technologies, such as GPS and wireless computer-to-computer communication, to greatly increase the efficiency of air travel. The greater accuracy of positioning provided by GPS, in turn, allowed air traffic controllers to increase the density of airplanes in a given area. Use of the cyber commons has given air traffic controllers greater insight into the status of planes in flight, and airline companies rely on access to cyberspace for day-to-day operations, such as scheduling and ticketing. This reliance on the space and cyber commons represents a significant vulnerability, should either of these commons become contested. The American air travel system got a small taste of the effects of lost access in November 2009, when a Federal Aviation Administration computer outage in Salt Lake City forced air traffic controllers to manually direct aircraft, instead of using computers, causing significant delays throughout the country.[71]

Diffuse Authority: America's ability to preserve the openness of the air commons will be challenged by its decentralized system of responsibility, in which dozens of agencies and departments are charged with securing specific aspects of the air commons. For example, airport security is handled by the Department of Homeland Security, while plots and acts of terrorism are investigated by the Federal Bureau of Investigation. Other than direct military threats and combat air patrols over American cities, the U.S. Air Force is largely uninvolved in defending the air commons. This lack of a central organizing authority presents a particular challenge for American policymakers as they develop initiatives to maintain the openness of the commons.

Space

The openness and stability of the space commons are challenged by the inherent fragility of satellites and the space commons itself, as well as the development and proliferation of anti-satellite jamming and strike capabilities.

Fragility of the Space Commons: Satellites are highly vulnerable. They are susceptible to kinetic and directed energy attacks, as well as jamming from the surface of the Earth. Even modest damage to satellite subsystems, such as its optics or solar arrays, can prove disastrous. Compounding this fragility is the vulnerability of space infrastructure that develops, launches, maintains and operates spacecraft. The United States possesses only two launch sites that are meant to handle large launch vehicles, and four overall. Each has a small number of launch pads, and the two large facilities are on coastlines, increasing their vulnerability to monitoring and attack. Moreover, the United States does not stockpile launch vehicles or significant numbers of spare satellites, limiting America's ability to replenish space assets in times of conflict.

The high speeds and the amount of debris in orbit — hardware and spacecraft fragments that have broken up, exploded or otherwise become abandoned — render the space commons themselves inherently fragile. There are more than 19,000 objects in orbit larger than 10 centimeters, and more than 1.5 million objects less than 10 centimeters.[72] Since 1947, more than 6,000 satellites have been put into space, and about 800 are operational now. These objects in orbit make for a crowded, and dangerous, commons (Figure 3). A tiny speck of paint that had broken off of a satellite once dug a pit in a space shuttle window nearly a quarter-inch wide, causing a near catastrophe. It is estimated that a pea-sized ball moving in orbit would cause as much damage to a satellite or manned spacecraft as a 400-pound safe travelling at 60 mph.[73] Without a more robust governance regime, this situation is likely to worsen.

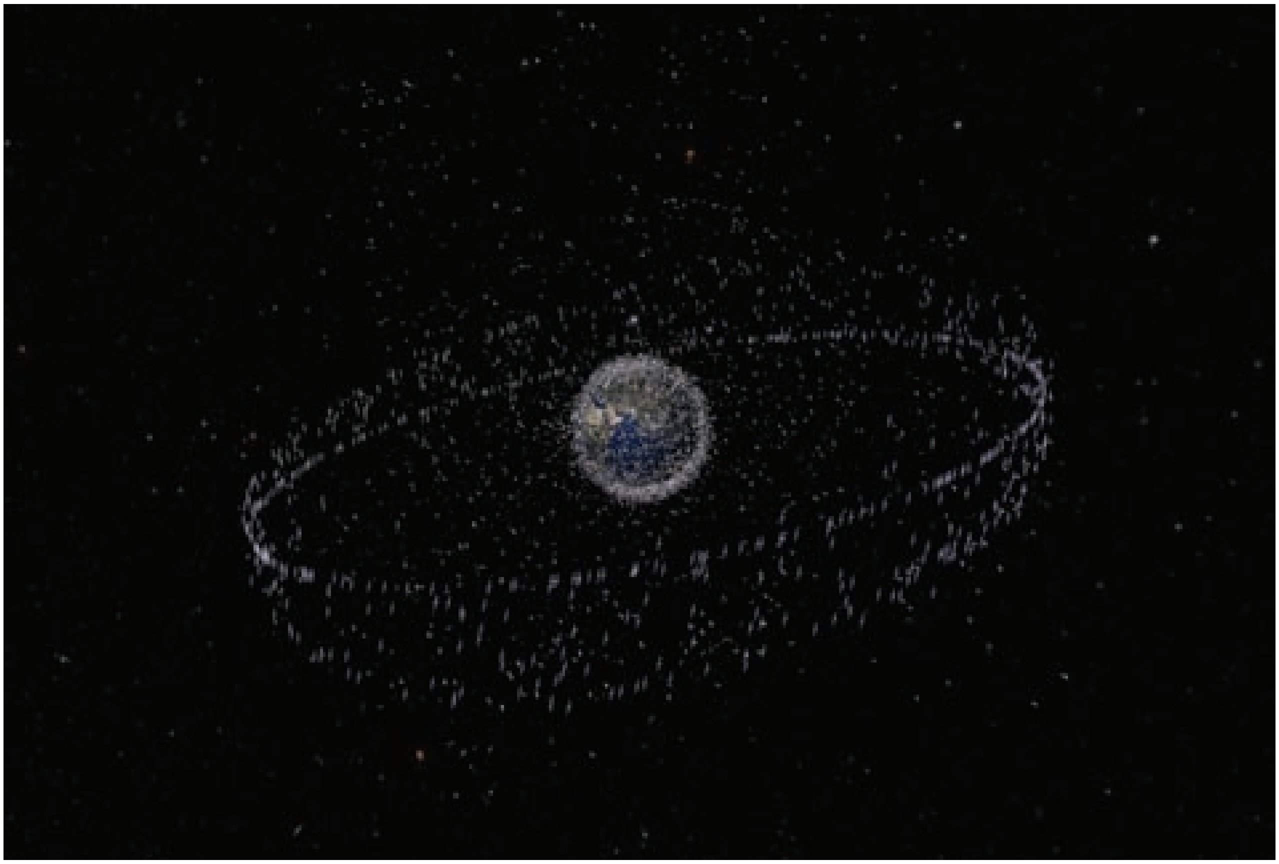
The destruction of satellites threatens the space commons, as explosions in orbit create millions of small pieces of debris, some of which can remain for decades. About 50 percent of all trackable objects in orbit are due to in-orbit explosions or collisions.[74] A broad kinetic anti-satellite campaign could be analogous to fighting World War II in an environment where all the stray bullets, mortars and bombs do not simply fall to Earth, but continue to fly around the world for decades, rendering much of the surface of the Earth uninhabitable. Similarly, orbits littered with debris from a kinetic anti-satellite campaign would be useless for the satellites upon which the global economy depends.

This fragility represents an Achilles' heel for the space commons and the U.S. military. The Commission to Assess United States National Security Space Management and Organization succinctly summarized its concerns about American vulnerabilities:

> The relative dependence of the U.S. on space makes its space systems potentially attractive targets. Many foreign nations and non-state entities are pursuing space-related activities. . . . An attack on elements of U.S. space systems during a crisis or conflict should not be considered an improbable act. If the U.S. is to avoid a "Space Pearl Harbor" it needs to take seriously the possibility of an attack on U.S. space systems.[76]

Burgeoning ASAT Capabilities: A growing number of states have recognized American reliance on space, have access to space, and are developing capabilities to exploit U.S. vulnerabilities.[77] Recent developments demonstrate that access to, and use of, space is becoming increasingly contested. These developments threaten the American way of war, given the U.S. military's use of space for everything from logistics to Command, Control,

Figure 3: Artist's Impression of Trackable Objects in Orbit Around Earth.



For visibility, size of debris is exaggerated relative to the Earth.[75]

Communications, Intelligence, Surveillance and Reconnaissance (C3ISR). These developments also threaten the space commons in general:

- China successfully tested a direct-ascent anti-satellite missile in January 2007, which created over 35,000 pieces of debris larger than 1 centimeter.[78] China also reportedly used lasers to temporarily blind an American satellite in 2006.
- Russia provided Iraq with GPS jammers in 2003, which were somewhat successful in countering American precision-strike weapons.[80]
- Several states and non-state actors have used radio and cyber capabilities to disrupt or degrade an adversary's space capabilities. Indonesia jammed a Chinese-owned satellite. Iran and Turkey have jammed satellite broadcasts of national dissidents.[81] In 2003, Iran jammed satellite broadcasts of Voice of America, and in March of that year, Iran jammed GPS signals. In 1999, hackers attacked a British satellite via cyberspace. In 2008, Brazilian hackers were arrested for using homemade communications dishes to "hijack" transponders on a U.S. Navy satellite.[82] More recently, the Iranian government reportedly jammed U.S. satellite and radio broadcasts during the protests surrounding its 2009 presidential election.

The threshold to access space is lowering, allowing several countries to develop indigenous abilities to access and operate in space. While these efforts are primarily commercial and civilian in focus, many new space programs have military components. In May 2008, Japan's legislature passed a law ending a ban on the use of its space program for defense. France's new defense white paper calls for doubling investment in space assets, including spy satellites. In late June, India announced that it would "optimize space applications for military purposes," and one of its most senior military officers candidly stated: "With time we will get sucked into a military race to protect our space assets, and inevitably there will be a military contest in space."[83]

Space may, in the coming decades, be more accessible to non-state actors. The high costs associated with developing, putting into orbit, and maintaining assets in space have, to date, kept space a domain for states, but costs are falling. Private companies have been attempting to develop relatively cost-effective space platforms for commercial launch purposes. The companies Scaled Composites and Virgin Galactic have developed a craft, *White Knight Two*, which they hope will carry a manned space capsule into orbit. In future years, it is possible (if not likely) that advanced high-altitude flight capabilities demonstrated by the *White Knight Two* will proliferate, making low orbit accessible for actors that do not have the resources to develop a full-fledged space program.

The implications of new actors operating within the space commons are potentially significant. Long the domain of the United States and the Soviet Union, space in the coming decades will become more crowded, with inexperienced actors who may not have responsible mentorship of the space commons in mind. Indeed, some may use space to strike at the United States and the international system, a kind of terrorism in zero gravity.

CYBER SPACE

The cyber commons today is a complex and anarchic environment lacking effective international agreements. Currently state and non-state actors are able to hack, intrude, corrupt and destroy data with relative impunity. While economic and technological necessity have allowed for the creation of standards and protocols to enable consistent communication, security in the cyber commons is often self-provided by users rather than by a central authority.

At the same time, the increasing use of the Internet and other aspects of the cyber commons by advanced states to manage domestic infrastructure creates new strategic vulnerabilities that adversaries cannot ignore. For example, sustained power outages or catastrophic breakdowns in

Cyberspace has changed the dynamic of political and military competition, as states may be able to compete aggressively in cyberspace while still being deficient in other measurements of national power.

transportation systems could result in significant physical damage and casualties, not to mention severely disrupting crucial economic, military and social activities. More disturbingly, attacks against these systems are technologically feasible.[84]

The distributed and interactive nature of cyberspace, combined with the low cost of computing devices, has lowered the threshold for actors to operate with great effect in cyberspace. Actors do not necessarily have to build complex weapons systems, like the Joint Strike Fighter, in order to leverage the benefits of cyberspace. Instead, accessibility and anonymity have created an environment in which smaller organizations and political actors, especially those who seek to hide from retribution in other environments, can achieve a disproportional increase in capabilities to conduct their operations and disrupt those of adversaries. The ease of achieving anonymity on the Internet also facilitates the rapid orchestration of operations across wide geographic areas with less chance of tipping off adversaries that disruptive attacks are imminent. A 2005 Washington Post article noted that al Qaeda "has become the first guerrilla movement in history to migrate from physical space to cyberspace."[85]

Cyberspace has changed the dynamic of political and military competition, as states may be able to compete aggressively in cyberspace while still being deficient in other measurements of national power. Weak adversaries can use cyberspace to exploit vulnerabilities of their more powerful adversaries and, for instance, steal intellectual property from advanced states. Just as the expansion of global maritime trade required the development of colonies, naval fleets and their supporting infrastructures, cyberspace will require political and military measures to protect economic and informational interests. The United States will have to learn how to protect its cyberspace presence in a cost-effective fashion.

Indeed, using the cyber commons to achieve rapid strategic impact has become a tool for non-state actors. Organized criminal activity, Internet posting of terrorist videos of beheadings and malicious disruption on a global scale can all spread rapidly.[86] Cyberspace has multiplied opportunities for small groups to achieve large effects by getting their message to a global audience. This increases their geographic base for acquiring resources, whether through voluntary contributions or illicit activity. In the future, these groups will use cyberspace as a place where guerilla campaigns, orchestrated dispersal and surreptitious disruption can occur. The challenge for the United States is to create a recognizable signature in cyberspace that renders such nefarious groups vulnerable to retaliation and future deterrence.

Cyberspace offers opportunities for disrupting and crippling even the largest state opponents through new methods of attack. The disruptive attacks against U.S. and South Korean government and economic sites in early July 2009 illustrate this. While the actors behind the attack remain unknown, it is known that they utilized a botnet of tens of thousands of computers based on a long-known vulnerability to network security protocols.[87] In this volume, Dr. Greg Rattray and his co-authors argue that the behavior of viruses and malicious code in the cyber commons is similar to the behavior of biological diseases.[88] They argue that the dynamics of infection and transmission parallel the dynamics of malicious code and viruses in the cyber commons.

Although the major threat to the openness of the global cyber commons stems from its anarchic and decentralized nature, several state and non-state actors are developing the capability to challenge U.S. and international access to the cyberspace.

- **Russia** reportedly has developed a robust ability to deny its adversaries access to cyberspace. In April 2007, during an imbroglio surrounding the removal of a Soviet-era monument, the websites of the Estonian Parliament, ministries, media outlets, and banks were attacked and defaced. While the Estonian government immediately blamed Russia for the attack, they could not definitively link it to Moscow.[89] Georgia faced similar attacks during its war with Russia over South Ossetia in 2008.
- **China** reportedly has developed several types of computer network operations. According to a Pentagon report, China's military has "established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks."[90] Indeed, according to the Pentagon, China's military has integrated these sorts of strikes into its exercises, using them as first strikes against enemy networks.
- **Al Qaeda** apparently has developed plans to target key businesses, government agencies, financial markets and civil infrastructure using cyberspace.[91]

An American Strategy to Protect the Global Commons

The United States should pursue a range of political and military initiatives, as well as military investments, to sustain the openness of the commons, reduce the burden of leadership from the United States, and improve the ability of the U.S. military to operate in an environment in which access to the commons is contested. In this pursuit, the United States should not limit itself to using only the military. Rather, it should utilize all elements of national power, including diplomacy, economic investment, public diplomacy, and military power.

Since World War II, American power has been derived in part from providing global public goods that also serve vital U.S. interests: stability in key regions, a vibrant global economy and fair access to the global commons. Theorist Joseph Nye has argued that considering the relationship of American power to global public goods helps to unveil "an important strategic principle that could help America reconcile its national interests with a broader global perspective and assert effective leadership."[92] It is time to recommit to this vision and to re-imagine America's stewardship of an international system that benefits both the United States and the world.

Focusing U.S. power on leading the effort to sustain these basic features of the global system is well within America's strategic tradition. Recall that America's Cold War defense and national security policy was predicated on exactly these priorities. The United States used all the elements of its power to *contain* what American diplomat George Kennan called "Russian expansive tendencies," but it also helped construct and then *sustain* an international system, the broad contours of which continue to underpin today's world.[93] Indeed, NSC 68, the famous Cold War planning document written in 1950, embraced these goals: "One is a policy which we would probably pursue even if there

Since the end of the Cold War, the international system has become an effective means for states to peacefully assert their own interests and pursue prosperity through integration into the global economy.

were no Soviet threat. It is a policy of attempting to develop a healthy international community. The other is the policy of "containing" the Soviet system. These two policies are closely interrelated and interact on one another."[94]

Since the end of World War II, the United States has led and sustained an international system that has enabled states to peacefully assert their own interests and pursue prosperity through integration into the global economy. Indeed, before becoming Deputy Secretary of State, James Steinberg argued: "Far from justifying a radical change in policy, the evolution of the international system since the collapse of the Soviet Union actually reinforced the validity of the liberal internationalist approach."[95] In future years, as states that have benefited from global integration come into their own as regional powers, they can use their newfound influence to sustain the system that has enabled their rise. The United States should channel the newfound power of rising states, and lead a global effort to protect and sustain the openness and stability of the global commons.

To achieve this new vision, the United States should pursue three key objectives.

RECOMMENDATION: BUILD STRONGER GLOBAL REGIMES

Washington should work with the international community, including potential adversaries, to develop bilateral and multilateral agreements that preserve the openness of the global commons. As Secretary of Defense Gates declared in May 2009, "Whether on the sea, in the air, in space, or cyberspace, the global commons represent a realm where we must cooperate—where we must adhere to the rule of law and the other mechanisms that have helped maintain regional peace."[96]

Maritime: As the world's oldest commons, the maritime domain has a rich tradition promoting the freedom of the seas. From international agreements to traditions of responsible seamanship, the maritime commons enjoys support from a robust set of global regimes.

The United States could greatly advance the openness of the global commons by ratifying UNCLOS. While the United States has long conformed to UNCLOS in practice, its arguments against exclusivity are undermined by not ratifying the Convention. In the words of several naval officers interviewed by the authors, not ratifying UNCLOS prevents the United States from having a "seat at the table" as continental shelves are identified, sovereign control of coastal waters is assigned, and UNCLOS provisions are interpreted.

Air: Like the maritime domain, the air commons has a robust set of regimes and a long international tradition of supporting the freedom of the skies. Yet, the international agreements that undergird the air commons are almost entirely bilateral—to date, almost 4,000 bilateral air transport agreements are registered with the International Civil Aviation Organization (ICAO).[97] The United States should lead an effort to multilateralize these agreements, which would greatly improve standardization and efficiency in civil air transportation.

Additionally, the United States should continue to strengthen peacetime aviation security. While there is no single means to accomplish this end, the United States should strive for the harmonization and implementation of best practices at airports and aviation facilities. Promulgating standards for security, from baggage inspection to airport surroundings, would greatly enhance the security of the air commons.

Space: Space is in serious need of stronger international regimes. Although fundamentally flawed, the stated goal of the space governance treaty proposed by Russia and China—"keeping outer space from turning into an arena for military confrontation, in assuring security in outer-space and safe functioning of space objects"—is laudable. To accomplish this objective, the international community should adopt two mutually supporting agreements.

1. **Kinetic No-First-Use in Space:** Given the foundational role of space in the international economy and American military operations, the United States and international community have a significant interest in preventing the kinetic destruction of satellites in orbit. An agreement that no state will be the first to kinetically destroy an object in orbit and create debris, except in cases to protect human populations from out-of-control satellites, would protect U.S. and international interests in preserving the openness of the space commons without restricting U.S. military interests in dissuading and hedging against threats in space. As this approach regulates behavior and not capability, it bypasses obstacles such as the need to define "anti-satellite weapons" and verification.

2. **Against Harmful Interference in Peacetime:** An international agreement against harmful interference of space objects would encompass a prohibition against the jamming, blinding, and hacking of satellites. Such disruptions—even if they do no permanent damage to the satellite itself—threaten the openness of the space commons. However, such actions would be acceptable during times of conflict.

In future years, as states that have benefited from global integration come into their own as regional powers, they can use their newfound influence to sustain the system that has enabled their rise.

With these agreements in place, the United States would be able to research kinetic and non-kinetic military capabilities for use in extremis while developing defenses against a condensed range of threats. The international community would also benefit, as the use of kinetic weapons would be restrained, as would the creation of destructive orbital debris. Moreover, prohibiting harmful interference of space systems in peacetime would offer better protection while labeling such interference more clearly as acts of hostility.

Additionally, the United States should revise its National Space Policy to encourage the development of global regimes designed to promote the openness of the space commons. The current policy, published in 2006, is blatantly hostile to any form of international agreement that limits U.S. activities in space:

> Proposed arms control agreements or restrictions must not impair the rights of the United States to conduct research, development, testing, and operations *or other activities* in space for U.S. national interest [emphasis added].

While the United States should certainly retain some ability to deny an adversary the use of space during a time of conflict, it must recognize that international agreements that limit the behavior of the United States in space will also apply to other states. Properly crafted international agreements can effectively limit threats to U.S. satellites while retaining U.S. freedom of action in space.

Cyberspace: To exercise leadership, the United States must be perceived as acting within a broader global agenda and not merely looking for advantage and dominance in this environment. The Internet was spawned from a Department of Defense-funded experiment, however it grew into a new environment for human interaction. As this experiment developed into a global commons, the United States had the vision to facilitate its global use and to cooperate broadly in the diffusion of the technology. It supported Internet governance structures that include people, groups and governments around the world.

The United States must understand the utility of a cooperative strategy to advance its interests. It should continue to leverage its place on the high ground to mobilize international and global action. Additionally, the United States should collaborate with states and others to develop norms for proper behavior through declaratory statements, and it should promote international efforts, such as the Convention on Cybercrime, to maintain a healthy and clean cyber commons.

The United States should lead global efforts to clean up the cyber environment. A clean, healthy cyber commons serves national security purposes, making it easier to identify the source of attacks and reducing the spread of botnets and other threats by malicious actors. A cleaner cyber commons would also reduce risks to U.S. military systems and operations that require cyberspace to conduct network-centric warfare and to project U.S. power globally.

Any effort to clean up the cyber environment will require international engagement for success. As in other commons, the Internet is too interconnected to make standalone national defenses effective. While there are existing programs to build the capacity of national Computer Emergency Readiness Teams (CERT), the United States should move beyond working with governments to engage and support global multi-stakeholder organizations such as IETF or ICANN. In addition, the United States should encourage network operator groups to play active roles in ensuring the technological systems and operations of the cyber commons are more resistant to abuse by malicious actors and are resilient in the face of attacks. In making the commons a better place for all users, these organizations can reach across political boundaries and remain outside the interplay of day-to-day political struggles.

RECOMMENDATION: ENGAGE RESPONSIBLE PIVOTAL ACTORS

In 1999, the historian and strategist Paul Kennedy and his colleagues called for an American strategy that focuses attention on "pivotal states" whose futures are "poised at critical turning points, and whose fates would significantly affect regional, and even international, stability."[98] With respect to the global commons, the United States should identify pivotal actors who share an interest in maintaining open access to the global commons, build their capacity to promote and protect those interests, and engage their support in efforts to build a lasting set of institutions and norms to protect the commons. Assistance provided to the littoral states surrounding the Strait of Malacca, which enhanced local control of a strategic choke point without increasing U.S. or foreign military commitments, could be an important model for future efforts to engage pivotal actors to secure the global commons.[99]

Maritime: The Malacca Model can most easily be replicated in the maritime domain. Naval power is traditionally distributed and cooperative, and it lends itself well to the kind of engagement that the United States will have to pursue to maintain the openness of the global commons. The identification and engagement of key littoral states along critical sea lanes of communication, such as Australia, South Korea, Japan, Malaysia, Indonesia, Singapore, India, Egypt, Israel and Spain, should be relatively straightforward. These states already have close relationships with the United States, and America has encouraged their contributions.

For strategically located states that have intentions toward the global commons that are compatible with U.S. interests, the United States and its partners should selectively and carefully provide technical assistance, financial assistance and training to improve their maritime capabilities. With improved capabilities, these states could gradually assume responsibility to maintain the openness of the maritime commons in their regions.

A more difficult task for the United States and its allies will be engaging states with important geographic locations that do not have a clear commitment to maintaining the global commons. China is the most obvious example. While China's development of a blue-water navy could be utilized to promote openness and stability in the commons, the development of anti-access capabilities (such as an anti-ship ballistic missile) raise significant questions about China's intentions. Similarly, while China's contribution to counter-piracy operations off the coast of Somalia was a positive commitment to openness, China's behavior in the South China Sea suggests a preference toward exclusive access. The United States should encourage China's participation in multilateral operations to preserve the openness of the maritime commons. At the same time, the United States should work to counter, dissuade and deter China's apparent leanings towards developing anti-access capabilities and exclusionary policy practices.

Air: To protect the air commons, a key aspect of engaging responsible pivotal actors will be building their air forces, which will be in the mutual interest of the United States and the partner countries. For the United States, new partnerships mean production contracts and the development of capable air forces that are interoperable with the U.S. military. For the pivotal actor, partnering with the United States means gaining access to advanced technologies and building a relationship with the world's dominant air power.

In addition to building military air capabilities, engaging pivotal actors in the air commons should include assistance in the construction of robust air infrastructure. The United States should encourage private investments and target foreign assistance to build airports and supporting facilities, enhance their security, improve navigation systems networks, and train its operators and managers. Tapping into the air commons is a proven mechanism for bringing jobs and economic growth to a region, especially in developing nations. Additionally, the air commons allows greater social and economic integration across borders. In short, by promoting broader use of the air commons, the United States can not only promote the openness of the air commons, but also bring greater prosperity and stability to states worldwide.

Space: The rise of several new space powers, including Japan, India and South Korea, offers the United States ample opportunities for positive engagement. As an experienced space power and the world's leader in space technologies, the United States can leverage its superior position in space to encourage the responsible behavior of pivotal space actors. This will mean encouraging the use of space for scientific exploration and collaboration, instead of as a theater for nationalistic chest-thumping.

The Malacca Model

The Strait of Malacca, a narrow, 500-mile-long waterway between peninsular Malaysia and the Indonesian island of Sumatra, is one of the most important shipping lanes in the world. Some of the world's largest economies, such as China, Japan and South Korea, depend on access to the Malacca Strait for access to the Indian Ocean and Middle Eastern energy sources beyond. In all, about 40 percent of the world's traded goods travel through the Strait of Malacca, including an estimated 15 million barrels of oil per day.[100]

The Strait of Malacca is also one of the world's most vulnerable strategic choke points—its narrowest point (Phillips Channel near Singapore) is only 1.5 nautical miles wide. Historically, piracy has been a major threat to the openness of the channel. In 2004, the Strait of Malacca saw 38 pirate attacks, the second highest total in the world that year.[101] Yet, piracy has fallen drastically—only two attacks were recorded in 2008. The reason for this sudden drop in pirate attacks should be seen as a model for how American engagement of responsible pivotal actors can help improve the openness and stability of a common without increasing American burdens.

Historically, the littoral states along the strait (Indonesia, Malaysia, and Singapore) were distrustful of one another, precluding any cooperation. When the threat of piracy escalated in 2004, these states decided to collaborate to address the problem and prevent the need for foreign (read: American) military intervention. The three countries began to coordinate sea and air patrols and share intelligence, while Indonesia addressed internal problems that had driven its citizens to piracy as a way to earn a living.

In the background of this newfound cooperation were the United States, Japan and Australia, quietly facilitating increased coordination and providing technical assistance and training. Thus, the United States and its allies were able to help like-minded, pivotal actors to maintain the openness of a commons without violating the regional state's sense of autonomy or taking on additional burdens for the U.S. military.

Cooperation between these actors has not been limited to counter-piracy. In early September 2007, naval forces from the United States, India, Japan, Australia and Singapore participated in the joint exercise MALABAR-07-02, the largest multi-national Asian naval exercise in decades. In the eastern Indian Ocean, these navies exercised a wide range of scenarios, including mock air battles involving Indian and American aircraft carriers, sea strikes near the Strait of Malacca, and anti-piracy drills off the Andaman Islands. This exercise roughly coincided with then-Chief of Naval Operations Adm. Michael Mullen's call for a "thousand-ship navy" consisting of countries with shared interests in counter-piracy, counter-proliferation and other naval issues.

Central to the responsible use of space will be the development and promulgation of space situational awareness (SSA), or the ability of a space power to know what objects are in orbit and identify potential problems before they emerge. SSA is a closely-held secret, but it need not be. The United States could, and should, develop a version of SSA that can be shared with responsible space-faring nations.

Another potential area for the engagement of responsible space actors is the tracking, and eventual mitigation, of space debris. The Inter-Agency Space Debris Coordination Committee (IADC), composed of space agencies from the United States, the European Union, Russia, Japan, Italy, the U.K., France, China, Germany, India and the Ukraine, has already been established to exchange information on space debris research activities and facilitate cooperation. Yet, additional cooperation to limit the creation of additional orbital debris and to mitigate existing debris is needed, and it will be a major challenge in the coming decades.

As in the maritime commons, the United States will be challenged to engage states that have unclear capabilities and intentions. The United States should engage emerging, responsible space powers with technical assistance and cooperative scientific missions while emphasizing the importance of maintaining the openness and stability of the space commons. Moreover, the United States should use cooperation and the potential for technological exchanges to entice these states to behave responsibly and contribute positively.

Cyberspace: The seeds of international cooperation to maintain the openness of the cyber commons are already sprouting. The U.S. CERT Coordination Center (US-CERT/CC), other national CERTs, and international organizations such as the Forum of Incident Response and Security Teams (FIRST) perform some of the same functions for cyber security as do the World Health Organization and the Centers for Disease Control for public health. But they are not nearly as comprehensive. As an example, the US-CERT/CC provides risk management and threat awareness at the system and software levels, assists in vulnerability reporting to vendors, and facilitates information sharing.

The United States should take steps to make international organizations such as FIRST more comprehensive, and it should give them the same level of legitimacy and capability to address shared cybersecurity concerns as the WHO has in the realm of global health. Because of the lack of a global consensus on cybersecurity approaches, the United States would initially have to build a coalition of like-minded actors (including states and corporations) to promote the health and openness of the cyber commons.

Washington should also utilize public-private partnerships and encourage country- and local-level information sharing on cyber defense. National organizations should exchange information with local groups, and help them implement security measures. Sector-specific entities (for example, in banking or energy) should address security for companies in their sector. Collecting and publishing best practices for security and threat management from constituent organizations, sharing and monitoring data, championing research efforts, and assisting with response activities during times of crisis are activities these cyber-defense organizations should undertake. Such an effort would produce a national view of cyber threats, events, and collaborative response that can be linked into the global community just as America's CDC is linked to other nations' public health programs through the WHO.

RECOMMENDATION: RESHAPE AMERICAN HARD POWER TO PROTECT THE GLOBAL COMMONS

Washington should clearly signal America's intentions to stand by its long tradition of supporting the openness and stability of the global commons. While the building of global regimes and the engagement of responsible pivotal actors can go a long way toward promoting this goal, these steps are not sufficient to ensure an open and stable global commons. The United States should develop a robust military capability as well. Such a capability could dissuade efforts to undermine the commons and defeat any actor that attempts to limit access by the United States, and its allies and partners. As a precaution, the Pentagon should also develop capabilities to enable effective U.S. military operations when a commons is unusable or inaccessible.

Maritime: In the coming decades, U.S. naval capabilities will need to operate in a more contested environment in which the use of regional bases will be uncertain. An increased reliance on expeditionary warfare, and threats from advanced cruise missiles, anti-ship ballistic missiles, Maritime Armed Groups, terrorists, and pirates will require the flexibility to respond to a diverse set of challenges, far from home, with varying degrees of regional support.

In an age when the United States will rely more on expeditionary power than on forward basing, aircraft carriers and advanced surface ships will be at the center of America's ability to project power around the world. The Pentagon's proposed budget from Fiscal Year 2010 included slowing the rate of aircraft carrier production by one year, which will ultimately reduce the active U.S. carrier fleet to 10. Secretary of Defense Gates also requested a delay in the development of a next-generation guided missile cruiser, finishing production of the over-budget and delayed DDG-1000 Zumwalt-class destroyer, and restarting the highly-capable Arleigh Burke-class guided missile destroyer. While the U.S. Navy will still be the dominant naval power with considerable power projection capability, the loss of one aircraft carrier is a significant reduction in available blue-water firepower. Most significant for operating in oceans with anti-access threats will be the revitalization of the Arleigh Burke-class destroyer, which is upgradeable to a missile defense capability that counters ballistic and cruise missile threats.

Additionally, a robust littoral capability will be essential to preserving the openness of strategic maritime commons, such as the Strait of Hormuz and the Persian Gulf, where low-end distributed threats present a particular hazard. The Pentagon's FY 2010 budget request included the accelerated development of the Littoral Combat Ship (LCS) program, which is intended to be smaller, faster and more agile in order to effectively operate in the near-shore environment. A fleet of these relatively inexpensive yet highly capable ships,[v] commanded by the U.S. Navy and its partners, would be a robust defender of the openness and stability of the commons.

Yet the United States must do more to counter anti-access capabilities and reassure allies. As forward bases come under threat of ballistic missile strikes, and their utility becomes increasingly constrained by political sensitivities of the host countries, the United States should continue the pursuit of a robust and flexible force posture and logistics chain, while investing in base-hardening and missile defenses.

The United States must adjust to the increasing reluctance of many host countries to support large military bases. Maintaining the ability to sustain expeditionary power projection is important, but even the most advanced carrier strike groups rely on regional bases for logistics support. Thus, the United States cannot rely on

[v] The rising costs of the LCS (which has gone from a planned per-ship cost of 223 million dollars to over 700 million dollars for the first ship of its class) are highly concerning.

The Littoral Command Ship-1.

(LT ED EARLY/U.S. Navy)

maritime expeditionary power alone—some form of regional basing support will be required if the United States is going to retain the ability to support extended power projection.

The United States should pursue the creation of a more flexible network of smaller bases and supply stations around the world that support the U.S. military's logistical needs yet require a smaller geographic and political footprint with the host nation. This will require moving away from the Cold War model of large, overtly-military bases to dual-use civil-military facilities based on more implicit bilateral agreements.[103] Supporting this should be a sustained effort to cultivate strong diplomatic and economic ties with strategically-located states. An example is Singapore's Changi Naval Base, which can accommodate the largest of ships, including an aircraft carrier.[104]

Air: The Department of Defense appears confident about the future of its air-to-air advantages in the coming decades.[105] Yet air superiority requires more than a technological or numerical advantage in air-to-air platforms. The ranges of current and projected surface-to-air and surface-to-surface missile systems possessed by potential adversaries, or on the global market, will reshape dramatically the familiar terms of competition in the air. The United States should bolster the range and survivability of its air power. The utilization of long-range reconnaissance and strike systems, combined with cruise-missile-equipped attack submarines, would enable the United States to operate in some denied environments.[106]

Space: While global regimes and responsible behavior by pivotal actors can go far toward mitigating this problem, the United States should develop capabilities to rapidly replace satellites lost in a conflict, and research ways to harden satellites against kinetic and nonkinetic attack.

However, replenishment and hardening is insufficient, as it does not address the fundamental problem that the United States relies on a commons that is inherently fragile and vulnerable. In the coming decades, the United States should not allow its military to remain dependent on space to fight modern wars. This vulnerability may be simply too tempting a target for adversaries during a major conflict. Thus, the U.S. military should develop capabilities and doctrine to ensure it can operate at a high level of effectiveness without the use of space for C3ISR. Networks of sub-orbital, stealthy and unmanned planes with extended flight times offer significant promise.

Cyberspace: The cyber warfare environment is decentralized, anarchic, broad in scope and remarkably fast in tempo.[107] The speed with which attacks on a network can be initiated and adjusted will require the United States to develop rapid response capabilities, entailing higher levels of automated decision-making. Writing elsewhere in this volume, Dr. Greg Rattray and his co-authors point out that:

> Rules of engagement often call for high-confidence identification of potential targets, but a commander may not fully trust automated systems to make the call regarding weapons employment. Unfortunately, cyberspace presents myriad opportunities for adversaries to subvert automated systems and turn them against their operators, or against third parties.[108]

Yet adapting to the particulars of cyber warfare obscures the fact that the U.S. military remains highly dependent on commercial networks for rapid C3ISR. Although it will be highly challenging, the Pentagon must begin to develop technologies and concepts that will allow the military to operate effectively without use of the Internet. This will, in part, mean a reversion to reliance on commander's intent and the empowerment of lower levels of command. But it will also mean increased dispersion and robustness of physical infrastructure, so the effects of the destruction or compromise of a particular node is contained.

Conclusion

America's power and the stability of the existing international order depend upon the openness and stability of the global commons. Goods flow, ideas promulgate, militaries operate and people travel through these commons with little thought to how and why they are kept open.

The rise of new economic powers will fundamentally change the dynamics of the international system, and the development and proliferation of disruptive military threats will challenge the openness of the commons. The United States must realize that, as these challenges develop, it will not have the capacity to maintain these commons on its own. Thus, the development of a responsible and effective international effort, supported by global regimes, pivotal actors, and the U.S. military will maintain the stability of the commons and act as a bulwark against the forces of exclusivity and chaos.

In the end, however, protection of the global commons will depend on America's will to lead. Despite the rise of new powers and the enduring capabilities of old allies, no other country has the ability to lead a global effort to protect the commons. No other country can challenge America's legacy of building global institutions to advance shared goals. The United States should summon the will to apply its diplomatic, economic, military and moral power in defense of the global commons. This act of leadership will protect vital American interests and those of the international community for years, and even decades, to come.

That they have power to hurt and will do none,
That do not do the thing they most do show,
Who, moving others, are themselves as stone,
Unmoved, cold, and to temptation slow,
They rightly do inherit heaven's graces
And husband nature's riches from expense;
They are the lords and owners of their faces,
Others but stewards of their excellence.

— William Shakespeare
Sonnet 94

Summary of Recommendations

MARITIME

- Ratify UNCLOS.
- Selectively and carefully provide technical and financial assistance and training to improve the maritime capabilities of states whose intentions toward the global commons are compatible with U.S. interests and whose geographic locations are strategic.
- Encourage states with unclear intentions toward the global commons to participate in multilateral operations to preserve the openness of the maritime commons while countering, dissuading and deterring efforts to develop anti-access capabilities or pursuing exclusionary policy practices.
- Maintain robust power projection capabilities with aircraft carriers, missile defense-capable destroyers and an adaptable logistical system.
- Continue to pursue a robust and flexible force posture and logistics chain while investing in base hardening and missile defenses.
- Develop the ability to operate in some denied environments with the utilization of long-range reconnaissance and strike systems, combined with cruise-missile equipped attack submarines.

AIR

- Pursue multilateral civilian air transportation agreements.
- Standardize best practices at airports and aviation facilities around the globe.
- Build the air forces of allies and partners whose military air capabilities are under-developed.
- Assist in the construction of a robust air infrastructure in under-developed states with objectives in the global commons that are compatible with U.S. interests.

SPACE

- Pursue an international no-first-use agreement against kinetic strikes against satellites, except in cases to protect human populations from out-of-control satellites.
- Pursue an international agreement against the harmful interference of satellites in peacetime.
- Revise the U.S. National Space Policy to encourage the development of global regimes designed to promote the openness of the space commons.
- Encourage the use of space for scientific exploration and collaboration.
- Encourage the responsible use of orbits and prevent the creation of harmful debris.
- Develop a publicly releasable version of space situational awareness (SSA) that is shareable with other responsible space-faring nations.

- Develop robust international efforts among responsible space powers to track and mitigate orbital debris.
- Engage emerging responsible space powers with technical assistance and cooperative scientific missions, coupled with an emphasis on the importance of maintaining the openness and stability of the space commons.
- Use cooperation and the potential for technological exchanges to entice states with unclear intentions to behave responsibly and contribute to the openness and stability of the space commons.
- Develop capabilities to rapidly replace satellites lost in a conflict.
- Research technologies to harden satellites against kinetic and non-kinetic attack.
- Develop capabilities and doctrine to ensure the U.S. military can operate at a high level of effectiveness without the use of space for C3ISR.

CYBERSPACE

- Establish norms for proper behavior within the cyber commons.
- Promote international efforts to maintain a healthy and open cyber commons, such as the Convention on Cybercrime.
- Move beyond working with governments to engage and support global multi-stakeholder organizations like the Internet Engineering Task Force (IETF) and the Internet Corporation for Assigned Names and Numbers (ICANN).
- Encourage network operator groups to cross political borders to play active roles in improving the health, openness and resilience of the cyber commons.
- Make international organizations, such as the Forum of Incident Response and Security Teams (FIRST) more comprehensive, to bring them to the same level of legitimacy and capability for cybersecurity as the World Health Organization (WHO) does for global health.
- Utilize public-private partnerships and encourage information-sharing on cyber defense among state and local organizations.
- Develop rapid response capabilities, including higher levels of automated decision-making.
- Develop technologies and concepts that will allow the military to operate effectively without use of the Internet.

ENDNOTES

[1] International Maritime Organization, “International Shipping: Carrier of World Trade,” (2005), available at http://www.imo.org/includes/blastDataOnly.asp/data_id%3D18900/IntShippingFlyerfinal.pdf.

[2] As a percentage of the total dollar value of trade. *The Economic and Social Benefits of Air Transport 2008*, An Air Transport Action Group Study, (2008): 2-9.

[3] The Space Foundation, *The Space Report, 2009*, Colorado Springs, CO: The Space Foundation, (2009): 5.

[4] Interview with cybersecurity expert.

[5] International Maritime Organization, “International Shipping: Carrier of World Trade,” (2005), available at http://www.imo.org/includes/blastDataOnly.asp/data_id%3D18900/IntShippingFlyerfinal.pdf.

[6] *The Economic and Social Benefits of Air Transport 2008*, An Air Transport Action Group Study, (2008): 2-9.

[7] The Space Foundation, *The Space Report*, 2009, Colorado Springs, CO: The Space Foundation, (2009): 5.

[8] Interview with cybersecurity expert.

[9] “U.S. National Defense Strategy, 2008,” *U.S. Department of Defense*, (June 2008): 16.

[10] Michele Flournoy, “Stability Operations: A Comprehensive Approach to the 21st Century,” Comments at the Brookings Institution, (27 March 2009), http://www.brookings.edu/~/media/Files/events/2009/0327_stability/20090327_stability.pdf.

[11] Robert M. Gates, Speech to the International Institute for Strategic Studies, (31 May 2008), http://www.defense.gov/speeches/speech.aspx?speechid=1253.

[12] Barry Posen, “Command of the Commons,” *International Security* (Summer 2003): 5-46. “The United States enjoys the same command of the sea that Britain once did, and it can also move large and heavy forces around the globe. But command of space allows the United States to see across the surface of the world’s landmasses and to gather vast amounts of information. . . . Air power, ashore and afloat, can reach targets deep inland; and with modern precision-guided weaponry, it can often hit and destroy those targets.”

[13] *Ibid.*, 21.

[14] Michael Wynne, “Space: The Ultimate High Ground Creating Strategic and Tactical Conditions for Victory,” *High Frontier*, Vol. 3, No. 4, (August 2007): 4.

[15] See Michele Flournoy and Shawn Brimley, “The Contested Commons,” Proceedings (July 2009).

[16] National Intelligence Council, “Global Trends 2025” (November 2008) 93.

[17] See Barry Posen, “The Case for Restraint,” *The American Interest* (November/December 2007): 7-17.

[18] Robert Kaplan, “America’s Elegant Decline,” *The Atlantic*, (November 2007).

[19] See Jim Thomas, *Sustainable Security: Developing a Security Strategy for the Long Haul* (Washington: Center for a New American Security, 2008).

[20] “A Cooperative Strategy for 21st Century Seapower,” U.S. Navy, Marine Corps and Coast Guard, (October 2007).

[21] Thucydides wrote, “[T]hey devote a very small fraction of time to the consideration of any public object, most of it to the prosecution of their own objects. Meanwhile each fancies that no harm will come to his neglect, that it is the business of somebody else to look after this or that for him; and so, by the same notion being entertained by all separately, the common cause imperceptibly decays.” Thucydides, *History of the Peloponnesian War*, Book I, Sec. 141; translated by Richard Crawley (London: J. M. Dent & Sons; New York: E. P. Dutton & Co., 1910). Aristotle wrote, “That all persons call the same thing mine in the sense in which each does so may be a fine thing, but it is impracticable; or if the words are taken in the other sense, such a unity in no way conduces to harmony. And there is another objection to the proposal. For that which is common to the greatest number has the least care bestowed upon it. Each one thinks chiefly of his own, hardly at all of the common interest; and only when he is himself concerned as an individual. For besides other considerations, everybody is more inclined to neglect the duty to which he expects another to fulfill; as in families many attendants are often less useful than a few.” Aristotle, *Politics*, Book II, Chapter III, 1261b; translated by Benjamin Jowett as The Politics of Aristotle: Translated into English with Introduction, Marginal Analysis, Essays, Notes and Indices (Oxford: Clarendon Press, 1885), Vol. 1 of 2.

[22] Garret Hardin, “The Tragedy of the Commons,” *Science*, Vol. 162, (13 December 1968): 1243-1258.

[23] *Ibid.*

[24] Mancur Olson, *The Logic of Collective Action*, (1971).

[25] Robert Keohane, *After Hegemony*, Princeton University Press, (1984).

[26] Elinor Ostrom, “Governing the Commons: The Evolution of Institutions for Collective Action,” (Cambridge University Press), 1990; and Thomas Dietz, Elinor Ostrom and Paul C. Stern, “The Struggle to Govern the Commons,” *Science*, (12 December 2003): 1907.

[27] Alfred Thayer Mahan, “The Influence of Sea Power Upon History, 1660-1783,” in *Roots of Strategy: Book 4*, ed. David Jablonsky, (Mechanicsburg, Penn.: Stockpole Books, 1999): 78.

[28] Adapted from Dr. Greg Rattray, Chris Evans and Jason Healey, “American Security in the Cyber Commons,” *Contested Commons: The Future of American Power in a Multipolar World* (January 2010) 137-176.

[29] *The National Strategy for Maritime Security*, Washington, DC: The White House, (September 2005): 7-8. http://www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf.

[30] Julian S. Corbett, Some Principles of Maritime Strategy. Classics of Seapower series. Annapolis, MD: Naval Institute Press, (1988).

[31] Frank Hoffman, “The Maritime Commons in the neo-Mahanian Era,” *Contested Commons: The Future of American Power in a Multipolar World* (January 2010) 49-75.

[32] *The Economic and Social Benefits of Air Transport 2008*, An Air Transport Action Group Study, (2008): 2.

[33] *The Economic and Social Benefits of Air Transport 2008*, An Air Transport Action Group Study, (2008): 2-9.

[34] For a comparison of these two theorists, see Jeffrey G. Lofgren, "21st Century Air Power Theorists: Who Has it Right, John Warden or Robert Pape?" National War College, (2002), http://handle.dtic.mil/100.2/ADA442423.

[35] Robert Gates, "Speech to the Economic Club of Chicago," (16 July 2009), http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1369.

[36] For more on space policy, see Michael E. O'Hanlon, *Neither Star Wars nor Sanctuary*, (Brookings Institutional Press, Washington DC 2004).

[37] PDD/NSTC 8, National Space Policy, (14 September 1996) in R. Cargill Hall, *Presidential Decisions: NSC Documents, Supplement: Newly Declassified Excerpts*, (Washington, DC: George C. Marshall Institute, April 2006): 23.

[38] *National Space Policy*, (31 August 2006).

[39] National Intelligence Council, "Global Trends 2025," (November 2008): iv.

[40] International Monetary Fund, *World Economic Data*, (October 2009). Analysis by the authors.

[41] International Monetary Fund, *World Economic Data*, (October 2009). Analysis by the authors.

[42] Fareed Zakaria, "The Rise of the Rest," *Newsweek*, (12 May 2008).

[43] Richard Haass, "The Age of Nonpolarity," *Foreign Affairs*, (May/June 2008).

[44] G. John Ikenberry, "Grand Strategy as Liberal Order Building," prepared for conference *After the Bush Doctrine: National Security Strategy for a New Administration* at the University of Virginia, (29 May 2007), available at http://www.princeton.edu/~gji3/Ikenberry-Grand-Strategy-as-Liberal-Order-Building-2007-word.pdf.

[45] Robert Kagan, "End of Dreams, Return of History," *Policy Review*, (August/September 2007).

[46] See G. John Ikenberry, "Liberal Order Building," in *To Lead the World: American Strategy After the Bush Doctrine*, Melvyn P. Leffler and Jeffrey W. Legro (eds), New York: Oxford University Press, (2008), and Robert Kagan, "End of Dreams, Return of History," *Policy Review* (August/September 2007). Also see Michele Flournoy and Shawn Brimley (eds), *Finding Our Way: Debating American Grand Strategy*, (Washington: Center for a New American Security, 2008).

[47] See Andrew Exum, "Hizballah at War: A Military Assessment," Washington Institute for Near East Policy, *Policy Focus* no. 63, (December 2006), http://www.washingtoninstitute.org/download.php?file=PolicyFocus63.pdf.

[48] See Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars,* (Arlington VA: Potomac Institute for Policy Studies, 2007).

[49] U.S. Department of Defense, "Report to Congress on the Military Power of the People's Republic of China," (2008).

[50] Robert Kaplan, "China's Two-Ocean Strategy," in *China's Arrival*, Abraham M. Denmark and Nirav Patel, eds., (Center for a New American Security, September 2009).

[51] For detailed assessments see Martin N. Murphy, *Smallboats, Weak States and Dirty Money*, New York: Columbia University Press, 2009; Peter Lehr, ed., *Violence at Sea: Piracy in the Age of Global Terrorism*, New York: Routledge, 2006; John S. Burnett, *Dangerous Waters: Modern Piracy and Terror on the High Seas*, New York, Penguin press, 2003; and Daniel Sekulich, *Terror on the Seas: True Tales of Modern-Day Pirates*, (St. Martin's Press, 2009).

[52] Peter Chalk, *Maritime Piracy*, testimony before the Committee on Transportation and Infrastructure, U.S. House of Representatives, (4 February 2009).

[53] International Maritime Organization, "Reports on Acts of Piracy and Armed Robbery Against Ships, Annual Report, 2008," London, UK, (19 March 2009).

[54] Fariborz Haghshenass, *Iran's Asymmetric Naval Warfare*, Washington, DC: The Washington Institute for Near East Policy, Policy Focus #87, (September 2008).

[55] Lt Col Anthony Russell, "Carpe Diem, Seizing Strategic Opportunity in the Arctic," *Joint Force Quarterly*, Issue 51, (4th quarter 2008): 94-101.

[56] Frank Hoffman, "The Maritime Commons in the neo-Mahanian Era," *Contested Commons: The Future of American Power in a Multipolar World* (January 2010) 49-75.

[57] "Russia plants flag under N Pole," *BBC News*, (2 August 2007).

[58] As cited in Ariel Cohen, "Russia's Race for the Arctic," *The Heritage Foundation*, WebMemo #1582, (6 August 2007), http://www.heritage.org/Research/RussiaandEurasia/wm1582.cfm.

[59] Andrew C. Revkin, "U.S. pushes to expand Arctic icebreaker fleet," *The New York Times*, (17 August 2008).

[60] Cmdr John Patch, USN (Ret.), "Cold Horizons: Arctic Maritime Security Challenges," *Proceedings*, (May 2009): 49.

[61] Baldauf, Scott, "Indian Air Force, in war games, gives U.S. a run," *The Christian Science Monitor*, (28 November 2005), http://www.csmonitor.com/2005/1128/p01s04-wosc.html.

[62] Govindasamy, Siva, "Russia, India to advance deal on PAK-FA fighter variant," *Flight International*, (12 November 2009), http://www.flightglobal.com/articles/2009/12/11/335995/russia-india-to-advance-deal-on-pak-fa-fighter-variant.html.

[63] Govindasamy, Siva, "China expects fifth generation fighter in 10 years," *Flight International*, 11 December 2009, http://www.flightglobal.com/articles/2009/11/12/334680/china-expects-fifth-generation-fighter-in-10-years.html.

[64] Govindasamy, Siva, "China to complete J-10 development before launching fifth-generation fighter," *Flight International*, (17 November 2009), http://www.flightglobal.com/articles/2009/11/17/335107/china-to-complete-j-10-development-before-launching-fifth-generation.html.

[65] Fulghum, David A. and Barrie, Douglas, "Russia Sells SA-20 to Iran," *Aviation Week*, (12 December 2008), http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=awst&id=news/aw121508p2.xml.

[66] Maples, Michael D., Lieutenant General, U.S. Army, ANNUAL THREAT ASSESSMENT: Statement before The Committee On Armed Services, United States Senate, (10 March 2009): 2, http://armed-services.senate.gov/statemnt/2009/March/Maples%2003-10-09.pdf; U.S. Department of Defense, *Annual Report to Congress: Military Power of the People's Republic of China*, 2009, 50, 66; http://www.defense.gov/pubs/pdfs/China_Military_Power_Report_2009.pdf.

[67] "Venezuela buys powerful missiles with Russian loan," *Reuters*, (14 September 2009), http://www.reuters.com/article/idUSTRE58C1YR20090914; Kopp, Carlo, Dr., *Proliferation of Advanced Surface to Air Missiles*, Air Power Australia, (June 2009), http://www.ausairpower.net/APA-S-300-Proliferation.html; "Russia has assured Iran on missile delivery: diplomat," *Agence France Presse*, (27 November 2009), http://www.google.com/hostednews/afp/article/ALeqM5gMp9L77JriWEquReS9_u_UiXrzXQ.

[68] Chang, Adrei, "China exports new surface-to-air missile," *United Press International*, (18 March 2009), http://www.upi.com/Business_News/Security-Industry/2009/03/18/China-exports-new-surface-to-air-missile/UPI-30271237410000/.

[69] David A. Shlapak, David T. Orletsky, Toy I. Reid, Murray Scot Tanner, Barry Wilson, "A Question of Balance," *The RAND Corporation*, (2009): 51.

[70] For example, see Italy's refusal to grant over-flight rights to the United States in support of Operation El Dorado Canyon, and Turkey's refusal to provide over-flight or basing access in support of strikes against Iraq in 2003.

[71] Lisa Stark, Devin Dwyer, and Scott Mayerowitz, "FAA Computer Glitch Knocked Out Electric Flight Information," *ABCNews*, (19 November 2009), http://abcnews.go.com/Travel/BusinessTraveler/faa-computer-glitch-delays-flights-nationwide/story?id=9124958.

[72] Timon Singh, "Space: The Final Junkyard," *EU Infrastructure*, (24 August 2008), http://www.euinfrastructure.com/news/Space-The-Final-Junkyard/.

[73] *Ibid*.

[74] *Ibid*.

[75] European Space Agency, "Space Debris: Evolution in Pictures," http://www.esa.int/SPECIALS/ESOC/SEMN2VM5NDF_mg_1.html, (20 November 2009).

[76] *Report of the Commission to Assess United States National Security, Space management and Organization*, (11 January 2001): viii.

[77] J. Michael McConnell, *Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence*, (7 February 2008): 33.

[78] Center for Space Standards and Innovation, "Chinese ASAT Test," http://www.centerforspace.com/asat/, (5 December 2007).

[79] "China jamming test sparks U.S. satellite concerns," *USA Today*, (5 October 2006).

[80] Kevin Pollpeter, *Building for the Future: China's Progress in Space Technology During the Tenth 5-year Plan and the U.S. Response*, (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, March 2008).

[81] *Report of the Commission to Assess United States National Security*, Space management and Organization, (11 January 2001): 20.

[82] Marcelo Soares, "The Great Brazilian Sat-Hack Crackdown," *Wired.com*, (20 April 2009). http://www.wired.com/politics/security/news/2009/04/fleetcom?currentPage=all.

[83] Gavin Rabinowitz, "Indian army wants military space program," *Associated Press*, (17 June 2008).

[84] Tim Wilson, "Experts: U.S. Not Prepared for Cyber Attack," describing Congressional testimony, www.darkreading.com/document.asp?doc_id=122732, (accessed 26 April 2007).

[85] Steve Coll and Susan B. Glasser, "Terrorists Turn to the Web as Base of Operations," *Washington Post,* (7 August 2005): A01.

[86] The Slammer worm in 2003 caused major disruption across the Internet in a period of less than 15 minutes. Paul Boutin, "Slammed! An inside view of the worm that crashed the Internet," *Wired*, (July 2003), http://www.wired.com/wired/archive/11.07/slammer.html.

[87] See Wikipedia for a summary of these attacks, http://en.wikipedia.org/wiki/July_2009_cyber_attacks.

[88] Dr. Greg Rattray, Chris Evans and Jason Healey, "American Security in the Cyber Commons," *Contested Commons: The Future of American Power in a Multipolar World* (January 2010) 137-176.

[89] Arthur Bright, "Estonia accuses Russia of 'cyberattack," *The Christian Science Monitor*, (17 May 2007).

[90] U.S. Department of Defense, "Annual Report to Congress on the Military Power of the People's Republic of China," (2009): 27-28.

[91] "Al-Qaeda planning cyber war against Britain, warns Lord West," *The Telegraph*, (25 June 2009).

[92] Joseph Nye, "Recovering American Leadership," *Survival* (February/March 2008): 63.

[93] See George Kennan, "The Sources of Soviet Conduct," *Foreign Affairs* (July 1947).

[94] Quoted from Ernest May, ed., *American Cold War Strategy: Interpreting NSC-68* (New York: St. Martin's Press, 1993): 41.

[95] James Steinberg, "Real Leaders Do Soft Power: Learning the Lessons of Iraq," *The Washington Quarterly* (Spring 2008): 159.

[96] Robert M. Gates, "Speech: International Institute for Strategic Studies," (30 May 2009), http://www.defense.gov/speeches/speech.aspx?speechid=1357.

[97] *Ibid*.

[98] Robert Chase, Emily Hill, and Paul Kennedy, *The Pivotal States: A New Framework for U.S. Policy in the Developing World*, (Norton: New York, 1999): 5.

[99] Note that this study use the slightly modified “pivotal actors” in order to acknowledge the importance of non-state actors in the maintenance of open and stable commons. Additionally, for the purposes of this study, “pivotal actors” includes great and emerging powers alike, whereas Dr. Kennedy’s original proposal focused on developing states alone.

[100] U.S. Energy Information Administration, World Oil Transit Chokepoints, http://www.eia.doe.gov/cabs/World_Oil_Transit_Chokepoints/Full.html, (January 2008).

[101] Michael Schumann, “How to Defeat Pirates: Success in the Strait,” *Time*, (22 April 2009).

[102] European Space Agency, “Space Debris: Evolution in pictures,” http://www.esa.int/SPECIALS/Space_Debris/SEMN2VM5NDF_mg_21_s.html.

[103] Robert Kaplan, “Power Plays in the Indian Ocean: The Maritime Commons in the 21st Century,” *Contested Commons: The Future of American Power in a Multipolar World* (January 2010) 177-192.

[104] Republic of Singapore Navy, “Our Bases,” http://www.mindef.gov.sg/navy/assets_bases.html.

[105] Robert Gates, “Speech to the Economic Club of Chicago,” (16 July 2009), http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1369.

[106] These proposals are more fulsomely discussed in Andrew F. Krepinevich Jr., “The Pentagon’s Wasting Assets,” *Foreign Affairs*, (July/August 2009).

[107] Dr. Greg Rattray, Chris Evans and Jason Healey, “American Security in the Cyber Commons,” *Contested Commons: The Future of American Power in a Multipolar World* (January 2010) 137-176.

[108] Dr. Greg Rattray, Chris Evans and Jason Healey, “American Security in the Cyber Commons,” *Contested Commons: The Future of American Power in a Multipolar World* (January 2010) 137-176.

CHAPTER II:
THE MARITIME COMMONS IN THE NEO-MAHANIAN ERA

By Frank Hoffman

The United States is a major trading nation, and its economy, environment and social fabric are inextricably linked to the oceans and their resources.

THE MARITIME COMMONS IN THE NEO-MAHANIAN ERA

By Frank Hoffman

Introduction

There is no denying geography. Its influence on geopolitics and the interaction of nations over the ages is inescapable. Many believe that history and geography have been negated by globalization, and that the world is now flatter, smaller and even more cooperative. But that is simply not true. Globalization in its present form speeds up the effects of actions all around the globe and magnifies their impact. The increasingly accelerated and interconnected nature of geopolitics and economic activity is generating new pressures and tensions.

Two prominent geostrategists from the late 19th century, Halford Mackinder and Alfred Thayer Mahan, recognized the challenges posed by the increasing interconnectedness of their era. In his famous 1904 presentation to the Royal Geographic Society, Mackinder characterized the growing economic interdependence of Europe as a closed political system of worldwide scope. He recognized that economic interdependence had made the world less resilient and more unstable as the "explosion of social forces" echoed sharply around the globe, and the weakest elements in the political and economic organisms of the world "shattered in consequence."[1]

Because of the reverberations in this tightly integrated structure, nations no longer could ignore major events that occurred far away. "Every shock, every disaster," Mackinder stressed, "is now felt even to the antipodes."[2] A century later, this interconnectedness is easier to recognize, and the system is more volatile and less collaborative than some pundits think.[3] Trends in climate change and energy security produce ripples faster and with greater effect than before.

Mahan and Mackinder emphasized the relationships among geography, demography and economic success. Mahan's research has been invaluable in framing the importance of geography and its relevance to modern strategists.[4]

He stressed the significance of powerful nations' command of the seas. The ocean was "a great highway" for the critical trade routes of international commerce.

Perhaps surprisingly, about 75 percent of the world's maritime commerce and nearly half the globe's daily oil needs pass through a handful of international straits and canals.

Mahan appreciated the close link between maritime power and economic development, as well as the application of sea power to sustain geopolitical influence. He who controls the commons has great leverage and can exploit that leverage to preserve the peace. This is clearly reflected in the current National Strategy for Maritime Security, which acknowledges that:

> The right of vessels to travel freely in international waters, engage in innocent and transit passage, and have access to ports is an essential element of national security. The free, continuing, unthreatened intercourse of nations is an essential global freedom and helps ensure the smooth operation of the world's economy.[5]

For many years, Britain's Royal Navy was the ultimate guarantor of the global commons. That great tradition and responsibility was transferred to the American Navy after World War II. For the better part of the last half century, the U.S. Navy ensured strategic access and served as the principal protector of international stability. However, with the end of the Cold War and the apparent rise of terrorism, few support the effort to maintain a substantial balanced fleet that can range the globe. Many analysts today are rightfully concerned about the "elegant decline" or outright neglect of America's naval power.[6]

Although several analysts write of a post-naval, post-oceanic or post-Mahanian era,[7] such views overemphasize novel elements at the expense of enduring realities and geopolitics. Mahan might concede some points to these scholars, but it is doubtful that he would agree that the oceans are any less critical to geopolitics. He would point to ever higher levels of international trade and the widening use of oceans for commerce and energy transportation as reinforcements of his arguments.

Contrary to the popular proponents of the information age, the significance of our oceanic highways has not diminished. At least 77 percent of all international trade moves by ship.[8] Many countries' critical energy imports arrive by sea. For example, about 80 percent of China's and Japan's crude oil imports are transported by ship. Perhaps surprisingly, about 75 percent of the world's maritime commerce and nearly half the globe's daily oil needs pass through a handful of international straits and canals. These strategic chokepoints risk the resilience of international commerce and the energy distribution network, underscoring the importance of the global maritime commons in an international system dependent upon free-flowing trade, energy resources and critical markets.

As long as the maritime commons remains critical geostrategically, Mahan's emphasis on obtaining and maintaining command of the seas as a matter of policy remains sound. Certainly, scholars from Chinese and Indian circles appear to find Mahanian thinking relevant. In fact, Chinese analysts are explicitly promoting Mahanian ideas.[9] While Mahan's emphasis on the *means* of attaining the command of the seas—by the concentrated application of capital ships in climatic battles—

may be dated, his emphasis on strategy, geography, economics and maritime power are not. Instead of post-naval or post-oceanic age, this paper contends that the maritime world is going back to the future, one best captured by the term *neo-Mahanian*.

While the ocean is still acknowledged as a great commons, several analysts acknowledge that it is "an increasingly restricted and contested common."[10] It is contested by rising powers in the Indian and Pacific oceans, powers that explicitly embrace Mahanian concepts about the relation of naval superiority to commercial success and authority on land. The sea is increasingly a site of conflict for maritime armed groups in lawless areas alongside failed or failing states. The global maritime commons is also contested by states seeking geopolitical and economic advantage in areas formerly overlooked by distance, low accessibility to resources and disagreeable climatic conditions.

With these themes in mind, this study will examine the rise of new naval powers in China, India and Russia, as well as the emergence of hybrid and non-state maritime threats. It will then offer a set of recommendations to preserve the maritime commons and advance the governance to better secure it for the international community.

Rising and Reassertive Powers

One of the notable trends in the international security environment is the "rise of the rest."[11] Renowned political writer Fareed Zakaria's term captures the emergence of several powers with geographic significance, demographic strength and dynamic economies. The phrase also encapsulates the reassertiveness of Russia, which has embraced state capitalism and benefited from enormous energy reserves to reclaim its status. Rising and re-emerging powers have rightfully caught the attention of those responsible for long-range planning in the national security community.[12] The capabilities they develop, and the missions they pursue, will fundamentally influence the nature of the maritime commons in the coming decade. If utilized for openness and stability, these 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.

CHINA: THE DRAGON AT SEA

Of all the rising powers, China's growing military modernization draws the greatest concern. There is an emerging consensus among the intelligence and defense community that China's Navy has passed a tipping point in its development. Up to this point, the People's Liberation Army (PLA) has pursued a deliberately measured modernization program to cow or coerce Taiwan, designed around conventional military systems. At the same time, the PLA's suite of submarines, missiles, mines, aircraft and amphibious vessels empower it to limit access along its coastline.[13] The nature and scale of this buildup has been steady and could now effectively disrupt or delay the arrival of U.S. naval forces in the event of a crisis around Taiwan. Or, it could be used to threaten ships operating in international trading lanes. In fact, the breadth of the PLA Navy's modernization recently has led analysts to pessimistic conclusions about the ability of Taiwan to defend itself.[14]

China's sustained investment in naval power is not completely malevolent. The Chinese government recognizes the importance of maritime security to its strategic interests. The latest Chinese defense white paper noted, "Economic risks are manifesting a more interconnected, systematic and global nature. Issues such as terrorism, environmental disasters, climate change, serious epidemics, transnational crime and pirates are becoming increasingly prominent."[15] In particular, the Chinese are aware of their long and exposed shipping lines and the critical reliance upon secure sea lanes for energy imports and economic prosperity.

China's naval officials are acutely aware of the vulnerability of energy resources, and they do not want their economic development to be held hostage by foreign powers or to be at the mercy of the U.S. or Indian navies.[16]

China, distrustful of the United States and the international system, is sensitive to its own growing economic dependence on access to foreign resources and markets.[17] The PLA Navy appears to be moving beyond internal security and defensive and coercive capabilities focused on Taiwan contingencies. It is expanding efforts to protect China's vulnerable sea lanes of communication (SLOCs) and energy distribution network from the Middle East through the Indian Ocean and the Strait of Malacca. As Adm. Dennis Blair, the Director of National Intelligence (DNI) recently testified, "We judge that China, over the past several years, has begun a substantially new phase in its military development by beginning to articulate roles and missions for the PLA that go well beyond China's immediate territorial interests."[18]

China has historically emphasized its land forces and regime control, but it is increasingly interested in expanding the breadth and depth of its maritime forces.[19] In facing up to its expanding interests and capabilities, the PLA Navy is beginning to get its sea legs and may no longer be content to merely defend its coastline. A more active PLA Navy will not necessarily replicate the practice of building a global network of military bases, as the British and American navies did in the 19th and 20th centuries, respectively. China's development of deep-water commercial ports along its vital SLOCs in the Indian Ocean are not military bases, or even operated by Chinese companies, but can still supply Chinese forces with fuel, food and spare parts. This network of private-owned and foreign controlled outposts will extend the PLA Navy's range into critical maritime areas and SLOCs to preserve China's access to energy resources and markets. The deployment of a small squadron to support the counterpiracy mission off the east coast of Africa demonstrated China's new range and interest in maritime security.

The PLA Navy's modernization over the past decade is impressive. China has commissioned five nuclear-powered and 22 conventionally powered submarines. It has also commissioned 16 surface combatants and a robust amphibious fleet. The Chinese naval force also includes about 40 *Hubei*-class small missile boats.[20] The latter are armed with eight C-802 anti-ship missiles.

Arguably, some of this capacity could benefit the international community, allowing China to partner with other like-minded nations in preserving free access to the global commons.[21] Yet, it would also give the PLA Navy an ability to pursue China's claims for territorial waters and resources that are contested by other nations.

China's submarine force is also growing, in both quantity and quality. Submarines have been considered a core element in Chinese naval power for some time. At present, the Chinese can field 60 relatively modern submarines, some of which were purchased from Russia and some domestically produced. Like its surface fleet, these boats deploy with short range, supersonic anti-ship cruise missiles (ASCM). If China can develop air-independent propulsion (AIP) technology for its diesel boats, it could markedly extend its operating endurance and vastly increase the complexity and duration of American anti-submarine warfare (ASW) operations. This expansion reveals an asymmetric approach to denying access to its coastal regions and its defensive chain, and it provides the PLA Navy with the ability to contend with efforts to interdict its SLOCs.[22]

The PLA Navy is producing four classes of submarines of varying sizes and missions. China has higher production rates than the United States for its undersea force and quite possibly a larger industrial building capacity in the event of an arms race.

- *Shang*-class (Type 093) nuclear-powered attack submarine (SSN)
- *Yuan*-class (Type 041) diesel attack submarine (SS)
- *Song* class (Type 039) diesel attack submarine (SS)
- *Jin*-class (Type 094) nuclear-powered, ballistic missile submarine (SSBN)[23]

Over the past 15 years, the Chinese have steadily placed into service 30 indigenously produced boats, about two boats a year. This buildup is in addition to the *Kilo*-class submarines they received from the Russians. These submarines represent a sizable advance in Chinese submarine capabilities, including quieter boats and the incorporation of the Russian-made SS-N-27 *Sizzler* ASCM.

Chinese officials have expressed significant interest in the development of an aircraft carrier.[24] The preparation of the older, former-Soviet *Varyag* for use as a training and experimentation ship indicates that the PLA Navy wants to develop this capability. Analysts think that China will pursue carriers, at least three of about 60,000 tons each. U.S. Chief of Naval Operations Adm. Gary Roughead has said "there is no doubt" that his counterpart in the PLA Navy wants a carrier.[25] While few dispute the ability of China's maritime industry to build such a product, there is little agreement on the timeline. For now, the consensus in the U.S. government and outside it is that China will not indigenously produce a carrier any earlier than 2015. However, by 2020 it could have several.

China's development of an anti-ship ballistic missile (ASBM) poses a unique threat to U.S. dominance of the maritime commons.[26] This breakthrough capability is consistent with PLA efforts to negate the existing advantages of America's naval preponderance in asymmetric ways. This land-based, mobile, long-range system is thought to be based upon the Dong Feng-21 family of ballistic missiles, exploiting China's growing surveillance and strike range. The missile has a range of 2,000 kilometers and is thought to possess a maneuverable re-entry warhead. Its complex guidance systems are linked to space-based control and intelligence networks that conduct initial target acquisition and guidance to the missile, giving it the ability to track and attack moving seaborne targets. Its size, extremely high speed (Mach 8 to 10), maneuverability and range have led Western naval analysts to label the evolving missile as a "carrier killer," and presume that its singular purpose is to threaten the current centerpiece of U.S. naval power projection operations: its 100,000-ton nuclear-powered aircraft carriers.[27]

If the Chinese could bring the ASBM to full operating capability, it could substantially negate much of America's existing edge in maritime power in the Western Pacific and profoundly affect maritime security and geostrategic stability in East Asia.

If the Chinese could bring the ASBM to full operating capability, it could substantially negate much of America's existing edge in maritime power in the Western Pacific and profoundly affect maritime security and geostrategic stability in East Asia. In operational terms, it would expand the anti-access capability and range of the PLA, and it would force U.S. naval planners to devote additional resources to defensive missions, potentially

Chinese Navy ship Qingdao (DDG 113) lowers a small boat during a search and rescue exercise with USS Shoup (DDG 86) off the coast of Southern California, Sept. 20, 2006.

(SA RAILYN C. RODRIGO/U.S. Navy)

compelling them to operate carriers from greater standoff range.[28] The commensurate shifts in doctrine, tactics, deception and defensive technologies for U.S. naval forces would be substantial and could undermine the large investment the United States has made in its Carrier Strike Groups — or negate its emphasis on sea basing.

Overall, China has made great strides with its naval modernization program. In short, China's Navy is not yet operationally mature but it is acquiring the necessary components of a full-fledged maritime power.[29] Its progress covers a broad range of capabilities, and investments in advanced and asymmetric systems designed to deny or contest access in the region remains a cause of concern for U.S. naval planners.

The PLA Navy is working to rectify its operational limitations in power projection and system integration with some sense of urgency and with substantial resources.[30] Also, it is working not merely to mirror the U.S. Navy, but to construct a uniquely Chinese model that serves its needs and interests and exploits its particular strengths. It should be judged on that basis, not American standards.

RUSSIA: THOUGH DOWN, THE BEAR REMAINS FORMIDABLE

Russia's naval capacity is about half that of the former Soviet Union, but its robust defense industrial base and a commitment to modernization from Moscow will make Russia a significant naval power in its own right, as well as a major proliferation source of high-end anti-access weapons. While Russia is currently suffering a severe economic relapse, President Dmitry Medvedev's regime is dedicated to a significant military modernization program. Russia retains a substantial defense industrial base capable of designing and manufacturing advanced military capabilities, including submarines, naval patrol aircraft, attack jets, integrated air defense systems and ASCMs for both its own use and for export. Russia's leaders have committed to significant increases in investment levels for military modernization.[31]

Experts debate whether Russia's "resurgence" is sustainable.[32] Russia faces rough times because of its lack of economic diversity and lack of foreign investment. It relies excessively on declining oil reserves to prop up the government's budget, but it will still be the world's largest exporter of natural gas for some time. Its prospects are dampened by a poor educational base, declining demographics, crumbling infrastructure and limited investment in public institutions such as health care.[33]

Yet Russia, with its large land mass, vast natural resources and a population of 140 million, is a strategic force. It has the human capital to produce an advanced military arsenal should it decide to devote the resources to do so. Clearly, its official pronouncements suggest it desires to retain its superpower status, and it would be imprudent to ignore Russia's sense of anxiety over its diminished status and its perception of encirclement.[34]

The Russian naval assets reflect Moscow's poor management of defense resources, with about 230 naval vessels in its total inventory.[35] This includes only 112 major combatants (see Table 1) A number of these ships are equipped with Russia's modern anti-ship missile systems. The U.S. Navy is increasingly challenged by this cruise missile threat.[36] However, the manpower and maintenance and operations funding for the fleet is greatly reduced, and many are laid up in reserve.

The Russian submarine fleet may be Russia's strongest naval asset, with the potential ability to contest the maritime commons. At present, the Russian Navy includes 11 nuclear ballistic missile submarines (SSBN). A new series, the *Borei* class, is in development. The first sub in the series, the *Yuri Dolgoruky*, already has been built and is undergoing tests. Two others have been started, but the *Bulava* missile designed to equip the new class has had numerous test failures. The fleet does have 14 modern *Akula* nuclear attack subs (SSN), which are roughly comparable to the American *Los Angeles* class. Naval intelligence reports also include eight SSGNs, which are nuclear subs with large loads of cruise missiles. Russia also has 20 *Kilo*-class diesel electric boats. However, patrols and training time have been curtailed and the operational effectiveness of the submarine force is considered questionable.

The surface fleet, however, is beginning operational deployments again. Over the past few years, the Russian flag has been deployed to Venezuela and Panama, as well as to Somalia and the Gulf of Aden for anti-piracy missions. This past summer, Russian submarines made their first patrols off the U.S. coastline in 15 years, and they were probably not looking to participate in the "cash for clunkers" program.[37] The Russians have also made port calls in France, Portugal, Syria, Turkey and Japan.

The deep decline of the Russian fleet has been halted, but not reversed. The potential exists for it to become a significant instrument in regaining Russia's lost prominence in foreign affairs. While its total inventory is modest in relation to the U.S. Navy, it should not be ignored.[38]

Table 1

COMPARATIVE NAVAL STRENGTH: MAJOR COMBATANTS[39]

BASIC SHIP CLASS	PLA NAVY	RUSSIAN NAVY	U.S. NAVY
Carriers	0	1	11
Submarines — Total	62	53	71
Submarines — Strategic	5	11	14
Submarines — Attack	57	42	57
CG	0	5	19
DDG	29	33	52
FFG	46	10	21
Amphibious	60	10	32

INDIA'S NAVAL EMERGENCE

India's Navy displays a growing reach and maturity, which could be a force for openness and stability of the commons if appropriately applied. It is the world's fifth largest fleet, and it incorporates sophisticated capabilities befitting India's growing political and economic importance.[40] Its fleet includes an aircraft carrier, about 40 surface combatants and 12 diesel submarines. While India's naval force is not considered a threat to U.S. security interests in any way (quite the contrary), China's strategists are concerned about the potential threat posed by the Indian Navy to Chinese SLOCs.

China's extended reach is of concern to New Delhi, and Indian naval modernization is likely to continue to be pegged to perceptions of Beijing's intentions. Each country is pursuing economic development and requires energy security to advance those interests. These ambitions could lead to a challenge for primacy in the maritime domain between China and India. Some analysts are concerned that "their concurrent entry into the nautical realm … portends worrisome trends" worsened by concerns that the U.S. Navy can no longer guarantee security in the region.[41] Chinese analysts point to India's naval plans and its geographic position astride critical lines of communication as an explicit shift east to thwart the development of the People's Republic of China. While a naval competition is not in the cards in the near term, there is a palpable amount of uncertainty about long-term stability.

Since India gained independence, its Navy was the most poorly resourced of India's armed forces. This is natural, given its large land borders and its identification of China and Pakistan as its most serious rivals. Defense spending has been rising at close to 10 percent each year since 2005, and the Navy is getting a larger share. Almost one-third of New Delhi's military spending today is devoted to modernization.[42] Much of the technology supporting this modernization has originated in Russia, which supplied a significant amount of its best aviation, submarine and cruise missile technologies.[43]

This higher resource level has allowed India's maritime leaders to implement the goals set forth in their 2007 *Maritime Military Strategy*. Their modernization plans call for India to possess a fleet centered on three aircraft carriers and 60 major combatants. One of the carriers is to be the *Vikramaditya*, formerly the Russian *Admiral Gorshkov*. The refit of the Russian vessel and a pair of domestic carriers appear to be delayed because of contractual and economic constraints. India is making more progress in upgrading its aged submarine fleet. Its current force of Russian-built *Kilos* and German-designed *Type-209s* are to be refurbished with land-attack missiles. The Indians plan to acquire six French submarines, but they also launched their own indigenously produced nuclear submarine—the *Arihant*, or "destroyer of enemies"—in July. The *Arihant* displaces 6,000 tons and is armed with 12 K-15 *Sagarika* missiles with a range of 700 kilometers.

Overall, India's modernization is purposeful but not ambitious. India seeks to contribute to cooperative security and to protect its substantial interests in the Indian Ocean. The key for the United States will be to engage India on the importance of maintaining the openness of the commons, building their capabilities, and helping New Delhi assure India's neighbors of its benign and constructive intentions.

Hybrid Maritime Threats

Defense scholars describe the emerging character of modern conflict as "hybrid warfare." This term attempts to capture the blurring and blending of previously separate categorizations of different modes of conflict. Hybrid wars are more than just conflicts between states and other armed groups.[44]

They incorporate a full range of modes of warfare, such as conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. Hybrid wars can be conducted by states and non-state actors. These multi-modal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battle space to achieve synergistic effects in the physical *and* psychological dimensions of conflict. The novelty of this combination, and the innovative adaptations of existing systems, is a further complexity. As one original and insightful student of war notes:

> Hybrid forces can effectively incorporate technologically advanced systems into their force structure and strategy, and use these systems in ways that are beyond the intended employment parameters. Operationally, hybrid military forces are superior to Western forces within their limited operational spectrum.[45]

The combination of irregular and conventional force capabilities, either operationally or tactically integrated, would pose a significant challenge to the openness of the maritime commons.[46] The war between Hezbollah and Israel in the summer of 2006 is an example of a hybrid threat against the commons.[47] Hezbollah incorporated a maritime dimension to that conflict by successfully engaging and striking an Israeli corvette at sea with an Iranian supplied anti-ship missile, probably a Chinese variant of the C-802 *Silkworm*. The Israeli ship, unaware that it needed to activate its missile-defense systems, was taken by surprise. Israel had always included a maritime element in its counter-terrorism defenses, but Hezbollah surprised it with such an advanced missile capability.

The combination of irregular and conventional force capabilities, either operationally or tactically integrated, would pose a significant challenge to the openness of the maritime commons.

There is a warning here for other advanced naval forces not to overlook defensive requirements against maritime armed groups or hybrid threats that possess state-like capabilities despite their relative small size or non-state status. Irregular warfare is becoming increasingly lethal and complex, a tactic employed not only by the weak but also the cunning.

Iran presents another example of a hybrid threat to the openness of the maritime commons. Iranian military capabilities include a small fleet of frigates and fast patrol craft, and a few submarines (including *Ghadir* midget boats and *Hahang* littoral subs armed with torpedoes).[48] Iran also possesses the world's fourth largest mine inventory, estimated between 3,000 and 5,000 mines. Its inventory includes as many as 1,000 Chinese EM11 influence mines and the EM52 rocket-propelled mine. In addition to advanced mines from China, Iran bought 1,800 mines from Russia in 2000. The World War I-era contact mines used in the 1980s by Iran are a thing of the past, though Iran's dominant geographical position in the Strait of Hormuz remains a relevant problem for maritime and energy security.

U.S. planners must be prepared to deal with both the formal Iranian Navy and the Iranian Revolutionary Guard in the tight waters of the Persian Gulf. Iran is able to constrict, if not deny, access to this critical area, given the geography of the Gulf and Iran's menagerie of means by which to produce maritime mayhem. Historically, the Iranians have proven to be tactically innovative with limited resources.[49] Iran's coastline and 17 islands provide numerous hiding places for small boats and fast attack craft. This is a classic "contested zone," as Tehran is fully aware.[50] In addition to mines, the Iranian naval arsenal includes a modest inventory of Chinese anti-ship cruise missiles, largely upgraded versions of the Chinese HY-2 *Silkworm*, and the *Noor*, which is an upgraded copy of the Chinese C-802.[51] Iran is also fielding the *Raad*, which has replaced the HY-2 *Seersucker*. With its 1,000-pound warhead and terminal maneuverability, the SS-N-4 *Raad* could prove deadly to even large warships. As one study recently concluded, the Iranians are growing dangerous but are certainly not omnipotent.[52]

Iranian military doctrine suggests that it will employ asymmetric and highly irregular tactics that exploit the constricted geographic character of the Gulf and the advanced systems that they have acquired.[53] This posits a significant anti-access threat to military exercises and commercial shipping. Swarming tactics employing the *Tareq* (Boghammer), *Zolghadr* speed boats, and *Azarakhsh* fast attack craft and the newer, low-signature North Korean-built IPS-16 torpedo boats could prove lethal to unsuspecting Western navies.

The Iranians do have limitations: the ability to coordinate such attacks to maximize their effect and a restricted capacity for many Iranian boats to launch ASCMs from over the horizon. However, with selected investments and a new asymmetric naval doctrine, the Iranians might be attempting to offset the quantitative and qualitative superiority of Western and Gulf naval forces. Here again, access to the global commons is at risk.

MARITIME ARMED GROUPS

Maritime Armed Groups also challenge the international community's access to, and the conduct of economic activity within, the maritime commons.[54] These groups include pirates, as well as the rare but notable maritime terrorists and insurgents from the sea.

Piracy and other forms of maritime lawlessness do not directly endanger America's vital interests. However, they do undermine the openness and stability of the maritime commons, which threatens the safety of civilians and the freedom of navigation, plus commercial transportation, energy security and vital sea lines of communication. While many analysts tend to dissect each of the maritime threats (piracy, terrorism and insurgency) individually, the cumulative impact is obviously of enough concern for more than dozen nations to send their naval warships to the Gulf of Aden to secure their interests. China was concerned enough to initiate a three-ship task force to the region.

The maritime commons is at risk at its edges and transition points from small maritime armed groups. They have different agendas and aims, but their tactics, techniques and procedures are often the same, and they all cause increased instability, higher costs upon transportation networks and weaker security. The maritime security community is only slightly concerned about the overall increase in criminal activity in this arena. However, the anti-terrorism community is increasingly aware of the openness of the maritime transportation and commercial sectors, as either targets or potential channels through which armed groups can maneuver an "avenue of approach." Many will agree with counterterrorism expert Rohan Gunaratna's conclusion that "more armed groups are likely to mount guerrilla and terrorist tactics in the maritime domain in the future."[55]

The threat of piracy has drawn significant amounts of attention lately.[56] Almost 2,000 acts of attempted or successful piracy have occurred since 2003. The average annual rate is about 300 acts of piracy. Experts suggest that this rate is in fact higher as commercial carriers are reluctant to publicize their losses and the attendant security problem.[57] The International Maritime Bureau's Piracy Reporting Centre (IMB-PRC) reports that the incidence of attacks by pirates for the first nine months of 2009 exceeded the 2008 total.[58] More than 300 incidents were reported by October. Worldwide, piracy had fallen off after a spike in the early 2000's, largely because Indonesia and its neighbors suppressed pirates around the Southeast Asian straits. Now the greater problem exists in the Gulf of Aden and the Horn of Africa. Of the 293 attacks (attacks, attempted attacks and suspected attempts) during 2008, 37 percent occurred in this area. The International Maritime Organization (IMO) reports that the number of acts of piracy and attempted acts increased by 8.5 percent in 2008, though the number of successful attacks declined a bit.[59]

Increased levels of pirate activity off the coast of Somalia and the Gulf of Aden are notable, despite heavy attention by international officials and significant naval protection. In 2009, there has been a surge in activity off the east coast of Somalia: The number of attacks more than doubled, with 47 attacks in the first three quarters of 2009 compared to 19 in 2008. Likewise, incidents in the Gulf of Aden have doubled in 2009.

Table 2

ACTS OF PIRACY BY REGION AND YEAR

REGION	2003	2004	2005	2006	2007	2008	2009*
Far East	4	11	10	2	3	0	18*
Southeast Asia	185	162	112	86	77	62	32*
South Asia	87	32	37	53	30	23	22*
Middle East	3	5	12	7	11	?	15*
East Africa	29	15	53	29	66	42	153*
West Africa	64	58	27	32	54	61	32*
Latin America	71	44	25	29	21	17	28*
Other	2	2	0	1	1	1	6*
TOTAL	**445**	**329**	**276**	**239**	**263**	**206**	**306***

Source: International Maritime Organization. *Year to date, Jan. 1 – Sept. 30, 2009.

One daring act of piracy demonstrates the rising lawlessness. The *MV Faina*, a Belize-flagged Ukrainian vessel carrying military weapons, was seized off the Horn of Africa in late September 2008. The ship was carrying modern T-72 tanks and munitions to an unknown purchaser. The crew of 20 was held for ransom, and after a four-month standoff, the pirates received a 3.2 million dollars payoff delivered by parachute in exchange for the safe return of the ship, its cargo and its crew. As a pair of U.S. Navy ships stood nearby, the Somali pirates raced off. At the time, another 150 seamen were still being held prisoner ashore or on other pirated vessels.

The threat of piracy hit the front pages of American newspapers in April 2009 when pirates managed to get aboard the U.S. -flagged cargo ship *Maersk Alabama* about 400 miles east of Mogadishu. This was the first seizure of a U.S. crew around the Horn of Africa in modern times. The next day, the American destroyer *USS Bainbridge*—interestingly, named for a U.S. naval officer who defeated African pirates in the early 1800s off Tripoli—arrived. The pirates took the ship's captain as a hostage and attempted to negotiate for his ransom. After a few tense days, a team of Navy SEALs killed three of the pirates and a fourth was taken to the United States for subsequent prosecution.

Another notable case included the seizure of the tanker *Sirius Star* in November 2008. The hijackers in this case used a modern tugboat as their "mother" and loaded their arms into rubber boats for the attack. Surprising the crew, they managed to overtake the 300,000-ton tanker about 450 nautical miles out at sea. They commandeered the vessel, with its 25 sailors and two million barrels of crude oil worth over 100 million dollars. The pirates asked for a ransom of 25 million dollars, the biggest prize ever seized by pirates. The attack not only provided evidence of the increased range and brazenness of the scourge of piracy, but it also highlighted the increased vulnerability of energy lines of communication.[60]

Since late last year, an international force has tried to stem the impact of these piracies off the coast of Somalia. An international task force of as many as 20 ships has patrolled an area about four times the size of Texas. Naval participants in the combined task force included the United States, Turkey and Denmark. Other naval vessels have been supplied by China, Russia, India, Japan and South Korea.[61]

The task force scored some victories, foiling at least three hijackings and capturing 16 pirates in March before the *Maersk Alabama* incident. The number of successful attacks went down in the area patrolled by the task force, but the pirates simply shifted their efforts to an area off the coast of southeastern Somalia and managed to capture six ships in a single week.

One of the trends that cannot be overlooked includes threats to merchant sailors and cruise lines. The levels of violence have notably increased, with pirates willing to fire directly on ships and crews. While limited to small boats, the pirates are able to venture nearly 400 miles at sea, and they are prepared to employ modern technologies to navigate, operate or negotiate for their ransoms. The pirates are going after bigger targets as well, including crude-oil carriers.

Officials with the IMB credit the international naval community for reducing the number of successful hijackings, but note that the increase in attempted attacks suggests that naval patrols are only part of the solution. Piracy has not yet been deterred by this concerted effort. Most analysts contend that piracy is fundamentally an economic problem and that it cannot be solved at sea. Business appears to be booming—Somali pirates are estimated to have garnered 20 million dollars in ransom in recent years. Estimates of the total costs to industry range from 13 billion to 25 billion dollars, with little consensus on the true cost of longer routes, larger labor costs, impeded shipping, late deliveries and higher insurance premiums. Furthermore, the pirates' success rate has been lowered in 2009, but the increase in violent incidents suggests that pirates are more than willing to escalate the attacks and pursue larger ships at greater range.

Today's Somali corsairs could be laughed off as a transitory threat. Indeed, many naval analysts have been downplaying the threats posed by seaborne criminals and insurgents for some time.[62] However, today's lawlessness bears little resemblance to Johnny Depp's Capt. Jack Sparrow in "Pirates of the Caribbean." These primitive swashbucklers undermine the security of the commons and undercut the freedom of navigation and international trade that depends on it. Additionally, the costs of these acts are more than just commercial. In 2008, 815 crew members were taken hostage from vessels hijacked in this region. This represents a 207 percent increase over 2007.[63] In the first three quarters of 2009, 661 crew members have been seized, 12 kidnapped, six killed and eight remain unaccounted for.[64]

As Robert Kaplan, a senior fellow at the Center for a New American Security, notes:

> That a relatively small number of pirates from a semi-starving nation can constitute enough of a menace to disrupt major sea routes is another sign of the anarchy that will be characteristic of a multipolar world, in which a great navy like America's — with a falling number of overall ships — will be in relative, elegant decline, while others will either lack the stomach or the capacity to adequately guard the seas.[65]

Pirates are not the only form of a maritime armed group. A number of terrorist organizations have exploited maritime attacks, including Hamas, Hezbollah, Abu Sayyaf, al Qaeda and the Liberation Tigers of Tamil Eelam (LTTE). At one time, the latter possessed a strong brown-water capability for both support and attack operations. Its recent demise eliminated its base of operations and has decimated its leadership, but has not dimmed the example set by its Sea Tigers. The LTTE fielded small boat squadrons for years, assisted by other states, such as India, and by hiding its boat production capacity in New Zealand.[66]

Many terror organizations have been using maritime transportation assets to transport their weapons or operatives between regions, but now some seem willing to apply their limited but growing awareness of the sanctuary of the commons to gain an operational advantage. For instance, the Moro Islamic Liberation Front, Jemaah Islamiyah and ASG have used the waters of their respective areas as a means of maneuvering their resources. Abu Sayyaf took credit for the attack on the Philippine Superferry 14 in 2004, killing 114 passengers. The attacks in Mumbai in November 2008 were abetted by the seizure of a local fishing boat, the *Kuber*, the captain of which was killed. This host, or mother ship, was then used to launch several simultaneous assaults from small boats into the port area.[67]

Nigeria's insurgent group, the Movement for the Emancipation of the Niger Delta (MEND) has proven to be effective at mounting riverine and littoral operations. MEND has mounted patrols and attacks on oil facilities to extort resources or to abet its political agenda. It has conducted singular or swarming attacks of small boats with a range of 75 nautical miles. Its operations have occasionally interrupted or degraded the operations of Nigeria's oil production and distribution facilities.[68] This has slowed energy shipments that are increasingly important to the United States. The west coast of Africa is the source of about 15 percent of American oil imports, making it almost as important as Saudi Arabia to U.S. energy requirements.

Maritime terrorism is certainly rare but it can be occasionally highly successful, as demonstrated by the al Qaeda cell that attempted to attack the USS *Sullivan* and struck the USS *Cole* in Aden in October 2000.[69] That attack killed 17 U.S. sailors and sent a strong signal to the world's navies to take seriously the threat of terrorism at or from the sea. Another signal of the growing vulnerability of the commons was al Qaeda's somewhat successful assault in October 2002 on the *MV Limburg*. The 150,000-ton crude-oil tanker was rammed by a small suicide boat in the Arabian Sea off of Yemen. It produced a spectacular fire and great imagery for al Qaeda's exploitation, but it did not destroy the ship; one crewman was killed. It was a signal that al Qaeda was capable of mounting attack operations against energy targets. Their online chatter continues to feature discussions of attacks on energy networks, despite the loss of its Prince of the Sea, Abu Nasihari, al Qaeda's alleged maritime strategist.

The maritime security community is not alarmed, nor has it reached a consensus on the scope of the threat, and cannot determine if acts of terrorism will be centered in the Middle East, the west coast of Africa or in Southeast Asia. Dr. Martin Murphy, author of *Contemporary Piracy and Maritime Terrorism: The Threat to International Security*, is rather optimistic but is concerned by the use of the sea as a base for terrorism. He has recently made the observation that

> The most significant insurgent challenge in the near term might well come from jihadist groups. One of the most distinguishing features of jihadist insurgency is its global outlook. Organizations such as al Qaeda are skilled at opening new fronts in their war where they detect opportunity, observe weakness or are able to find local allies.[70]

Experts confirm this assessment, noting an ongoing emphasis on attacks with large economic consequences among al Qaeda and its affiliates.[71] This is nothing new for Osama bin Laden, who, well before Sept. 11, 2001, berated the United States as a "paper tiger" that could be subjected to a series of attacks and provocations to place it on the verge of financial ruin and collapse. U.S. intelligence officials would agree that such an attack would be consistent with al Qaeda's purported "bleeding strategy" designed to impose costs on the United States and its allies.[72] Since its attacks on the World Trade Center in 1995, al Qaeda has demonstrated an interest in undercutting principal components, if not symbols, of the American economy. RAND Corp.'s maritime security expert, Peter Chalk, concluded, "Attacking key pillars of the Western commercial, trading and energy system is a theme that, at least theoretically, has become increasingly prominent in the years since 9/11, and that is viewed as integral to the Islamist war on the United States and its major allies."[73]

Additional factors suggest that acts of violence by maritime armed groups may increase. The potential for a violent but visibly public act can draw publicity to a group if it is effective at gaining imagery and exploiting "propaganda of the deed." Maritime terrorism holds potential for that type of act, including seizure of a large number of hostages on a cruise liner or ferry, which are vulnerable and accessible options to gather a large number of innocent passengers in a confined space. Arguably, the skill sets for such an attack are less technologically challenging than seizing and flying an airliner into a building.

The potential for economic and environmental disaster is substantial. Significant disruptions or degradation of a regional hub or a critical energy SLOC could result in economic destabilization. Were this to occur in a principal commercial port or a critical oil-production center, the cascading economic effects could be significant but probably only temporary. A RAND team has identified the increased focus by al Qaeda on attacks that yield magnified economic consequences.[74]

Criminal organizations and criminal insurgencies are also finding opportunity and room to maneuver in the maritime domain. Narco-insurgencies are becoming transnational businesses, and they continue to develop fresh markets, explore alternative routes and refine current tactics. They are highly innovative and invest in relatively low-cost, unique platforms to counter detection efforts. They utilize self-propelled semi-submersibles (SPSS)—low-profile vessels can avoid visual and radar detection. These vessels now bring tons of illicit cargo to market. In 2008, U.S. Southern Command reported interdicting 11 SPSSs on their way to market, and it anticipates about 60 similar vessels will hit the waters in 2009, each with a potential cargo capacity of more than 330 metric tons of cocaine.[75]

While piracy and maritime terrorism are annoyances today, the domain will likely remain a theater for armed violence, "due to its openness, low levels of security, and its contribution to an international system that some groups want to preclude from interacting with their area."[76]

ANARCHY IN THE ARCTIC?

The only thing in the Arctic melting faster than the northern ice cap is the international comity, and the region is suffering from benign neglect. Global climate change is causing unprecedented alterations to the geography of the maritime commons, with profound implications for access to resources, the application of naval power, and geopolitical stability. The melting ice cap has opened up the region for short periods. Now it is beginning to dawn on several countries that this ecosystem disaster could have a silver lining. What was once a part of an untapped commons is now increasingly being contested. Sovereignty and border disputes have existed for years without resolution. Canada and the United States have conflicting interpretations of international law over waterway rights and access. The Russians and Danes, and the Russians and Norwegians, have competing boundary claims. The United Nations has attempted to bring some order out of these claims but with limited progress.[77] The resulting race has significant natural security implications for this country. This is not news to maritime strategists in the United States. As noted in the latest U.S. maritime strategy, the developments in this region pose "potential sources of competition and conflict for access and natural resources."[78]

> *With higher crude oil prices and projected energy shortages looming, the economic potential of the entire Arctic Circle is being eyed by numerous countries. Some estimates suggest that as much as 25 percent of the globe's untapped energy resources could be found there.*[79]

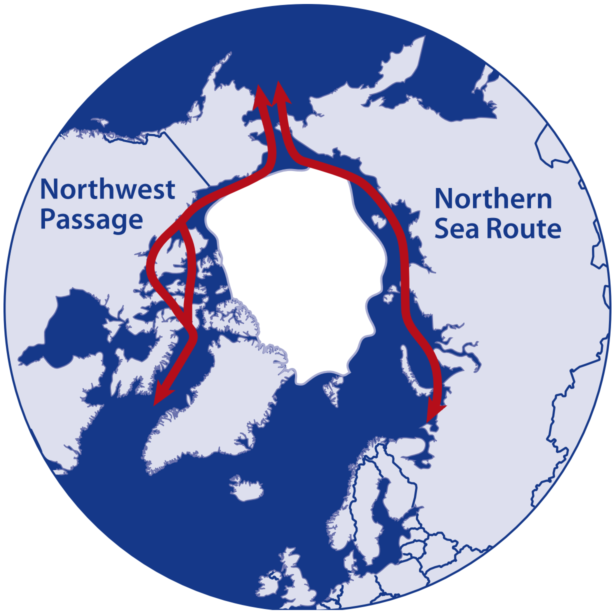
Access to heretofore inaccessible regions could become viable over time if trends continue. With higher crude oil prices and projected energy shortages looming, the economic potential of the entire Arctic Circle is being eyed by numerous countries. Some estimates suggest that as much as 25 percent of the globe's untapped energy resources could be found there.[79] One U.S. government analysis has concluded that there are likely to be no more than 90 billion barrels of accessible crude oil in the region, which is about what Russia (the world's second-largest producer) has remaining in its proven reserves.[80]

A succession of record summer temperatures has occurred over the past decade. In 2005, the Northeast Passage opened up along the Eurasian border for the first time in recorded human history. The famous Northwest Passage along Canada opened up for the first time in 2007, revealing potential transportation corridors of significant savings in time and fuel. Both of these passages were briefly open simultaneously (Figure 1). Although they are generally not navigable today, research and military vessels have transited through these passages during the past few years. There continues to be potential for ice-free conditions during the summer in the Arctic.

As the ice coverage has decreased dramatically in the Arctic, the possibility of more efficient international trade routes, like the Northwest Passage, are evident. Who owns, controls, and manages these waterways? The answer could be of strategic interest to America's trading partners and competitors. At present, there is little agreement on who should patrol and secure these routes—and the United States is not presently prepared to offer assistance in this area because of its antiquated icebreaking fleet. Russia, on the other hand, is prepared to secure its northern flanks and to support its claims to an Exclusive Economic Zone (EEZ) that could assure it strategic leverage with access and control over a vast resource base. Canada now plans to improve its ability to operate in Arctic waterways that are ever so slowly expanding as the frozen ice mass shrinks to its north.

The Russians, not surprisingly, have begun to take matters into their own hands. They have literally marked their claim by planting a Russian flag onto the deep ocean sea bed. In 2007, a Russian mission with two mini-submarines staked out the Kremlin's claim to the region with a 4-kilometer descent to the sea bed floor, where geological samples were collected; the Russians also dropped a titanium canister containing the Russian flag.

Figure 1: Impact of Melting Ice Cap on International Trade Routes.



Cartographer Hugo Ahlenius, UNEP/GRID-Arendal, http://maps.grida.no/go/graphic/arctic-sea-routes-northern-sea-route-and-northwest-passage.

They have published a national policy on the Arctic region, identifying this area as a "strategic resource base," and their latest national security strategy noted ominously, "With the ongoing competition for resources, attempts to use military force to solve emerging problems cannot be excluded."[81] Russia will modernize its icebreaker fleet and station more researchers in the Arctic as part of its push to stake its claim to the vast resources of the disputed polar region.

One might be tempted to overlook this statement as Russian rhetoric, except that the Kremlin has increased its military presence in the area (largely by maritime air patrols) and has announced the creation of a dedicated military force to patrol this contested corner atop the globe.[82]

America's reaction to this international security challenge has been sluggish. The George W. Bush administration in its waning days articulated the U.S. Arctic Policy. This policy tasks the secretaries of State, Defense, and Homeland Security, in coordination with heads of other relevant executive departments and agencies, to:

1. Develop greater capabilities and capacity, as necessary, to protect United States' air, land, and sea borders in the Arctic region.

2. Increase Arctic maritime domain awareness in order to protect maritime commerce, critical infrastructure, and key resources.

3. Preserve the global mobility of United States' military and civilian vessels and aircraft throughout the Arctic region.

4. Project a sovereign United States maritime presence in the Arctic in support of essential United States interests.

5. Encourage the peaceful resolution of disputes in the Arctic region.[83]

However, few forces or additional resources are being applied to implement this policy. The U.S. Navy has no ships prepared to operate in this area, though its aviation and submarine forces offer valuable assets—within limits. The U.S. Coast Guard keenly appreciates the transportation, commercial and public safety missions that are implicit in this region's growing importance, but it would require additional funding to advance American interests with confidence.[84]

Recommendations

Establish Robust Strategic Posture and Presence. In the coming decades, challenges in the maritime commons could lead to both traditional security missions and expanded demands for credible and competent maritime services, such as humanitarian assistance, disaster relief, freedom of navigation assurance, counterpiracy operations, and basic deterrence and dissuasion activities. Unfettered access to the Pacific and Indian oceans, as well as the Persian Gulf, remains critical to the international economic system and international stability more broadly.[85] The U.S. Navy and its maritime partners should be postured to best secure American interests in these regions and resourced accordingly. Preserving access and freedom of action in these regions should be a critical objective of American strategy.

As the Arctic melts, the area could become a flashpoint for renewed United States-Russia naval competition. American military leaders hope for a cooperative environment.[86] But as climate change continues, it will free up the Arctic for naval transit and become an important location for commercial traffic. The U.S. Navy and Coast Guard must adapt to this new environment and prevent naval competition from escalating in ways that damage the broader U.S.-Russian relationship.

Increase and Re-focus U.S. Maritime Security Investments. The United States should provide maritime services with sufficient resources to sustain adequate force levels and initiate long-delayed modernization efforts. Hard tradeoffs necessitate the acquisition of crucial programs at the expense of desirable capabilities. The current fleet provides a balanced force capable of forward presence and deterring major conflicts, but it needs additional resources to maintain its current technological edge and global reach.[87]

As noted by the chief of naval operations, sea control in key regions is at risk. If the United States is to exploit the sea as maneuver space and secure the commons, it must counter potential adversaries' missile capabilities, which demonstrate increasing reach, mobility, accuracy and lethality. In addition to strengthening ballistic and cruise-missile defensive systems, the Navy needs to reestablish itself in anti-submarine warfare and in littoral dominance in order to assure sea control. Ongoing programs, including the Littoral Combat Ship, would add

If the United States is to exploit the sea as maneuver space and secure the commons, it must counter potential adversaries' missile capabilities, which demonstrate increasing reach, mobility, accuracy and lethality.

greatly to American capabilities in these areas. The Coast Guard's major capitalization program needs greater funding to improve its endurance, range and sustainability. The Navy should also consider investing in other valuable capabilities, including rotary wing systems, unmanned systems and icebreaker capacity, to protect the maritime commons.

U.S. maritime capacity in the Arctic is insufficient and falls short of Russia's. American assets for presence and surface maneuvers in Arctic waters are limited in comparison. The U.S. Coast Guard owns three conventionally-powered icebreakers, but only two are operational. A more robust operational icebreaker fleet is essential for supporting U.S. military operations, maintaining American presence, and preserving U.S. economic and other interests throughout the region. Coast Guard investments in new icebreakers might not be enough. Ship-hardening requirements for both surface vessels and submarines should also be considered. Greater deployment options in the region may also be required, but until the impact of climate change is better understood, investments should be prudent and focused on better domain awareness and scientific research.

Protect the Littorals. The commons is *not* synonymous with blue water. Dominance in the open oceans may not ensure access to the great highway if it is contested in the littorals, deltas, crucial narrow or the roads that connect to most international trading hubs.[88] Access can be limited or challenged at ports, at either end of a shipment.[89]

In a neo-Mahanian world, the United States will need more than a navy that excels at traditional sea-control missions. Challenges to the openness of the maritime commons could increase instability throughout the developing world. Economic and environmental disputes could create maritime crisis situations (for example, in the Arctic, in the Strait of Hormuz, or in the South China Sea) that draw in the United States and risk escalation. Or, disputes over access to resources (fisheries, sea beds or oil deposits) and resource development within Exclusive Economic Zones could lead to conflicts between foreign navies that require American intercession or mediation to help prevent escalation. The United States will need the ability to maintain a naval presence and work cooperatively with foreign navies in littoral environments and contested zones.

Engage Existing Partners and Form New Partnerships. As Secretary of Defense Robert Gates recently said, "Whether on the sea, in the air, in space, or cyberspace, the global commons represent a realm where we must cooperate—where we must adhere to the rule of law and the other mechanisms that have helped maintain regional peace."[90]

The *National Defense Strategy* and the triservice maritime strategy advocate indirect approaches to solving security problems. In the naval realm, the United States should build up the capacity of friends, partners and allies to enhance maritime and natural security. Increased partnership will help to prevent maritime security challenges and facilitate prompt and cooperative responses when such challenges arise.[91]

The United States should also expand efforts to address nontraditional challenges, including maritime, energy and natural security, with its partners.[92] In order to enhance maritime security and reduce acts of violence and piracy at sea, maritime services should:

1. Prevent pirate attacks by reducing the vulnerability of the maritime domain.
2. Significantly enhance maritime domain awareness efforts.
3. Interdict acts of piracy consistent with international law and the rights and responsibilities of coastal and flag states.
4. Ensure that those accused of piracy are held accountable by facilitating prosecution of the suspected pirates in a just forum.

Like many challenges in the national security arena today, addressing transnational maritime threats requires a coordinated government approach that integrates the military, law enforcement, the judiciary, diplomacy, information activities and commercial interests.

American maritime services can do much to eliminate "shadow zones," or areas without persistent coverage by sensors, via cooperative engagement initiatives. But efforts should be concentrated in the Pacific and Indian oceans.[93] To do this, American strategists should engage American allies and friends in the Asia-Pacific arena.[94] With adroit U.S. engagement and astute capacity-building, these allies and friends can effectively preserve international maritime access in the Asia-Pacific. The United States also should continue to expand its engagement with China by enabling China's broader integration into the global system.[95] This engagement will necessarily be matched with involvement of the PLA Navy, to encourage its development as a force for openness and stability, not anti-access and exclusivity.

Elsewhere, the maritime services should continue to explore innovative initiatives to increase security cooperation and engagement options in the littorals and beyond.[96] The Navy Expeditionary Combat Command should be adequately resourced to ensure it can contribute to the effort, and programs such as the Global Fleet Station (a maritime security initiative aimed at strengthening global partnerships through training and cooperation activities) should be evaluated and institutionalized.[97]

The Department of Defense and Department of Homeland Security should expand military-to-military contacts and policy interactions with friends and allies that increase maritime domain awareness and interoperability. The United States should strongly consider working with nations such as Russia and China, which may not qualify as formal allies but which share common interests in using the global commons for peaceful pursuits. Efforts to provide maritime security as well as humanitarian operations in environmental crises build confidence and reduce threats and burdens. The United States should take up the offer by senior Chinese officials to strengthen regional security organizations and cooperation venues.[98] To the maximum degree possible, the United States should promote exercises and programs to establish and sustain interoperability in the maritime domain. The principal thrust of this effort should be part of a wider strategy that seeks to attract allies into a series of cooperative projects.[99] If the United States can build up the capacity of global navies to work with it to increase the speed, skill and volume of assistance to humanitarian and environmental crises, U.S. forces will not have to extend themselves as often or as far. Regular cooperative exercises that emphasize the skill development of potential partners in humanitarian crises prepare others to share the burden of response around the globe.[100]

Promote Multilateral Approaches to Maritime Security. In addition to bilateral engagement of allies and partners, the United States must continue to seek cooperative multilateral approaches, especially in Asia.[101] The governance of the maritime domain requires a multilateral collaborative effort and greater awareness, which can be instigated and supported by the United States. Washington should consider promoting the development of a maritime security index. This initiative would give equal weight to economic, environmental and security indices as a composite mechanism to gauge maritime challenges in a more holistic manner. The UN or other regional bodies could use this as an early warning system or triggering mechanism to initiate collective responses to criminal activity, environmental crises or threats to freedom of navigation in critical areas. Such a mechanism might be tied to a broader interpretation of the UN's "responsibility to protect" doctrine. This governance proposal would permit intervention in territorial waters where a sovereign nation has demonstrated an inability to preserve security and risks have risen to the point where international attention is warranted.[102]

Ratify the UN Convention on the Law of the Sea. Considering the strategic importance of the oceans for U.S. security and economic interests, it is imperative that the Senate ratify the UN Convention on the Law of the Sea (UNCLOS).[103] Doing so will benefit immediate U.S. national security interests and lay the groundwork to build up cooperative efforts to minimize conflict over the long term.[104]

Additionally, the treaty facilitates economic and environmental objectives. In order to give the United States equal access and protection to the global maritime commons, including the resource-rich sea beds of the continental shelf, Washington needs to shape and join the major international governance mechanisms set up with the UNCLOS treaty, which secures rights for commercial and military vessels at sea, and minimizes investment risks for potential development.

Not surprisingly, the leadership of the U.S. Navy has advocated UNCLOS ratification. America's nonparty status contradicts its strategy and narrative about cooperation and the rule of law.[105] As one defense official put it recently, it is not enough just to play by the rules—the United States must champion the rules and lead efforts to adapt to the international rules when necessary.[106] At present, American has abandoned its seat at the table and forfeited the opportunity to shape international policy.

The United States should continue to advocate for freedom of navigation in international waters, including Exclusive Economic Zones, and resist encroachment by coastal states with excessive claims. While ratification of UNCLOS will support U.S. claims when it comes to behavior within EEZs, regular operations within these areas would demonstrate America's commitment to openness within the maritime commons.

Conclusion

The robust naval heritage established by geostrategists like Mahan and Mackinder, which many Americans take for granted today, has maintained the openness of the maritime commons and provided an unparalleled capacity to leverage the oceans for diplomatic influence, commercial gain and security. Yet, the emergence of state and non-state maritime threats has made the "wide commons" less stable and secure than it once was. The openness of key oceanic highways, along with critical lines of communication, could be in jeopardy, and the situation is complicated by congested energy corridors and a few chokepoints. Geography, abetted by geology, demographics and economic needs, will produce unwanted but inescapable tensions in the near future. To ignore these realities is to ignore a looming challenge of our age.[107]

Over the past decade, the United States has devoted a great deal of strategic attention to two protracted campaigns in Iraq and Afghanistan. Maritime security and the preservation of the global commons has been, per necessity, a lower priority. However, as this diagnostic assessment reveals, this is not a prudent long-term strategy because it might allow the great sea highways and their narrows to become restricted or entirely contested.

This is not a post-naval or post-oceanic era. The maritime commons has become *more* important, not less. The competing major powers will depend more heavily on the sea for their critical energy imports.[108] At the same time, threats to access to the commons are increasing, and it is no exaggeration that a tipping point has been reached in East Asia.[109] Access is contested in the shallow brown-water littorals and natural geographic chokepoints. Stability and security will more often be contested directly or indirectly in open blue-water environments as well. In a neo-Mahanian age, the international community must secure both the commons and its contested zones when necessary. It must be recognized that operating in the maritime domain is not independent of the other "contested commons." Preserving and leveraging a competitive advantage in the cyber and space domains is required to operate effectively at sea and in the crowded littorals.

The international community in general, and the United States in particular, benefit greatly from the stability afforded by a secure maritime commons. American security interests are advanced by the ability to negate or counteract efforts by state and non-state actors to disrupt access to, or the ability to operate within, the commons. This freedom of movement and capacity to respond remains a crucial element of U.S. economic prosperity and American interaction with the global community, and a fundamental basis for the continued ability to deter aggression and reassure allies.

Without the ability to generate and apply military superiority at sea, to transport or sustain forces, or to engage aggressors, the United States would not be able to secure or advance its interests.

Without the ability to generate and apply military superiority at sea, to transport or sustain forces, or to engage aggressors, the United States would not be able to secure or advance its interests. Without the capacity to ensure access when and where needed, the United States will surrender its position as a final guarantor of stability to an international system that is largely reliant upon the use of Mahan's "great highway."[110] Unfettered access to the global commons is and will be more frequently challenged, and traditional approaches could less effective than the past.[111] Creative concepts to overcome challenges are necessary to preserve American access and influence in critical regions.

Failure to recognize these strategic challenges will have far reaching consequences for the exercise of American power and the maintenance of the maritime commons. An eclipse of U.S. power will impair America's ability to assist allies, preserve stability and secure global economic prosperity. An urgent and proactive strategy is needed, in concert with American allies and friends, to maintain access to the maritime commons.

ENDNOTES

[1] Mackinder, cited by Dr. Chris Seiple, *Revisiting the Geo-Political Thinking of Sir Halford John Mackinder: United States — Uzbekistan Relations 1991–2005*, dissertation, Medford, MA: Tufts University, Fletcher School of Politics, p. 229. Accessed at http://www.globalengage.org/assets/7DBF5E01-F4AB-4878-B3F5-8F1EB95C8AA7.pdf.

[2] Cited by Francis Sempa, "Mackinder's World," 2. Accessed at http://www.unc.edu/depts/diplomat/AD_Issues/amdipl_14/sempa_mac2.html.

[3] Thomas Friedman, *The World is Flat, A Brief History of the Twenty-First Century, (*New York: Farrar, Straus and Giroux, 2005).

[4] Colin S. Gray, "In Defence of the Heartland: Sir Halford Mackinder and His Critics a Hundred Years On," *Comparative Strategy*, Vol. 23. Issue 1, (January 2004): 9-25; Mackubin Thomas Owens, "In Defense of Classical Geopolitics," *Naval War College Review*, Vol. 52, No. 4, (Autumn 1999).

[5] *The National Strategy for Maritime Security,* Washington, DC: The White House, (September 2005): 7-8. Accessed at http://www.dhs.gov/xlibrary/assets/HSPD13_MaritimeSecurityStrategy.pdf.

[6] Robert Kaplan, "America's Elegant Decline," *The Atlantic Monthly*, (November 2007): 110.

[7] Cited by Francis Sempa, "Mackinder's World," (2). http://www.unc.edu/depts/diplomat/AD_Issues/amdipl_14/sempa_mac2.html.

[8] According to *Lloyd's List*, (Maritime Intelligence Unit) London, UK, (5 December 2007), http://www.lloydslist.com/lmiu/Article/20017485999/index.htm.

[9] James R. Holmes and Toshi Yoshihara, *Chinese Naval Strategy in the 21st Century: The Turn to Mahan*, London: Routledge, (2008).

[10] George Baer, "Notes Toward a New Maritime Strategy," *Naval War College Review*, (Spring 2007): 19.

[11] Fareed Zakaria, "The Future of American Power: How America Can Survive the Rise of the Rest," *Foreign Affairs*, (May/June 2008).

[12] National Intelligence Council, *Global Trends 2025: A Transformed World*, Washington, DC: GPO, (November 2008): 29-34. Gen. James N. Mattis, The Joint Operating Environment 2008, Suffolk, VA (December 1 2008): 26-32.

[13] For an updated assessment of this threat see Andrew S. Erickson, Lyle J. Goldstein, and William S. Murray, *Chinese Mine Warfare, A PLA Navy "Assassin's Mace" Capability*, Newport, RI: Center for Naval Warfare Studies, Naval War College, China Maritime Study No. 3, (June 2009).

[14] David A. Shlapak, David Orletsky, Toy I. Reid, Murray Scot Tanner, and Barry Wilson, *A Question of Balance, Political Context and Military Aspects of the China-Taiwan Dispute*, Santa Monica, CA: RAND, (2009).

[15] Information Office of the State Council of the People's Republic of China, *China's National Defense in 2008*. Beijing, China, (January 2009): 4, http://www.fas.org/programs/ssp/nukes/2008DefenseWhitePaper_Jan2009.pdf.

[16] Andrew Erickson and Lyle Goldstein, "Gunboats for China's New 'Grand Canals'?, *Naval War College Review*, (Spring 2009): 43-76. David Lai, "Chinese Military Going Global," *China Security*, (Winter 2009): 3-9.

[17] Eric A. McVadon, "China's Navy Today: Looking Toward Blue Water," p. 391, in Andrew S. Erickson, Lyle J. Goldstein, and Carnes Lord, eds., *China Goes to Sea: Maritime Transformation in Comparative Historical Perspective*, (Annapolis, MD: Naval Institute Press, 2009).

[18] Dennis Blair, Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence, (12 February 2009): 23. See also Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China, 2009*, Washington, DC, I; Mark Cozad, "China's Regional Power Projection: Prospects for Future Missions in the South and East China Seas," in Roy Kamphausen, David Lai, and Andrew Scobell, eds., *Beyond the Strait: PLA Missions Other Than Taiwan,* (Carlisle, PA: Strategic Studies Institute, April 2009).

[19] Ronald O'Rourke, "China Naval Modernization: Implications for U.S. Navy Capabilities-Background and Issues for Congress," Washington, DC: Congressional Research Service, RL 33153, (19 November 2008).

[20] I am indebted to Capt. Bud Cole, USN (ret.) of the National Defense University for insights on the scope of Chinese naval modernization.

[21] On Chinese maritime strategy see David Lei, "China's New Multi-faceted Maritime Strategy," *Orbis*, (Winter 2008): 139-157; and Toshi Yoshihara and James Holmes, "Command of the Sea with Chinese Characteristics," *Orbis*, (Fall 2005): 677-694.

[22] Lyle Goldstein and William Murray, "Undersea Dragons: China's Maturing Submarine Force," *International Security*, Vol. 28, No. 4, (Spring 2004): 161-196; James Clay Moltz, "Global Submarine Proliferation: Emerging Trends and Problems," March 2006. Accessed March 28, 2009 at www.nti.org/e_research/e3_74.html.

[23] For more details see Ron O'Rourke, 8-16.

[24] On potential PLA investments in power projection see Andrew S. Erickson and Andrew R. Wilson, "China's Aircraft Carrier Dilemma," *Naval War College Review*, (Autumn 2006): 13-45.

[25] Quoted in Christopher Bodeen, "China's First Aircraft Carrier on Horizon," *Seattle Times*, (21 April 2009). See discussion in O'Rourke, 17-20.

[26] *Chinese Military Power Report*, 20.

[27] Andrew Erickson and David D. Lang, "On the Verge of a Game-Changer," *Naval Institute Proceedings*, (May 2009). (Accessed 23 May 2009) at https://www.usni.org/magazines/proceedings/story.asp?STORY_ID=1856.

[28] For further explorations into the operational and technological challenges and implications of ASBMs see Andrew S. Erickson and David D. Yang, "Using the Land to Control the Sea?" *Naval War College Review*, (Autumn 2009): 53-79; and Mark A. Stokes, "China's Evolving Conventional Strategic Strike Capability: The Anti-ship Ballistic Missile Challenge to U.S. Maritime Operations in the Western Pacific and Beyond," Washington DC: Project 2049 Institute, (September 2009) (forthcoming).

[29] Eric A. McVadon, "China's Navy Today: Looking toward Blue Water," 380, in Andrew S. Erickson, Lyle J. Goldstein, and Carnes Lord, eds., *China Goes to Sea: Maritime Transformation in Comparative Historical Perspective*, (Annapolis, MD: Naval Institute Press, 2009).

[30] Aaron L. Friedberg and Robert S. Ross, "Here Be Dragons," *National Interest*, (September/October 2009).

[31] Vladimir Isachenkov, "Russian defense budget may rise 25 percent in 2009," *USA Today*, (19 September 2008). http://www.usatoday.com/news/world/2008-09-19-1019290860_x.htm.

[32] For contrasting perspectives on how to think about Russia see Paul Dibb, "The Bear Is Back," *The American Interest*, (November/December 2006) and Rajan Menon & Alexander J. Motyl, "The Myth of Russian Resurgence," *The American Interest*, (March/April 2007).

[33] Richard Jackson and Neil Howe, "The Graying of the Great Powers," Washington, DC: Center for Strategic International Studies, (2008): 7.

[34] Vivienne Walt, "Russia Rearms," *Time*, (16 April 2009), http://www.time.com/time/magazine/Article/0,9171,1891681,00.html.

[35] Milan Vego, "The Russian Navy Revitalized," *Armed Forces Journal International*, (May 2009): 34-36, 46-47.

[36] Thomas Mahnken, *The Cruise Missile Challenge*, Washington, DC Center for Strategic and Budgetary Assessment, (2005).

[37] Mark Mazzetti and Thom Shanker, "Russian Subs Patrolling off East Coast of U.S.," *New York Times*, (5 August 2009).

[38] Vego, 47.

[39] IISS, *The Military Balance*, London, (2008): 31-32, 213-216, 377-379.

[40] James R. Holmes, Andrew C. Winner and Toshi Yoshihara, *Indian Naval Strategy in the 21st Century*, (New York: Routledge, 2009).

[41] *Ibid*, 128.

[42] Holmes, Winner and Yoshihara, 82-94.

[43] Norman Polmar, "India's Navy Expanding Rapidly," *Military.com*, (9 June 2008), http://www.military.com/forum/0,15240,169493,00.html.

[44] For other scholars see Michael Evans, "From Kadesh to Kandahar: Military Theory and the Future of War," *Naval War College Review*, (Summer 2003); Erin Simpson," Thinking about Modern Conflict: Hybrid Wars, Strategy, and War Aims," conference paper presented at the Midwest Political Science Association, Chicago, Illinois, April 7, 2005; John J. McCuen, "Hybrid Wars," *Military Review*, (April/May 2008): 107-113; and David Kilcullen, *Accidental Guerilla*, (New York: Oxford University Press, 2009).

[45] Lt Col William. J. Nemeth, USMC, *Future War and Chechnya: A Case for Hybrid Warfare*, Monterrey, CA: Naval Postgraduate School, (June 2002).

[46] Lt Gen James N. Mattis USMC and Frank Hoffman, "Future Warfare: The Rise of Hybrid Warfare," *Naval Institute Proceedings*, (November 2005): 30-32; Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, (Arlington, VA: Potomac Institute for Policy Studies, December 2007); Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly*, (1st Quarter 2009).

[47] For a detailed analysis see Andrew Exum, "Hizballah at War: A Military Assessment," Washington, D.C: Washington Institute for Near East Policy, *Policy Focus #63*, (December 2006).

[48] Caitlin Talmadge, "Closing Time: Assessing the Iranian Threat to the Strait of Hormuz," *International Security*, (Summer 2008): 82, 117.

[49] David B. Crist, "Gulf of Conflict: A History of U.S. Iranian-Confrontation at Sea," *Policy Focus #95*, Washington, DC: The Washington Institute for Near East Policy, (June 2009).

[50] Barry Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security*, (Summer 2003): 22.

[51] Mahnken, 16-17. Talmadge, 100-101.

[52] Frederic Wehrey, et al, *Dangerous But Not Omnipotent: Exploring the Reach and Limitations of Iranian Power in the Middle East*, Santa Monica, CA: RAND, (2009).

[53] Fariborz Haghshenass, *Iran's Asymmetric Naval Warfare,* Washington, DC: The Washington Institute for Near East Policy, Policy Focus #87, (September 2008).

[54] I am indebted to the British scholar Martin Murphy for this term, which serves as a useful categorization versus conventional and hybrid threats but is not intended to imply relationships between various sub-categories or conflate the various methods and disparate goals of pirates, terrorists and criminal groups at sea.

[55] Rohan Gunaratna, "The Threat to the Maritime Domain: How Real Is the Terrorist Threat," 77 in Jeffrey H. Norwitz, ed., *Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency*, (Newport RI: Naval War College, 2008). For an optimistic assessment see Bjorn Moller, "Piracy, Maritime Terrorism and Naval Strategy," Report 2009-02, Copenhagen, Denmark: Danish Institute for International Studies, (2009).

[56] For detailed assessments see Martin N. Murphy, *Small Boats, Weak States and Dirty Money,* (New York: Columbia University Press, 2009). Peter Lehr, ed., *Violence at Sea: Piracy in the Age of Global Terrorism,* (New York: Routledge, 2006), John S. Burnett, *Dangerous Waters: Modern Piracy and Terror on the High Seas*, (New York: Penquin Press, 2003); Daniel Sekulich, *Terror on the Seas: True Tales of Modern-Day Pirates*, (St Martin's Press, 2009).

[57] Peter Chalk, *Maritime Piracy*, testimony before the Committee on Transportation and Infrastructure, U.S. House of Representatives, (4 February 2009).

[58] ICC Commercial Crime Services, "Unprecedented Increase in Somali Pirate Activity," (21 October 2009). http://www.icc-ccs.org/index.php?option=com_content&view=Article&id=376: unprecedented-increase-in-somali-pirate-activity&catid=60:news&Itemid=51.

[59] International Maritime Organization, "Reports on Acts of Piracy and Armed Robbery Against Ships, Annual Report, 2008," London, UK, (19 March 2009).

[60] The owners of the Saudi registered ship purportedly paid a 3 million dollar ransom to have its crew, vessel, and cargo returned safely. Michael G. Frodl, "Hijacked Super Tanker Exposes Vulnerability of Energy Supplies," *National Defense*, (March 2009).

[61] Steve Liewer, "Fighting Sea Piracy," *San Diego Union-Tribune*, (9 April 2009).

[62] On the limited nature of the threat posted by maritime terrorism see Martin N. Murphy, *Contemporary Piracy and Maritime Terrorism, The Threat to International Security*, London, IISS, Adelphi Paper 388, July 2007, pp. 73, 85; John Patch, "The Overstated Threat," Naval Institute Proceedings, (December 2008): 34-39.

[63] Chalk, testimony, 2.

[64] ICC Commercial Crime Services, "Unprecedented Increase in Somali Pirate Activity," (21 October 2009), http://www.ice-ccs.org/ndex.php?option=com_content&view=Article&id=376.

[65] Robert D. Kaplan, "Anarchy on Land Means Piracy at Sea," *New York Times*, (12 April 2009): A19.

[66] On the Sea Tigers of the LTTE, see Murphy, *Small Boats, Weak States and Dirty Money*, 310-322.

[67] Bill Roggio, "Analysis: Mumbai attack differs from past terror strikes," *Long War Journal*, (28 November 2008), http://www.longwarjournal.org/archives/2008/11/analysis_mumbai_atta.php.

[68] On the capabilities and past characteristics of MEND, see Murphy, *Small Boats, Weak States and Dirty Money*, 111-122.

[69] Martin Murphy, "Piracy and the Exploitation of Sanctuary," in Jeffrey H. Norwitz, ed., *Armed Groups: Studies in National Security, Counterterrorism, and Counterinsurgency*, Newport RI: Naval War College.

[70] Martin Murphy, "The Unwanted Challenge," *Naval Institute Proceedings*, (December 2008): 49. See also Martin Murphy, Suppression of Piracy and Maritime Terrorism, *Naval War College Review*, (Summer 2007): 23-45

[71] Peter Chalk, *Maritime Piracy*, testimony before the Committee on Transportation and Infrastructure, U.S. House of Representatives, (4 February 2009).

[72] Bruce Riedel, *The Search for Al Qaeda: Its Leadership, Ideology, and Future*, (Washington, DC: Brookings, 2009): 122-124.

[73] Chalk, 24.

[74] Peter Chalk, Bruce Hoffman, Robert Reville and Anna-Britt Kasupski, *Trends in Terrorism, Threats to the Untied States and the Future of the Terrorism Risk Insurance Act*, Santa Monica, CA: RAND, MG-393-CTRMP, (2005), xv.

[75] Adm. James G. Stavridis, U.S. Navy, Statement before the Senate Armed Services Committee, (17 March 2009), 11-12; William Booth and Juan Forero, "Plying the Pacific, Subs Surface as Key Tool of Drug Cartels," *Washington Post*, (6 June 2009): 1.

[76] Peter Chalk, *The Maritime Dimension of International Security: Terrorism, Piracy, and Challenges for the United States*, RAND (2008): 43; James Kraska, "Coalition Strategy and the Pirates of the Gulf of Aden and the Red Sea," *Comparative Strategy*, Vol. 28, (2009): 197-216.

[77] Peter Brookes, "Flashpoint: Arctic Security Heats Up," (5 November 2008), www.familysecuritymattrs.org/publications/id.1693.print/pub_details.asp.; John Patch, "Cold Horizons: Arctic Maritime Security Challenges," *Naval Institute Proceedings*, (May 2009): 48-54.

[78] *Cooperative Strategy for 21st Century Seapower*, 6.

[79] Anthony L. Russell, "Carpe Diem, Seizing Strategic Opportunity in the Arctic," *Joint Force Quarterly*, Issue 51, (4th quarter 2008): 94-101.

[80] CIA Factbook, (2008), https://www.cia.gov/library/publications/the-world-factbook/rankorder/2178rank.html.

[81] Cited in Patrick Goodenough, *CNSNews.com*, (14 May 2009).

[82] Damien McElroy, "Russia Sets Up Military Force in Arctic Claim," *Telegraph*, (27 March 2009).

[83] George W. Bush, National Security Presidential Directive 66 (NSPD 66), Washington, DC, (9 January 2009), http://www.fas.org/irp/offdocs/nspd/nspd-66.htm.

[84] For more suggestions see Scott G. Borgerson, "Arctic Meltdown: The Economic and Security Implications of Global Warning," *Foreign Affairs*, (March/April 2008), http://www.foreignaffairs.com/node/6322 and Scott G. Borgerson, "The Great Game Moves North: As the Arctic Melts, Countries Vie for Control," *Foreign Affairs*, (March 2005), http://www.foreignaffairs.com/node/640905.

[85] Kurt M. Campbell, Nirav Patel, Vikram J. Singh, *The Power of Balance: America in Asia*, Washington DC: Center for a New American Security, (June 2008): 73. "The United States must maintain a substantial and sustained forward deployed military presence in the region that is both reassuring to friends and a reminder to China that America will remain the ultimate guarantor of regional peace and stability." *Ibid*, 89.

[86] Tom Coghlan, "NATO Commander Warns of Conflict With Russia in Arctic Circle," *London Times*, (3 October 2009).

[87] See Robert O. Work and Jan van Tol, "A Cooperative Strategy for 21st Century Seapower: An Assessment," Washington, DC: Center for Strategic and Budgetary Assessment *Backgrounder*, (26 March 2008): 20. Eric J. Labs, Congressional testimony "Current and Projected Navy Shipbuilding Programs," before the Seapower and Expeditionary Forces subcommittee, House Armed Services Committee, (14 March 2008).

[88] Glenn Davis, Charles Dragonette and Randy Young, "Dangers at Sea," *Foreign Affairs*, (September/October 2007): 162. This trio notes that "the flow of oil is critically vulnerable not at sea but where the shore interfaces with the sea: at oil loading terminals and associated infrastructure. Oil refineries at both loading and discharge ports are similarly vulnerable, and they are presently the weakest link in the oil supply chain."

[89] On port security, see Stephen Flynn, "U.S. Port Security and the Global War on Terror," *The American Interest*, (Autumn 2005): 92-96.

[90] Robert Gates, Remarks As Delivered, IISS Shangra-La Dialogue, (30 May 2009).

[91] John G. Morgan Jr. and Charles W. Martoglio, "The 1,000 Ship Navy: Global Maritime Network," *Naval Institute Proceedings*, (November 2005): 17.

[92] Cossa, et al, *The United States and the Asia-Pacific Region, Security Strategy for the Obama Administration*, p. 6. See also James J. Przystup, "The United States and the Asia-Pacific Region: National Interests and Strategic Imperatives," Washington, DC: National Defense University, Strategic Forum No. 239, (April 2009): 5.

[93] Claude Berube, "The Post-Oceanic Navy, the New Shadow Zones and the U.S. Navy's Force Structure Challenge," *Small Wars Journal*, (May 2009), http://smallwarsjournal.com/mag/docs-temp/222-berube.pdf.

[94] Ralph Cossa, Brad Glosserman, Michael A. McDevitt, Nirav Patel, James Przystup, Brad Roberts, *The United States and the Asia-Pacific Region, Security Strategy for the Obama Administration*, Washington, DC: Center for Strategic and Budgetary Assessments, (February 2009). Ellen L. Frost, James J. Przystup, and Phillip C. Saunders, *China's Rising Influence in Asia: Implications for U.S. Policy*, Fort McNair, DC: National Defense University, Strategic Forum No. 231, April 2008; William H. Overholt, *Asia, America, and the Transformation of Geopolitics*, (New York: Cambridge University Press, 2008).

[95] For a comprehensive set of recommendations regarding China see Abraham M. Denmark, and Nirav Patel, eds., *China's Arrival: A Framework for a Global Relationship*, (Washington DC: Center for a New American Security, 2009).

[96] F. G. Hoffman, "Alternative Naval Forward Presence, Maritime Security Groups," *Marine Corps Gazett*e, (March 2007). See also Dakota Wood's description of Littoral Operations Groups in D. Wood, "The U.S. Marine Corps: Fleet Marine Forces for the 21st Century," Washington, DC: Center for Strategic and Budgetary Assessments, (November 2008). On Global Fleet Station initiatives see Kathi Sohn, "The Global Fleet Station, A Powerful Tool for Preventing Conflict," *Naval War College Review*, (Winter 2009): 45-58.

[97] Frank Hoffman, *From Preponderance to Partnership, American Maritime Power in the 21st Century*, (Washington, DC: Center for a Strategic and Budgetary Assessment, November 2008).

[98] Lt Gen Ma Xiaotian, PLA Deputy Chief of the General Staff, "The Major Powers and Asian Security: Cooperation or Conflict?" remarks at the 8th IISS Asian Security Summit, The Shangri-La Dialogue, (20 May 2009).

[99] Robert Kaplan, in Denmark and Patel, eds., *China's Arrival*, 56.

[100] Sharon Burke and Christine Parthemore, *A Strategy for American Power: Energy, Climate, and National Security*, Washington DC: Center for a New American Security, (June 2008): 31. Cossa, et al, 57-59.

[101] Campbell, et al, *The Power of Balance: America in iAsia*, 80-81.

[102] An initiative of then-UN Secretary-General, Kofi Annan. The responsibility to protect builds off the so-called "right of humanitarian intervention" as a foreign policy issue emanating from acts of genocide in Kosovo and Rwanda. In his report to the 2000 General Assembly, Annan challenged the international community to try to forge consensus, once and for all, around the basic questions of principle and process involved: when should intervention occur, under whose authority, and how. See his clarifications at http://www.un.org/News/Press/docs/2008/sgsm11701.doc.htm. The extension of this doctrine to areas where sovereign states have failed to protect their populations to protecting the maritime domain has not been taken up by the UN.

[103] Scott G. Borgerson, *The National Interest and the Law of the Sea*, New York: Council on Foreign Relations, Council Special Report, No. 46, (May 2009).

[104] For a detailed assessment of the U.S. position on the treaty see Brian Wilson and James Kraska, "American Security and the Law of the Sea," *Ocean Development and International Law*, Vol. 40, (2009): 268-290.

[105] Adm. Gary Roughead, USN, Statement before the HASC on the Department of the Navy FY 2010 Posture, (14 May 2009): 14.

[106] Michele Flournoy, "CSIS Rebalancing the Force: Major Issues for QDR 2010," (27 April 2009), event transcript.

[107] Robert D. Kaplan, "The Revenge of Geography," *Foreign Policy*, (May 2009): 96-105.

[108] The United States is the world's largest oil consumer, imports almost 66 percent of its oil, with at least 90 percent arriving by sea. Japan is almost completely dependent on maritime imports. In 2006, China imported over half of the oil it consumed, and India 68 percent. By 2025, import figures are expected to balloon to 75 percent of total consumption for China and approximately 85 percent for India, with at least 80 percent of their oil being shipped by sea. Dennis Blair and Kenneth Lieberthal, "Smooth Sailing: The World's Shipping Lanes are Safe," *Foreign Affairs*, (2007): 83-90.

[109] Paul S. Giarra and Michael J. Green, "Asia's Military Balance At a Tipping Point," *Wall Street Journal Asia*, (17 July 2009).

[110] Robert D. Kaplan, "Center Stage for the Twenty-first Century," *Foreign Affairs*, (March/April 2009): 16-32.

[111] Andrew F. Krepinevich Jr., "The Pentagon's Wasting Assets," *Foreign Affairs*, Vol. 88, No. 4., (July/August 2009): 18-19.

CHAPTER III:
SUSTAINING THE AIR COMMONS

By Lt Col Kelly Martin (USAF) and Oliver Fritz

SUSTAINING THE AIR COMMONS

By Lt Col Kelly Martin (USAF) and Oliver Fritz

Introduction

Open access to the air is a key enabler of today's global economy. In 2008, air transport facilitated the movement of 35 percent (3.5 trillion dollars) of the world's manufactured exports by value, as well as over 40 percent of the world's international tourists who in turn generated 3.4 percent of global gross domestic product (GDP).[1] The air transport industry directly employs 5.5 million people, generates another 26.5 million indirect jobs worldwide, and transports more than 2.2 billion passengers each year.[2]

Since World War I, access to the air has been a foundation of military power. Initially, air power helped militaries overcome geographic obstacles on the battlefield. Today, air power's depth and speed allows countries to achieve strategic effects from positions anywhere around the world. Contemporary American air power theorists emphasize the importance of influencing enemy leadership and striking the enemy's military.[3] Moreover, in addition to kinetic capabilities, states can exploit air power for logistics, surveillance, and reconnaissance to great strategic effect. Such capabilities confer enormous advantages to those states able to attain them; indeed, they have transformed the nature of warfare.[4]

Relative to other global commons, the air commons has reached a high level of maturity. It is managed effectively through a series of international organizations and bilateral agreements largely unseen by the casual traveler. Together, these agreements govern the use of the global air commons and provide a useful model for less well-governed commons, such as space and cyberspace.

While access to the air commons is widely available, it could be increasingly contested unless the international community takes steps to defend it. A successful set of international standards and

Disclaimer: None of the views expressed in this document by the authors represent those of the United States government or any of its departments or agencies.

Generally secure and open to all who have the technology and infrastructure to access it, the air commons enables people or goods to be anywhere on the globe within 24 hours.

bilateral access agreements exists but a single international agreement on access and overflight continues to elude the international community. International air travel agreements remain almost entirely bilateral, leading to inconsistencies and inefficiencies that restrict both commercial and military air activities. As demand outpaces the existing civil air infrastructure, that infrastructure will become increasingly brittle, hindering civilian access to the air commons. In addition, the air commons depends on public confidence in the safety of air travel, which terrorism could undermine. In the military arena, the proliferation of symmetric and asymmetric capabilities allows new air powers and non-state actors to increasingly challenge the *de facto* protector of the air commons, the United States.

This chapter will discuss the nature of the air commons and how it is governed and defended. It will then explore developments that may challenge the sustained openness and stability of the air commons in peacetime and emerging challenges to America's ability to control the air during wartime. In conclusion, it will recommend steps to modernize and expand access to the air commons, strengthen the international architecture that governs it, and reinforce the United States' command of the air commons.

The Nature of the Air Commons

The air commons is a shared physical space accessed by a network of almost 44,000 airports world-wide.[5] It spans the globe, across both land and sea, and rises to meet the floor of outer space. The ability to move through the air changes the way people view the world; they are no longer confined by geographical obstacles or limits. The air commons transforms distance, from months, weeks and days to hours. Generally secure and open to all who have the technology and infrastructure to access it, the air commons enables people or goods to be anywhere on the globe within 24 hours.

States exercise unquestioned authority over airspace up to 60,000 feet over their geographic borders and extending 12 miles out from their coastlines. However, an integrated network of agreements enables a highly functioning global air transport system that facilitates easy travel across borders. International governance is maintained by a system of systems, composed of international organizations and bilateral agreements. This overarching structure serves two functions. It allows economic gain through the transfer of goods and people and it binds states to an established international framework. The pursuit of economic gain historically has driven international efforts to protect the air commons, but it has been the diplomatic and military leadership of the United States that has kept it open and stable.

There is a natural tension between the aspiration to freely operate within the air commons and the inherent desire of nations to protect sovereign borders. The desire of freedom to fly across any geography regardless of territorial boundaries goes back to the concept of *mare liberum*, or freedom of the seas. The question of national airspace first arose with the use of balloons in the Franco-Prussian War in the late 1800s; however, it was the advent of powered flight in the wake of World War I that caused nations to understand the potential threats and advantages of the air commons as a medium for warfare. Still, nations searched for the agreements that would allow exploitation of the air commons for economic gain.

As uses of the air commons expanded, the international community initiated regulatory efforts to achieve greater access, particularly across borders. Developing lasting international agreements proved unrealistic at that time, but in 1919 international agreements successfully established the important precedent that each nation enjoys "complete and exclusive sovereignty over the airspace above its territory."[6]

The inter-war period in the first half of the 20th century saw an explosion of commercial air travel in the United States and Western Europe as aircraft technology became more reliable and cost-effective.[7] To take advantage of this economic growth potential, the U.S. government began to invest heavily in aviation infrastructure, improving 358 existing airports and building 585 airports.[8]

Airpower came into its own during World War II, for both military and civil purposes. The allied powers recognized the importance of developing an international air infrastructure to govern civil aviations and built the necessary institutions to achieve that goal. In September 1944, the International Civil Aviation Organization (ICAO) was established amongst nations, and the following year saw the creation of the International Air Transport Association (IATA) among private businesses. In large part, these agreements charted the way for the creation of an open air commons and catalyzed economic development.

Today, at any given moment, tens of thousands of flights traverse the skies around the world, with each one controlled and directed in a uniform manner: English remains the language of international air travel, and management of air traffic is routinely passed from one control station to another. This feat is possible because of the universally accepted standards set forth by ICAO, Standards and Recommended Practices (SARP). SARPs cover all aspects of international civil aviation, including safety, personnel licensing, operation of aircraft, air traffic services and accident investigation.[9] Within this international structure, each country has its own regulatory authority. In the United States, the Federal Aviation Administration (FAA) is empowered with broad authority for rule-making, pilot and aircraft certification, and safety enforcement.

Subsequent liberalization of national civil air programs further facilitated the openness of the air commons. In the late 1970s and early the 1980s, the United States and Great Britain led the reforms to deregulate the airline industry, open markets, and privatize national airlines. Competition increased and ticket prices plummeted causing soaring growth in air traffic.[10] In the 1990s, the United States sought to further liberalize the air transport market through Open Skies agreements, which focused on free-market competition, market-force pricing and normal business protections. Today, the United States has 90 bilateral and two multilateral agreements; other countries followed the American example and have signed thousands of Open Skies agreements.[11] This liberalization produced significant economic gains. A 2008 study on air liberalization found that, in the years following the liberalization of markets, there has been, on average, a 12 percent to 35 percent increase in air traffic growth across different markets. The study also found that 320 country pairs not under an Open Skies agreement could see a 60 percent increase in traffic growth under more liberal agreements—compared with increases of 6 percent to 8 percent without them. This 60 percent increase could translate to the creation of 24.1 million jobs and an additional 490 billion dollars in GDP.[12]

Governing the Global Air Commons: A History

In September 1944, the United States hosted the International Civil Aviation Conference in Chicago to develop an international agreement that would establish certain freedoms of the air and set an international standard for air operations. Many nations still at war viewed maintaining tight control over their territorial skies as critical to national security.[i] However, more than 50 countries attended (the Soviet Union opted out), and they created the International Civil Aviation Organization (ICAO), an independent agency of the United Nations charged with promoting the "safe, secure, and sustainable development of civil aviation through the cooperation amongst its member states."[ii]

In a second attempt to establish an economic oversight structure, 31 countries met in Havana, Cuba, in April 1945. A total agreement could not be reached, but the delegates created the International Air Transport Association (IATA) to standardize the necessary logistics for international air travel, creating interoperability among carriers. One of the IATA's first missions was to standardize documentation procedures and develop fare and rate schedules that would make international air travel rationalized and predictable. The IATA also offered a clearinghouse through which debt settlements between airlines could be reconciled. In its first year, 17 airlines adjudicated 26 million dollars in outstanding payments to other airline companies.[iii]

These conferences were largely successful, but a single international agreement that allowed for open access to airports and routes did not materialize. Lacking such a multilateral agreement, the United States and Great Britain, in winter 1945, signed the Bermuda Agreement, a bilateral agreement that recognized the IATA, established a proportionality of services to airlines, and delegated the level of its usage to the management of the airlines. The Bermuda Agreement became the template for all subsequent bilateral agreements. To date, almost 4,000 bilateral air transport agreements are registered with the ICAO.[iv]

The Chicago and Havana Conferences, along with the Bermuda Agreement, established the foundations for the growth of an open air commons leading to unprecedented global economic development. Today, 190 of the 192 United Nations member states are active members of the ICAO, maintaining sovereignty over their airspace yet benefiting from the economic advantages that open access to the air commons brings.

[i] Gerald L. Baliles, "Fear of Flying: Aviation Protectionism and Global Growth," *Foreign Affairs* (May/June 1997).

[ii] International Civil Aviation Organization, http://www.icao.int/icao/en/strategic_objectives.htm.

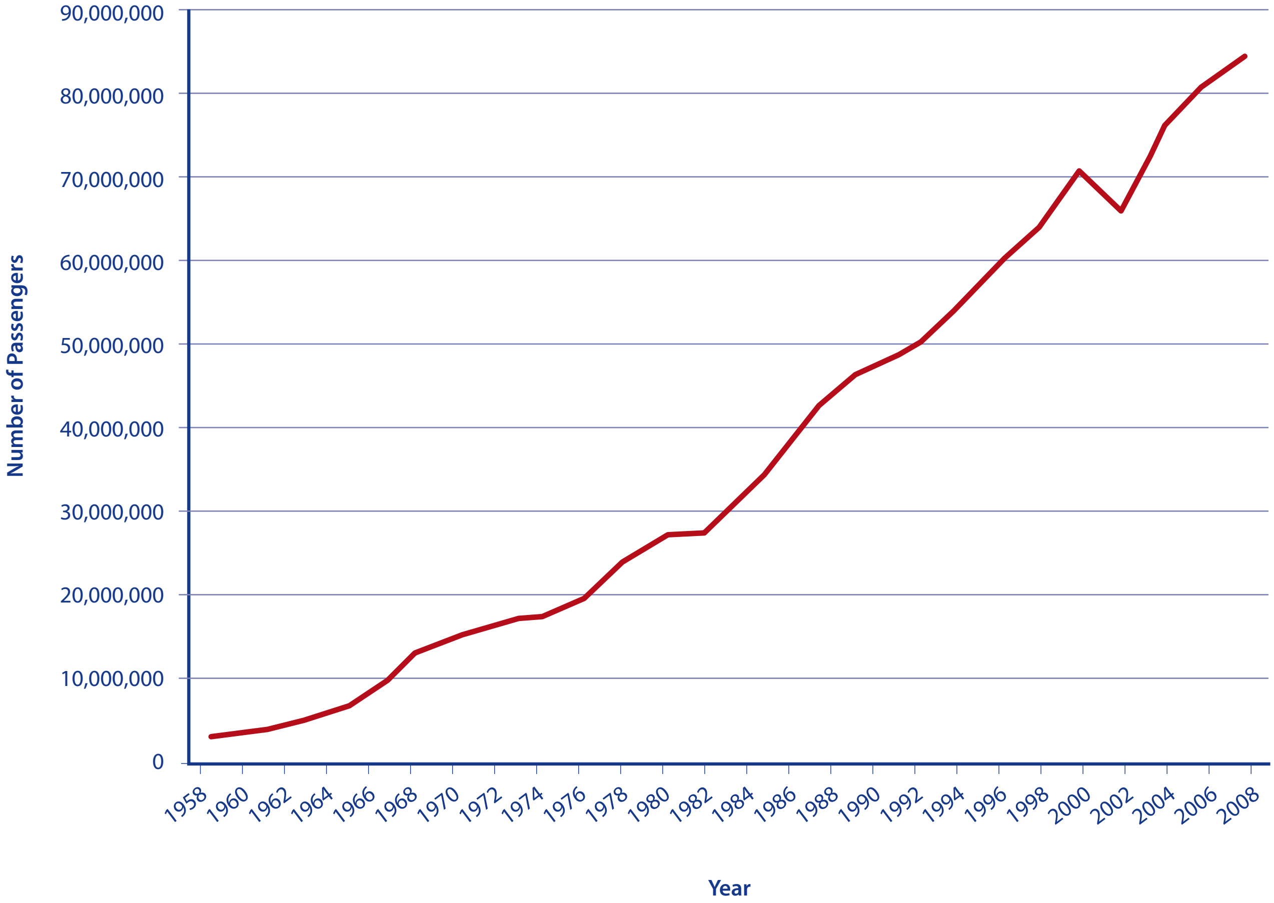
[iii] International Air Transport Association, http://www.iata.org/about.

[iv] *Ibid.*

American technological prowess and diplomatic leadership has helped to define and sustain the openness of the air commons. However, this dynamic is changing. New economic powers are increasing their investment in air infrastructure and industry. For example, in the 1960s, the United States controlled 90 percent of the aviation manufacturing market share.[13] In 2005, the rate had dropped below 50 percent, and it is projected to be at 35 percent by 2020.[14] Moreover, the customer base is becoming increasingly diverse, with more than 70 percent of commercial aircraft orders in 2005 coming from non-U.S. carriers.[15]

However, because of the durability of the established international architecture, this emerging multipolarity has not undermined the openness and stability of the air commons, and there are no signs that it will. The system of international agreements on air ensures a state's ability to gain access to the commons, but in a manner that ensures the continuity and survivability of the overall architecture. Moreover, the international community does a good job of "disconnecting" states that ignore its tenets. If a carrier refuses to comply with international standards, that carrier is denied access to controlled airspace. Similarly, individual carriers will avoid using a nation's airspace or its airports that do not comply with ICAO safety and security standards.

Figure 1: Growth in American Passengers, 1958 – 2008.



THE AIR COMMONS AND ECONOMIC DEVELOPMENT

The ability of nations to access the air commons has coincided with, and has in many ways driven, economic globalization. Civil aviation contributes significantly to the world's GDP and drives continued economic growth, especially in developing nations. More than just the jobs it creates, the aviation industry and airspace access links a state or a region to the global economy and accelerates growth across all industries.

These economic benefits extend beyond major economies to include emerging economies. Indeed, developing countries that improve their ability to access the air commons are experiencing the greatest return on their investments. A recent IATA study analyzed the relationship between the degree of access to the air commons and economic growth in 48 countries of various degrees of development from 1996 to 2005. On average, a 10 percent increase in connectivity resulted in a 0.07 percent increase in productivity and a double digit percentage return on investment, with significantly higher positive results in developing countries (Table 1).[16] The United Arab Emirates (U.A.E.) is an example of a country seeking to use aviation to attract foreign investment and spur economic growth.[17] By expanding its airports and surrounding infrastructure, the U.A.E. is establishing itself as a geographic transit hub for international air traffic between the various regions of the world.

U.S. MILITARY CONTROL OF THE AIR

While international agreements and economic self-interest supply the structure for an open and accessible air commons, the United States' authoritative command of the air commons facilitates collective security across land and sea. As Barry

Table 1

EXPANDING ACCESS TO THE AIR COMMONS IN THE DEVELOPING WORLD

	KENYA	CAMBODIA	JORDAN	EL SALVADOR	JAMAICA
Investment (U.S. dollars, millions)	351	538	360	488	168
Increase in national connectivity/ GDP	59%	46%	55%	35%	28%
Impact on GDP (%)	0.42%	0.32%	0.39%	0.25%	0.20%
Impact on GDP (U.S. dollars, millions)	209	100	100	85	26
Annual Economic Rate of Return on Investments (%)	59%	19%	28%	16%	16%

Posen argues in his seminal piece on commanding the global commons, it is a fact that the United States "gets vastly more military use out of the sea, space, and air than do others that it can credibly threaten to deny their use to others; and that others would lose a military contest for the commons if they attempted to deny them to the United States."[18] In addition to securing U.S. access to the commons, command acts as a guarantor of access and the assurance of security for U.S. allies and willing participants.

The United States is the world's first and only global air power. The first step for most military operations is the achievement of "air superiority" or limiting the ability of the adversary to use the air. In this sense, control of the air means freedom from attack and freedom to attack, move and observe. Air superiority frees forces on land, at sea, and in the air from the threat of enemy aerial attack and allows them to mass and maneuver at will. In fact, no U.S. solider or Marine has been killed by enemy aircraft in over 50 years. In this role, the U.S. Air Force has been unmatched, to the point that no credible challenger exists and air superiority is simply assumed by U.S. military planners.

Based on technological superiority and the ability to rapidly and effectively move people, equipment and weapons, the air commons remains the primary medium for projecting American power. Kinetic air power can damage and destroy vital centers of enemy power, regardless of distance or terrain. Moreover, non-kinetic air power projection—airlift, reconnaissance, air refueling—is essential to the execution of operations. Air power's high speed and agile maneuverability allow actions to occur within hours, anywhere in the world (given basing and mid-air refueling support). Air power can insert and extract friendly ground forces, as well as supply them from great distances. In Operation Iraqi Freedom, 80 percent of all beans, bullets and bodies entering Iraq passed through Sather Air Base in Baghdad en route to forward operating bases around the country.[19] Air is also critical to intelligence, surveillance and reconnaissance (ISR), as well as medical evacuation and search and rescue. Through combined use of large-bodied aircraft and aerial refueling, injured personnel arrive at life-saving medical treatment centers in the United States within hours of being wounded.

Based on technological superiority and the ability to rapidly and effectively move people, equipment and weapons, the air commons remains the primary medium for projecting American power.

In addition to the ability of air power to deter, coerce, deny, or punish, air power can be a powerful and swift means of providing relief and facilitating support where the need is greatest. Echoing the marathon efforts to re-supply Berlin amidst a Soviet blockade in the late 1940s, air power has been repeatedly use to provide direct material relief, enable local authorities, and deploy joint and inter-agency expertise into areas in need. As a tool for engagement and building partnerships, air power can act decisively or enable elements of the entire U.S. government to reach out and directly influence crises and disasters around the globe.

The ability to effectively and efficiently exploit the air commons is a core asymmetric advantage for the United States. Adversaries who wish to fight or oppose the United States attempt to avoid conflicts

The enduring ability of the United States to master the air during wartime drives adversaries to develop responses that threat to undermine traditional advantages enjoyed by U.S. forces.

in the air, or develop capabilities that undermine the ability of the United States to effectively control the air. Such capabilities are rapidly developing and proliferating among would-be adversaries. In fact, Posen suggests that "perhaps the most contested element of U.S. command of the commons is command of the air" because of its importance and perceptions that U.S. vulnerabilities are increasing.[20]

Contesting the Air Commons

Over time, the air commons became dependent on a complex system of norms, infrastructure, technology, and technical standards to meet the demands of a growing traveling public. This complexity, and the steps nations have taken to master it, is producing trends that could eventually disrupt the air commons. During peacetime, the density of the system that supports the air commons provides abundant opportunities for intentional or accidental disruption. Similarly, the enduring ability of the United States to master the air during wartime drives adversaries to develop responses that threaten to undermine traditional advantages enjoyed by U.S. forces.

PEACETIME CHALLENGES AND THREATS

The flying public's high level of confidence in civil aviation's safety is a prerequisite for the effective use of the open air commons. During peacetime, challenges to the air commons come from intentional acts and mistakes that undermine the perceived safety and efficiency of air travel. Indeed, given the unique role of the air commons in moving people, the perception of flight safety often outweighs reality and a high level of confidence is essential for the effective openness of the air commons. However, there is increasing evidence that air traffic control systems are at risk of technical or intentional degradation. Beyond the air traffic control system that binds thousands of daily flights, terrorist attacks in the air or on the ground are likely to continue, and potentially increase in lethality. These shortfalls may decrease the reliability and safety of air travel, distorting how the air commons is used.

Brittle Air Traffic Control Systems

The U.S. air traffic control system (ATC) is burdened with a navigation system that dates to the 1950s and an airspace management system from the 1980s, with its many single points of failure and interconnected vulnerabilities. The demand for the air commons is outstripping the American civil aviation infrastructure's ability to safely and efficiently manage movement within it.[21] Problems associated with burned-out circuit boards, software upgrades, power outages, or even a car hitting a single utility pole, reveal a lack of resilience or redundancy.[22]

Forecasts indicate that domestic and international air traffic will exceed the limit of current ATC systems.[23] Technological advances, such as the advent of radar and the integration of the Global Positioning Satellite (GPS) system, allow for increased capacity for commercial air travel. An accurate understanding of an airplane's location—with three-dimensional positioning—empowers air traffic controllers to allow more aircraft into a given amount of airspace. Such precision allows major airline hubs and air routes to function more efficiently without sacrificing

U.S. Navy Cmdr. Craig Reiner flies an F/A-18C Hornet strike fighter from Fleet Readiness Center Southwest over Naval Air Station North Island, Calif., and the aircraft carrier USS John C. Stennis (CVN 74) Nov. 18, 2008, in San Diego.

(U.S. Navy)

safety. However, technologies like GPS must be widely distributed to realize these gains. Accurate positioning with GPS only works if the satellite constellation provides sufficient accuracy and *all* airplanes are equipped with GPS receivers. With a single airplane lacking a GPS receiver, it is impossible for air traffic controllers to be sure of the airplane's position, forcing a reduction in the density of aircraft to reduce the chances of a collision.

The use of GPS on airlines has grown dramatically and is now a requirement to operate in designated controlled airspace.[24] According to current FAA modernization plans, GPS will be the linchpin of a broader "NexGen" system of navigation, communications, weather forecasting and redundancy. Rather than relying on brittle, segmented areas of airspace, GPS enables an air transportation system that is more durable and less reliant on an increasingly fragile ground control system.

However, there are concerns about GPS serving as the foundation of this more efficient, safer system. In 2009, the Government Accountability Office (GAO) reported that delays in the Air Force's acquisition of replacement GPS satellites could affect optimal precision. The probability of maintaining a constellation of at least 24 operational satellites — the number needed for optimal precision — will fall below 95 percent between 2010 and 2014, at times falling to about 80 percent.[25] With a two-year delay in the launch of the GPS III, the probability of having a full constellation could fall further, to nearly 10 percent by 2017.[26] As a result, the aviation industry has expressed concern over the loss of an increasingly core element of air operations.

Going forward, ATC systems will rely increasingly on communications in cyberspace and space-based positioning, navigation and timing (PNT) systems such as GPS, to further increase density, efficiency and capacity in the civil air system. The United States and European Union are pursuing similar efforts to utilize space-based assets and cyber networks, with a growing emphasis on automation.[27] American and EU officials have acknowledged the importance of interoperability with each other's systems, but efforts to improve coordination with other regional systems continues to lag.[28]

Cyber Attacks

In addition to apprehension about the technical integrity of the American ATC system, there are growing concerns over emerging cyberspace threats to the air commons. As much as accidents can disrupt service and safety, intentional attacks on the accuracy of air traffic control systems could produce even more confusion, false information, and even system-wide failures. The U.S. Department of Transportation Inspector General has reported that the FAA experienced more than 800 cyber incidents in 2008.[29] It is significant that the same report noted that an attack across the Internet in 2006 affected ATC systems and forced the FAA to shut down parts of the system overseeing Alaska.[30]

At very low cost, a hacker could induce sufficient confusion into the air transportation system to cause its closure. These are not necessarily as deadly as direct kinetic attacks, but cyber attacks on the civil ATC systems of the United States and allied nations would diminish the efficiency, reliability, and overall benefits of air transportation.

Terrorism

As the scope and scale of commercial air transport grew in the post-World War II era, so did the perceived utility of using the air commons as a medium for criminal activity and terrorism. Beyond the use of hijacking to commit extortion or ensure safe passage, individuals and organizations seek the direct destruction of airports and aircraft as political acts in and of themselves.

Airports are more hardened than many installations, but they are frequent terrorist targets (Table 2).[31] As the entry and exit points for all air travelers, airports offer a unique opportunity for an individual or organization looking to make an open and disruptive attack on public confidence.

Table 2

TERRORIST ATTACKS ON AIRPORTS, 1970 – 2008
Munich, February 1970: Small arms attack on El Al bus passengers.
Tel Aviv, May 1972: Small arms attack on passenger arrival terminal.
Athens, August 1973: Small arms and grenade attacks on passenger lounge.
Rome, December 1973: Small arms and grenade attacks on passengers in airport lounge and aircraft on the tarmac.
Rome and Vienna, December 1985: Small arms and grenade attacks at El Al and Trans World Airlines ticket counters.
Kimpo, South Korea, September 1986: Improvised explosive device.
Srinagar, India, January 2001: Small arms and grenade attack.
Glasgow, UK, June 2007: Vehicle-based improvised explosive device.

The use of a shoulder-fired anti-air missile known as a Man-Portable Air Defense System (MANPADS) to attack air travel is another, more lethal threat that completely circumvents airport security. The most recent incident in peacetime targeted an Israeli-chartered Boeing 757 taking off from Mombasa, Kenya, in 2002. The two infrared guided SA-7 missiles fired at the 757 missed, however defending civilian airliners from future MANPADS attacks is difficult at best, suggesting this threat will not diminish. A complex and cluttered urban environment provides perpetrators with easy means of dispersal and escape after the missile is launched. A civilian airliner's defenses are constrained by the very same urban environment, as well as by the costs and perceptions of other defensive measures. The typical defense against infrared guided weapons includes free falling flares dispensed from the target aircraft to distract the incoming missile, but these cannot be used over urban environments due to the risk of fire once they reach the ground. More sophisticated countermeasures, including active defenses such as the use of directed energy, may cost up to 1.3 million dollars per aircraft, meaning a total of 38 billion dollars to develop, procure, install, and sustain them across the entire U.S. commercial fleet alone.[32] Already constrained by high operating costs and fierce price competition, the airline industry has not moved toward this approach on its own and will likely require government assistance.

The number of MANPADS attacks on civil aircraft is low—an estimated 40 MANPADS attacks on civil aircraft since the 1970s, of those only six occurred during peacetime (two of those attacks killed all passengers and crew on board).[33] Looking to the future, the proliferation of capable, cheap MANPADSs into the hands of non-state actors strongly suggests that the threat will increase.

Today, nearly 20 countries possess the capability to produce MANPADSs and production since 1967 is estimated to top 1 million.[34] The most pressing peacetime threat from these weapons is not from the state militaries that possess the majority of these weapons, but from the wide array of non-state groups—such as al Qaeda and Hezbollah—that possess between 5,000 and 150,000 MANPADSs.[35] Considering the wide range of these estimates, the civil aviation industry should be concerned.

Once at cruising altitude, commercial airlines are relatively safe from threats on the tarmac or from low-altitude MANPADSs. However, hijacking and purposeful destruction remain a threat. In fact, an increasing focus on the destruction of multiple aircraft and the use of aircraft as weapons signal a significant shift in the terrorist threat to the air commons. For instance, earlier hijacking episodes were frequently accompanied by demands for transportation, the release of prisoners, and the immediate achievement of larger political goals. By the late 1980s, however, the outright destruction of Air India Flight 182 and Pan Am Flight 103 suggested a more direct and deadly use of aircraft as an instrument of terror.

Al Qaeda is the most notable and recent practitioner of this tactic. The September 11 commission report detailed how high-ranking deputy Mohammed Atef led a study in the late 1990s that identified mass casualties, not negotiating leverage, as the primary goal of any al Qaeda led hijackings.[36] Khalid Sheikh Mohammed carried his enthusiasm for destroying 12 U.S. airliners at once (the 1995 Bojinka plot) into the emerging al Qaeda network, and presented the use of aircraft as weapons as part of a larger set of options for attacking the United States.[37] The evidence suggests that the commercial air system will continue to be a target for extremists aiming at the West. Since September 2001, aircraft continue to be singled out for destruction, and al Qaeda has continued to issue direct threats against Western airlines.[38]

A Chinese air force Su-27 Flanker fighter aircraft during a visit by then-Chairman of the Joint Chiefs of Staff Marine Gen. Peter Pace to Anshan Airfield, China, March 24, 2007.

(STAFF SGT. D. MYLES CULLEN/DOD)

From the perspective of a terrorist, the morbid desirability of attacks on the air transportation network relates to the high level of effect created by a relatively small act. Osama bin Laden himself noted in an October 2004 message that the effects of the attacks and the subsequent response to the attacks on September 11 far outweighed the costs to plan and execute the attacks.[39] Some of these effects could be common to any large-scale terrorist attack, but the large spillover characteristics of comparatively simple attacks on airlines cannot be underestimated.

MILITARY THREATS TO U.S. CONTROL OF THE AIR

For most nations, wartime posture towards the air commons is the inverse of their posture in peacetime. Instead of striving to sustain access and openness to all who meet a basic threshold of

A hallmark of the American way of warfare has been control of the air and the resulting freedom from attack and the freedom to attack. If control of air is in question — if air is accessible to many — forces on land, sea and in the air are vulnerable.

safety and technical expertise, the greatest benefit from the air commons during wartime derives from dominant control that explicitly limits access to the air. Echoing Luttwak's "paradox of war," what is logical for air in peacetime is illogical in wartime.[40] A hallmark of the American way of warfare has been control of the air and the resulting freedom from attack and the freedom to attack. If control of air is in question — if air is accessible to many — forces on land, sea and in the air are vulnerable.

Historically, the United States has arguably controlled the air during most military operations since World War II. As a result, both state and non-state adversaries are developing strategies and technologies to counter this persistent U.S. advantage. The most direct counter is the development of symmetric, or similar, capabilities to challenge U.S. aircraft in the air. Countries like Russia and China are not only increasing their own inventories of aircraft that, in many ways, outclass U.S. capabilities, but are exporting this hardware and knowledge to other countries around the globe. While the United States may not confront China or Russia directly, it is likely that U.S. control of the air will be contested with capabilities derived from Russia or China. More broadly, however, the larger threat to U.S. control of the air will be strategies that avoid a direct air-to-air contest, and degrade the utility of control of the air or target U.S. capabilities on the ground, where they are most vulnerable. Irregular warfare and the proliferation of precision surface-to-surface weapons may diminish the effects of control of the air or even place the achievement of control of the air altogether at risk.

Advanced Combat Aircraft

The U.S. Air Force and Navy are pursuing the F-22 and F-35 as the mainstays of the future fighter force. Integrating stealth and advanced avionics, these aircraft are at the core of the United States' investment strategy for achieving and sustaining control of the air. Looking to this future, the small F-22 force and slow-growing F-35 inventory likely will face much more capable air-to-air opponents relative to those seen in the past 20 years. Instead of fighting opposing air forces with relatively inferior equipment and training, future contests for control of the air will be more balanced and raise serious concerns over the America's ability to control the air.

The proliferation of advanced combat aircraft is largely the result of exports from Russia, with China playing an increasing role in cooperative research and development (Table 3). Of the advanced combat aircraft in service and on order, there is a wide presence of Russian-made or license-produced Sukhoi aircraft. Described as "Generation 4.5" and superior in many ways to the current Fourth Generation F-15, F-16 and F/A-18s in U.S. service, these Russian-developed fighters possess additional hard points for large numbers of air-to-air and air-to-ground weapons, vectored thrust maneuverability, extended range, and powerful radar and electro-optical sensors. In short, these emerging aircraft represent a potent technical competitor to the current generation of U.S. combat aircraft. In a departure from previous experience, the aircrews of these advanced aircraft may have training and operational prowess that could rival that of U.S. pilots. The well publicized Cope India exercises in 2004 and 2005 included media reports that U.S. forces were frequently "shot down" during exercises with the Indian Air Force and that the U.S. Air Force was surprised by the technical improvements made to the Indian

Table 3

ADVANCED COMBAT AIRCRAFT IN SERVICE OR ON ORDER[42]

NATION	AIRCRAFT	NUMBER IN SERVICE / ON ORDER
United States	F-22 F-35	113 / 64 0 / 2443
Russia	Su-27/30 Su-34 PAK-FA	445 10 / 48 Unknown
United Kingdom	Eurofighter F-35	33 / 161 0 / 150
China	Su-27/30/33 J-10 J-12	180 / 185 140 Unknown
India	Su-30 Multi-Role Combat Aircraft PAK-FA	53 / 177 0 / 126 Unknown
Pakistan	JF-17	8 / 142
Italy	F-35	0 / 131
Australia	F-35	0 / 100
Turkey	F-35	0 / 100
France	Rafale	44 / 62
Venezuela	Su-30	24
Malaysia	Su-30	12 / 6
Vietnam	Su-30	4

MiG-21s and Su-30s, as well as the quality of the pilots.[41]

In addition to being exporters or license producers, Russia and China are developing “fifth-generation” fighter aircraft and are heavily involved in cooperative research with other countries. The Russians have long been developing the PAK-FA program with MiG and Sukhoi design teams. In November 2009, India and Russia announced an expansion of their cooperative work on the PAK-FA and industry sources believe 2017 to be the target date for an Indian prototype.[43] While currently an importer and license producer of Su-30 aircraft, China is clearly moving toward an indigenously developed next generation combat aircraft. U.S. Secretary of Defense Robert Gates predicted that China will have no fifth-generation aircraft comparable to the F-22 by 2020. However, the deputy commander of the Chinese Air Force publicly declared that China will in fact have such an aircraft in service by that date.[44] Subsequent comments from the head of the state-owned military aircraft company, AVIC, did little to clarify this contradiction and suggested that China would instead focus expanding the capabilities of the current J-10 fighter, noting the potential for sales to Pakistan.[45]

Beyond the debate over specific dates, the larger issue is the broad pursuit of capabilities that outclass current U.S. fighters and compete directly with the next generation of U.S. fighter aircraft. With expertise and technology flowing out of China and Russia, U.S. control of the air likely will be more vigorously contested. Even if the United States never directly confronts Russia or China, these trends suggest that the United States will be fighting Russian and Chinese equipment. Given the small size of the F-22 fleet and recent concerns over cost growth and delays in the 300 billion dollars F-35 program, the ongoing proliferation of advanced combat aircraft should be cause for significant concern. With the increasing focus on irregular warfare and other asymmetric threats, the symmetric threats to U.S. control of the air should be neither forgotten nor discounted.

Surface-to-Air Missiles

In addition to states pursuing traditional military capabilities in the air, U.S. control of the air has pushed state and non-state actors to develop asymmetric methods of competition that are in fact more difficult to counter than previous, force-on-force challenges.

The challenge of SAMs is familiar to any analysis of air operations since the Vietnam War. The emergence of an integrated air defense system in North Vietnam and the resulting losses of U.S. Air Force and Navy aircraft drove the development of an integrated set of tactics, equipment and entirely new aircraft. When escorts emerged during the strategic bombing campaigns of World War II, enemy fighters were the only threat. However, during Vietnam, the threat from air and ground drove the use of electronic warfare and fighter escort aircraft became standard for all “strike packages” ranging over North Vietnam. Dense air defenses in Central Europe, and the shocking effectiveness of the SA-6 SAM against the Israeli Air Force during the 1973 Yom Kippur War reinforced the need to suppress enemy air defenses and pushed the United States to design a more fundamental response to surface-to-air systems in the form of radar signature reduction known as stealth.

The effectiveness of the U.S. response to these air defenses, including a small stealth fighter force, burst into full view in 1991 during the 1,000-hour air campaign over Iraq and the 100-hour ground war that followed. Faced with a Soviet-designed and equipped air defense system, the Air Force and Navy secured air superiority over Iraq and faced little sustained opposition except unguided ground fire. In fact, the brief air campaign over the Balkans in 1995 repeated the operational pattern of suppressing enemy air defenses followed by relatively unchallenged operations.

However, by 1999, operations over Kosovo offered a glimpse into the emerging challenges to U.S. control of the air that are likely to accelerate. U.S. and NATO air forces were not able to execute a sequential campaign that secured enduring control of the air and they never fully defeated the more resilient and capable air defenses fielded by the Serbs. Eschewing wireless communications that are subject to tracking, jamming and destruction, the Serbs used buried land lines to integrate their air defenses and limit the ability to target specific air operations centers that would bring down the entire network. In addition, the Serbs changed their standard SAM operations to operate the radars only briefly before launching a salvo of weapons. While not capable of changing the overall outcome — 79 days of air strikes did conclude with Serbia's capitulation — the Serbs sustained a latent threat to U.S. control of the air that in fact brought down a stealthy F-117 and forced the use of jamming aircraft throughout the conflict.

The air defense environment is rapidly moving past these legacy systems. The easily defeated "middle" of the air defense spectrum is being displaced by a more lethal and resilient threat of MANPADSs and "double-digit" SAMs. Mostly developed during the last decade of the Cold War, these surface-to-air-missiles are coined "double digit" by their NATO code names and characterized by long range mobile launchers and advanced radars. As a system, these weapons are focused on countering U.S. control of the air through increased lethality, the defeat of stealth, and targeting of standoff command, control and refueling assets (Table 4). Double-digit SAMs not only

Table 4

THE EFFECT OF DOUBLE-DIGIT SAMS[46]

DOUBLE-DIGIT SAM CHARACTERISTIC	EFFECT ON CONTROL OF THE AIR
Long range and speed	• Limits survivability of non-stealthy aircraft. • Limits ability of all aircraft to approach within weapons range. • Able to target ISR, C2, and refueling aircraft operating at stand-off distances.
Radar capabilities	• Jam-resistance provides adversary with additional warning and awareness. • Low frequency radars offer improved capabilities against stealth.
Mobile launchers	• Increases difficulty of targeting launchers at long range. • Requires more accurate and up-to-date targeting information.
Distributed, resilient command and control	• VOIP, redundancy, and commercial IT means more resistance to jamming. • Less exposure to single point failures.

decrease the survivability of non-stealthy combat and support aircraft, but they are also more difficult to defeat using current tactics. In fact, Russian SA-20 SAM deployments reportedly caused NATO to decide against deploying the Airborne Warning and Control System (AWACS) aircraft during the conflict with Georgia in 2008.[47]

While the primary source of advanced SAM technology is Russia, the number of operators is growing. In early 2009, the director of the Defense Intelligence Agency noted that China possesses sixteen SA-20 battalions and an equivalent number of shorter-range, but still lethal, SA-10 systems.[48] Around the globe, other reported customers of the SA-10 and SA-20 include Iran, Libya, Algeria, Venezuela and Vietnam.[49] In addition, China is developing an indigenous variant of the SA-10, the HQ-9, which is now available for export, repeating the trend of proliferation seen with combat aircraft.[50]

Advanced SAM systems are relatively easier to field and operate than other weapon systems that challenge U.S. control of the air. Combat aircraft and aircraft carriers require years of extensive training, maintenance and flight operations to reach competency, but the SA-10/20 systems are well-suited for conscript operators and are able to achieve operational capability within months of deployment.[51] In this way, advanced SAMs may upset the long held assumption that adversaries might have advanced equipment but lack the expertise and training to use the equipment effectively. The United States will not only face advanced SAMs but also lack the advantage of poorly trained adversaries.

Threats to Bases on Land and Sea

Building on a 50-year cycle of measure and countermeasure, surface-to-air threats surely will challenge U.S. control of the air. Absent from much of this struggle, however, was any need to actually defend U.S. operating bases or the long logistical lines to sustain these bases. In fact, the United States routinely operates from secure sanctuaries on land and at sea in order to achieve control of the air. Since the Cold War these runways, taxiways, hangars, fuel bunkers, air operations centers, carrier battle groups, munitions ships and oilers that enable control of the air commons have rarely been systematically threatened.

Distinct from changing SAM threats, the emerging threat from precision surface-to-surface missiles will cause a potential revolution in how the United States conceives of and plans for securing control of the air. Rather than focusing on wresting control of the air from another country, the United States also will have to defend its own bases and airspace. Faced with a variety of ballistic missiles, cruise missiles, rockets, and artillery capable of striking airbases and aircraft carriers, the threat to the air commons is as much about challenges to bases, aircraft carriers, and logistics on the surface as it will be about challenges to aircraft in the air.

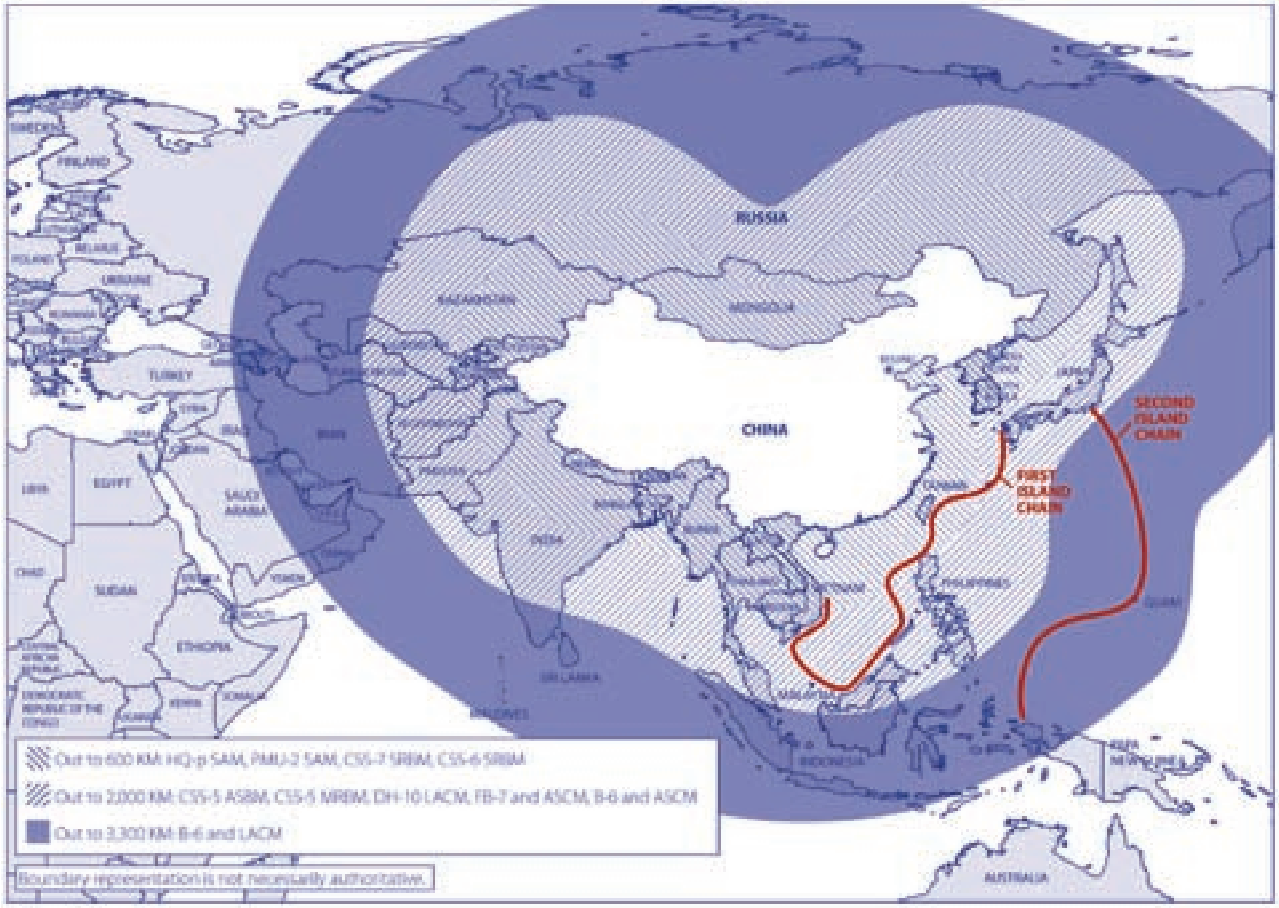
Destroying bases is more effective and efficient than facing a dispersed, maneuvering, and armed opponent in the air. Germany's focus on British fighter bases in the Battle of Britain, the Japanese attempt to catch U.S. aircraft carriers at Pearl Harbor, attacks on U.S. airbases in Vietnam, and the targeting priorities of U.S. air campaign planning all illustrate the enduring quest to destroy the logistical underpinnings of air power on land or at sea.[52] Long a hallmark of U.S. air campaigns, this tactic will soon be a viable threat against U.S. forces.

Proliferating ballistic and cruise missiles are the most significant threats to U.S. bases. Russia and China are by far the largest operators of non-nuclear ballistic and cruise missiles and act as the fundamental source of hardware and technical assistance around the globe.[53] In particular, the growth of China's missile capabilities threatens to undermine the ability of the U.S. Air Force and Navy to credibly project power into the western

Pacific. China's Joint Anti-Air Raid operational strategy incorporates aircraft, ballistic missiles, cruise missiles, and space and air-breathing intelligence to comprehensively degrade the ability of an adversary to deploy into the region and sustain operations. In 2009, Gates noted that these "investments in cyber and anti-satellite warfare, anti-air and anti-ship weaponry, and ballistic missiles could threaten America's primary way to project power and help allies in the Pacific—in particular our forward air bases and carrier strike groups."[54] The main operating bases in Okinawa, the main islands of Japan, as well as the increasingly important base on the U.S. territory of Guam are already well within striking distance of Chinese missile systems (Figure 2).[55]

Typically, the ability of the United States to integrate land-and sea-based aviation ensured a capable and effective means of achieving control of the air. However, China is adapting to U.S. carrier aviation, significant to the 1996 Taiwan Straits crisis, by developing robust anti-ship capabilities to target U.S. carrier battle groups. Recently identified by the Office of Naval Intelligence, this variant of the DF-21 ballistic missile is the "world's first anti-ship ballistic missile" and "specifically designed to defeat U.S. carrier strike groups."[56] Combined with growing inventories of anti-ship cruise missiles and other sub-surface threats, the ability of U.S. carriers to effectively project power using carrier-based aircraft is at risk.

Figure 2: Chinese Anti-Access


RUSSIA
FINLAND
UKRAINE
KAZAKHSTAN
MONGOLIA
TURKEY
IRAN
CHINA
JAPAN
SECOND ISLAND CHAIN
FIRST ISLAND CHAIN
EGYPT
LIBYA
SAUDI ARABIA
CHAD
SUDAN
ETHIOPIA
KENYA
DEMOCRATIC REPUBLIC OF THE CONGO
INDIA
SRI LANKA
MALDIVES
PHILIPPINES
GUAM
INDONESIA
PAPUA NEW GUINEA
AUSTRALIA
▨ Out to 600 KM: HQ-9 SAM, PMU-2 SAM, CSS-7 SRBM, CSS-6 SRBM
▨ Out to 2,000 KM: CSS-5 ASBM, CSS-5 MRBM, DH-10 LACM, FB-7 and ASCM, B-6 and ASCM
■ Out to 3,300 KM: B-6 and LACM
Boundary representation is not necessarily authoritative.

United States Department of Defense, "Annual Report to Congress on the Military Power of the People's Republic of China," 2009.

As with advanced SAMs, the threat to U.S. control of the air may be greatest in rising states such as China, but regional powers—most notably North Korea and Iran— also pose a significant threat as they are also gaining access to these weapons. Iran and North Korea's test programs have not been absolute success stories, but their willingness to press on with research and development, cooperate across borders, and engage with non-state technical experts suggests that such anti-access weapons will present an enduring threat to the United States. Less expansive and accurate than the Chinese arsenal, these ballistic missiles nonetheless can range across the Middle East and northeast Asia to target cities or bases. Short distances and choke points mean that Iran's inventory of anti-ship missiles can quickly target ships operating in the confines of the Persian Gulf. Given these threats, the historical pattern of multiple bases and carrier strike groups operating relatively close to the adversary may no longer be viable.

While typically a concern during state-on-state conflict, operations in Iraq, Afghanistan and Lebanon also illustrate the emerging threat to bases from irregular warfare. For years, forward operating bases and airbases in Iraq and Afghanistan coped with relatively inaccurate mortar and rocket attacks. Often surrounded by crowded, urban environments, U.S. forces employed sophisticated counter-battery radars and to identify the point of origin for these attacks while employing rapid reaction infantry and security forces to push out the security perimeter around these installations.[57] Hezbollah vividly demonstrated the ability of a non-state actor to operate with the lethality and reach of a state when it successfully hit an Israeli warship with a surface-to-surface missile during the 2006 conflict. The widespread use of shorter-range Katyusha rockets, longer-range systems, and even anti-ship missiles marked a dramatic shift in the threats likely to face the logistical nodes that support U.S. air power during steady state operations.[58]

Looking to the future, the widespread availability of GPS and other off-the-shelf technologies mean that rockets and mortars will become more disruptive to U.S. air operations as they increase in accuracy. Already in use or under development with the U.S. Army, GPS-guided artillery and mortar rounds in the hands of the Taliban, Hezbollah, or other non-state actors would challenge the ability of the United States to base fighters, unmanned aerial vehicles (UAV), airlift assets and other aircraft. Better terminal guidance and "fire and forget" guidance would dramatically improve the accuracy of these weapons, popularized as G-RAMM (guided rockets, artillery, mortars, and missiles).[59] It would be a far cry from the occasional "golden BBs" that found success in Vietnam, Iraq, and Afghanistan if insurgents could more consistently and accurately target taxiways, fuel bunkers, aircraft revetments and hangers, power generation and dorms. Taking cues from IEDs and traditional ambushes, these precision indirect fires would amplify the pressure on supply convoys and put the associated logistics tail—from port to flight line—at risk. Increasing force protection will be one likely response but will require the diversion of manpower, equipment, and leadership time away from the mission. Similarly, moving to more secure and distant bases on land or at sea will mean increased refueling requirements, less time on station, and decreased effectiveness in interdiction and close air support.

Irregular Warfare

Threat to bases from precision weapons from non-traditional forces suggests the broader strategic challenge irregular warfare will pose to U.S. control of the air. Overall, the emergence of irregular warfare itself challenges the effectiveness and decisiveness that control of the air typically has meant in wartime. Motivated and shaped by a variety of social, economic and political forces, irregular warfare presents a more complicated and less linear battlespace than traditional state-on-state conflict. Foremost, the absence of large, massed formations means a more diffuse target for airborne sensors and weapons. The ability to decisively find and destroy adversary capabilities is degraded and the lack of physical centers of gravity challenges mainstream targeting strategies. When the enemy shares space with civilians in urban environments, the ability to distinguish friend from foe is difficult from five meters—and incredibly difficult from 5,000 meters. Moreover, even if adversaries can be identified from the air, their close proximity to civilians—the very population that is the ultimate center of gravity—means the risk of collateral damage.

To compensate for these new challenges, the United States adapted equipment and procedures to identify diffuse enemies and target them even more precisely. The United States has employed long-term force posture adjustments, such as smaller yield weapons, UAVs and widespread distribution of streaming video; targeting pods primarily to observe and secondarily to guide weapons; and JSTARS (Joint Surveillance and Target Attack Radar System) to assess long-term patterns of behavior and detect enemy activity. In spite of these adaptations, commanders are still concerned about the effects of airstrikes in irregular warfare and they have scaled back the use of air power in Afghanistan. Gen. Stanley McChrystal's statement that "air power contains the seeds of our own destruction if we do not use it responsibly," reflects the self-deterring effect that irregular warfare may have on the United States' use of air power.[60] These changes to U.S. policy governing use of air power illustrates that even if the U.S. military's control of the air commons is not contested, the value of that control may decline.

The growing asymmetric threats to basing and the logistical foundations of air power will force a re-ordering of priorities in the U.S. Air Force and Navy. Increasingly accurate and available rockets, artillery, missiles, and mortars will be able to disrupt air operations when aircraft are not at speed and altitude. Rather than targeting air power in the air where it is strongest, targeting bases on the surface will nonetheless have the same effect: limiting U.S. control of the air commons.

Even if the U.S. military's control of the air commons is not contested, the value of that control may decline.

Altogether, the air commons is under increasing stress during peacetime and wartime. The limitations of the current ATC system, combined with questions over GPS, raise concerns over an air transportation system that is already being directly targeted through a range of terrorist methods. In peacetime, the goal is openness and access in the air; in wartime, the use of the air is optimized when access is limited and one actor controls all activity, thus ensuring freedom to attack and freedom from attack. As a reflection of the benefits of controlling the air, nations and non-state actors are developing symmetrical and asymmetrical responses that limit the United States' ability to control the air commons. Whether through combat aircraft, advanced surface-to-air missiles, threats to bases at land and sea, or irregular warfare, adversaries are reducing the margin of control that underpins U.S. military operations.

Protecting the Air Commons: Recommendations

The air commons is an essential medium for the pursuit of trade and economic growth in peacetime and a proven means of exerting control in wartime. There is not a single military or commercial remedy to defend a space that can so rapidly and violently shift between peace and war. Moreover, given the links between air and the other domains of land, cyber, space and sea, protection of the air commons cannot occur only in the air. The United States should therefore adopt a multifaceted strategy to protect the openness of the air commons. This strategy should include the following elements:

1. **Modernize civil systems to ensure safe passage and maintain the public confidence that is so crucial to the air commons.**

- **Continue to advocate advanced ATC systems that are interoperable worldwide.** The increased density and complexity of the air commons requires increased enhancement of the ATC, primarily through incorporation of space and cyberspace technologies. To maintain seamless operations within the air commons, ATC systems must be fully interoperable worldwide.
- **Ensure reliable, accurate, and global means of navigation and timing for air traffic.** Real and perceived concerns over the reliability of GPS require the United States to act decisively in order to remain the provider of choice for global navigation. The United States should continue to facilitate global, nondiscriminatory access to the air commons by bolstering the current GPS constellation or by the concerted development of a follow-on space system. To ensure access to this global public good the United States must remain the indispensable nation promoting cooperation and engagement concerning the air commons. As a primary producer and user of aerospace technology, the ability of the United States to shape this competitive marketplace also will reap substantial economic benefits.

2. **Expand access to the air commons and increase the number of stakeholders.**

- **Encourage liberalization.** The United States should continue to encourage regional progress towards liberalizing Open Skies agreements. Ultimately, it should create an overarching international air regime focused on the principles of free-market competition while maintaining its quality of service and the highest standards for safety. The United States should also encourage regional trade organizations (such as Asia-Pacific Economic Cooperation) to institute more liberalized policies. Expanded access to the air commons will not only create valuable spillover effects—such as economic development—but will also increase the number of stakeholders willing to protect the air commons in the future.
- **Use foreign assistance to develop the aviation capabilities of pivotal countries.** Enabling access to the air commons promotes economic development in countries or regions of concern to the United States. Access facilitates integration into international markets, creates industries and small businesses, establishes a mechanism for increased employment, and provides an opening for increased international investment and integration. As such, the United States should target foreign aid investments to countries' aviation infrastructures to include airports and supporting facilities, navigation systems networks, and training for operators and managers.

3. **Improve the security of air traffic in peacetime.**

- **Continue to strengthen peacetime aviation security.** The ability of terrorists and criminals to exploit the air commons has been a hallmark of the past 50 years. While it lacks a single point solution, the United States should strive for the harmonization and implementation of best practices at airports and aviation facilities. Terrorists seek to destroy public confidence in air travel because losing that confidence would have damaging ripple effects across the U.S. and global economy. The United States should fight back by building public confidence and the underlying aviation security systems necessary to achieve that objective.

- **Encourage the expansion and enforcement of global norms and treaties against proliferation of MANPADSs.** The current web of relevant agreements—including the Wassenaar Arrangement, ICAO, the Organization for Security and Co-operation in Europe, Organization of American States, and the Asia Pacific Economic Cooperation—has made progress in limiting MANPADS exports to and a ban on transfers to non-state actors. The United States should continue to finance and pursue the destruction of excess MANPADSs and ensure close end-user controls on its MANPADS exports. In addition, the United States should encourage rising powers with large stakes in the safety and viability of a robust air transportation system to abide by existing agreements and, more importantly, restrict the transfer of these weapons. Given the role of Russia and China in the proliferation of other advanced weapons, the United States should ensure the reappointment of the Special Envoy for MANPADS Threat Reduction, and encourage responsible MANPADSs stewardship for these rising global powers.

4. Maintain U.S. control of the air.

- **Bolster the range and survivability of U.S. air power.** As threats to bases and aircraft grow, the United States should reassess the mix and capabilities of its air power portfolio. The ranges of current and projected surface-to-air and surface-to-surface missile systems will dramatically reshape the familiar terms of competition in the air. Apart from defending airbases and aircraft carriers themselves, the United States should continue to press for a sufficient number of long-range, stealthy aircraft. The F-35 may possess the stealth and avionics to compete against future threats, but its unrefueled range—akin to an F-86 *Sabre* from the Korean War—may risk being locked out of operating bases well within the threat rings of surface-to-surface missiles.[61] In addition, the Air Force and Navy should consider further procurement of stand-off weapons for use from ground, sea and air units. Aside from changes in the capability of platforms, the United States should consider the role weapons can play in ensuring a credible and survivable deterrent and, if needed, a war-fighting force from the air.
- **Dramatically increase the resilience of airbases and carrier strike groups.** Across irregular and conventional war-fighting scenarios, the sources of air power—bases and aircraft carriers—are increasingly at risk. To complement changes in capabilities, the United States should pursue a three-part strategy for improving the resilience of airpower's logistical underpinnings. First, the United States should investment in active base defenses, including Aegis, Terminal High Altitude Area Defense (THAAD), and other alternatives, including directed energy, to cope with the future volume of potential G-RAMM attacks on U.S. bases and carrier battle groups. Second, the United States should enhance passive base defenses to increase ambiguity in the minds of potential adversaries. While continuing to develop a small number of well-known main operating bases, the United States should initiate a sustained political and diplomatic effort to expand the number of accessible airfields and facilities in U.S. territories and within the borders of allies and partners. For all bases, the United States also should expand the use of decoys and hardened shelters, and the availability of rapid repair equipment. Finally, the United States should reduce airpower's reliance on energy, a fundamental enabler of air operations at land and at sea and a prime target for emerging G-RAMM threats. Including propulsion, design, materials and operating concepts, the United States should seek a decisive reduction in the operational risks associated with the

To reap continued benefits of the air commons in the future, it is time to streamline and strengthen the institutions that protect access to the air while countering new threats to that access.

disruption of assured energy supplies. Only with sufficiently defended and supplied bases on land and at sea will the United States continue to control the air.

Conclusion

Dependable and open access to the air commons is vital to U.S. national interests and a thriving international economy. This access is also essential to American military power. For these reasons, the United States should reinvigorate its long-standing commitment to defend the air commons and expand access to the air. The air commons has achieved a level of global governance not seen in the other commons, largely because of the vision of its developers, the international agreements that manage use of the air, and the recognized interdependence of all participating states. To reap continued benefits of the air commons in the future, it is time to streamline and strengthen the institutions that protect access to the air while countering new threats to that access.

As the only global air power, the United States has a decisive and asymmetric advantage against would-be adversaries. No state is able to compete directly with the United States in the air commons. This dominance forces challengers to look for ways to contest the air from the other domains and commons, threatening not only air assets themselves, but also the basing and logistical line. To defend against these new threats, the U.S. military should learn from its mistakes and adapt to new tactics, as well as incorporate better technologies. The United States takes undisputed control of the air for granted. It should not. Defending this control will require active steps by the United States, with tremendous benefits for U.S. national security.

ENDNOTES

[1] *The Economic and Social Benefits of Air Transport 2008,* An Air Transport Action Group Study, (2008): 2-9.

[2] *Ibid.*

[3] For a comparison of these two theorists, see Jeffrey G. Lofgren, "21st Century Air Power Theorists: Who Has it Right, John Warden or Robert Pape?" National War College, (2002), http://handle.dtic.mil/100.2/ADA442423.

[4] For a further look at air as transforming warfare, see Eliot Cohen, "The Mystique of U.S. Air Power," *Foreign Affairs,* January/February 1994, and William Perry, "Desert Storm and Deterrence," Foreign Affairs, (Fall 1991): 66.

[5] Central Intelligence Agency, *World Fact Book,* (2009), https://www.cia.gov/library/publications/the-world-factbook/fields/print_2053.html.

[6] "Convention Relating to the Regulation of Aerial Navigation" as quoted in the Federal Aviation Administration's essay entitled *International Civil Aviation,* http://www.centennialofflight.gov/essay/Government_Role/Intl_Civil/POL19.htm.

[7] By way of example, American Railway Express shipped 45,859 pounds of cargo in 1927, and by 1931, it had grown to shipping over 1 million pounds of cargo via air. In 1940, over 3 million Americans flew. See the Federal Aviation Administration's essays entitled *A History of Commercial Air Freight,* available at http://www.centennialofflight.gov/essay/Commercial_Aviation/AirFreight/Tran10.htm and *Air Travel: Its Impact on the Way We Live and the Way We See Ourselves,* http://www.centennialofflight.gov/essay/Social/impact/SH3.htm.

[8] Federal Aviation Administration's essay entitled, *Government Funding of Airports,* available at http://www.centennialofflight.gov/essay/Government_Role/airports-growth/POL10.htm.

[9] International Civil Aviation Organization, available at http://www.icao.int/icao/en/anb/mais/index.html.

[10] Statement by President Jimmy Carter on signing the bill into law, February 15, 1981, available at http://www.presidency.ucsb.edu/ws/index.php?pid=32939. According to the FAA, prior to deregulation, U.S. domestic market carried 205 million passengers in 1975; after deregulation, that number jumped to 297 million (1980).

[11] Open Skies Agreement Highlights, U.S. State Department, available at http://www.state.gov/e/eeb/rls/fs/2009/119760.htm; Department of Transportation, Office of International Aviation, available at http://ostpxweb.dot.gov/aviation/X-40%20Role_files/bilatosagreement.htm.

[12] *The Economic Impact of Air Service Liberalization,* An InterVISTAS-ga2 study, (2008): ES-2.

[13] Dr. David Pritchard, *Globalization of Commercial Aircraft Manufacturing,* University of Buffalo, (January 2005), http://www.leeham.net/filelib/pritchard84thannualtrbmeetingjan05b.ppt.

[14] *Ibid.*

[15] *Ibid.*

[16] IATA, *Aviation Economic Benefits,* (2008), http://www.iata.org/NR/rdonlyres/35FC46A4-20FB-4E10-9B0C-77651B78A4CD/0/890700_Aviation_Economic_Benefits_Summary_Report.pdf.

[17] "Middle East takes to the air!" *Foreign Affairs* (September/October 2009).

[18] Barry Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security*, Vol 28, No.1, (Summer 2003): 8.

[19] Interview with Lt Col Kelly Martin, 447th Expeditionary Operations Support Squadron Commander, (January 2009).

[20] *Ibid*, 21.

[21] Bureau of Transportation Statistics, Department of Transportation, *Airline On-Time Statistics and Delay Causes — Causes of National Aviation System Delays, National* (June 2003 - October 2009), http://www.transtats.bts.gov/OT_Delay/ot_delaycause1.asp?type=5&pn=1, (20 December 2009).

[22] Notable air traffic control disruptions since 2000 include: Atlanta and Salt Lake City, November 2009; Atlanta, August 2008; Atlanta, June 2007; Los Angeles, September 2004; Palmdale, May 2001; and Palmdale, October 2000.

[23] Federal Aviation Administration, *NGATS Implementation Plan,* (2009): 5-6; and National Air and Space Administration, *Next Generation Air Transport System Air Traffic Management-Airspace Project, 1 June 2006*, 1.

[24] Need source for growth of GPS in aircraft; for more on role of GPS in the NextGen system, see Federal Aviation Administration, *NextGen Implementation Plan 2009,* Washington, DC: Federal Aviation Administration, (2009), http://www.faa.gov/about/initiatives/nextgen/media/ngip.pdf.

[25] Government Accountability Office, *GLOBAL POSITIONING SYSTEM: Significant Challenges in Sustaining and Upgrading Widely Used Capabilities,* April 2009, Washington, DC: Government Accountability Office, (2009): 19-20; http://www.gao.gov/new.items/d09325.pdf.

[26] *Ibid*, 22.

[27] For more information regarding the NextGen system, see the Federal Aviation Administration's *NextGen Implementation Plan,* (2009), http://www.faa.gov/nextgen; and for more information comparing SESAR and NextGen, see NCOIC's *Comparison of the SESAR and NextGen Concepts of Operations* report, (May 2008), https://www.ncoic.org/apps/group_public/download.php/12026/SESAR_NextGen_Comparison%2020090317FINAL.pdf.

[28] Eric Platteau, *SESAR Joint Undertaking — Focus on: Interoperability*, (10 December 2009), http://www.atc-network.com/News/32094/SESAR-Joint-Undertaking---Focus-on--interoperability.

[29] Federal Aviation Administration, *Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems*, Report Number: FI-2009-049," (4 May 2009): 4; http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/ATC_Web_Report.pdf.

[30] Brenner, Joel, "Business Strategies in Cyber Security and Counterintelligence," *Remarks to the Applied Research Laboratories at the University of Texas at Austin*, (3 April 2009):, 3-4, http://www.dni.gov/speeches/20090403_speech.pdf.

[31] U.S. Department of State, Significant Terrorist Incidents, 1961-2003: A Brief Chronology, (March 2004), http://www.state.gov/r/pa/ho/pubs/fs/5902.htm and "Airport incident 'was terrorism'" *British Broadcasting Company*, (1 July 2007), http://news.bbc.co.uk/2/hi/uk_news/scotland/6257846.stm.

[32] Chow, James, et al, *Protecting Commercial Aviation against the Shoulder-Fired Missile Threat*, Santa Monica, CA: RAND Corporation, (2005): 23-24, Table 7-1, http://www.rand.org/pubs/occasional_papers/2005/RAND_OP106.pdf.

[33] Bolkcom, Christopher, *Homeland Security: Protecting Airliners from Terrorist Missiles*, Congressional Research Service Order Code RL31741, (16 February 2006): 9, http://fas.org/sgp/crs/terror/RL31741.pdf. U.S. Department of State, Bureau of Political-Military Affairs, Office of Weapons Removal and Abatement, *MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense Systems*, (31 July 2008), http://merln.ndu.edu/archivepdf/terrorism/state/107632.pdf.

[34] *Ibid*.

[35] *Ibid*.

[36] National Commission on Terrorist Attacks on the United States, 153.

[37] *Ibid*, 154.

[38] See "'Airlines terror plot' disrupted," *British Broadcasting Company*, (10 August 2006), http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk_news/4778575.stm; and "More plane terror plots 'likely'," *British Broadcasting Company*, (8 September 2009), http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk_news/8244065.stm?ad=1. http://news.bbc.co.uk/2/hi/uk_news/8244065.stm; " . . . from compounds, bases and means of transport, especially Western and American airlines — will be the direct targets of our next operations," (June 2004), http://www.cbsnews.com/stories/2004/05/25/terror/main619569.shtml.

[39] Bin Laden, Osama, "Transcript: Translation of Bin Laden's Videotaped Message," *Washington Post*, (1 November 2004), http://www.washingtonpost.com/wp-dyn/articles/A16990-2004Nov1.html.

[40] Luttwak, Edward, *Strategy: The Logic of War and Peace*, (Cambridge, MA: Belknap Press of Harvard University Press, 1987): 7.

[41] Baldauf, Scott, "Indian Air Force, in war games, gives U.S. a run," *The Christian Science Monitor*, (28 November 2005), http://www.csmonitor.com/2005/1128/p01s04-wosc.html.

[42] Flightglobal.com, "Directory: World Air Forces," *Flight International*, (11-17 November 2008): 52-76, http://www.flightglobal.com/assets/getasset.aspx?ItemID=26061.

[43] Govindasamy, Siva, "Russia, India to advance deal on PAK-FA fighter variant," *Flight International*, (12 November 2009), http://www.flightglobal.com/articles/2009/12/11/335995/russia-india-to-advance-deal-on-pak-fa-fighter-variant.html.

[44] Govindasamy, Siva, "China expects fifth generation fighter in 10 years," *Flight International*, (11 December 2009), http://www.flightglobal.com/articles/2009/11/12/334680/china-expects-fifth-generation-fighter-in-10-years.html; Gates, Robert M., *Speech to the Economic Club of Chicago*, Chicago, IL, (16 July 2009), http://www.defense.gov/speeches/speech.aspx?speechid=1369.

[45] Govindasamy, Siva, "China to complete J-10 development before launching fifth-generation fighter," *Flight International*, (17 November 2009), http://www.flightglobal.com/articles/2009/11/17/335107/china-to-complete-j-10-development-before-launching-fifth-generation.html.

[46] Bolkcom, Christopher, *Military Suppression of Enemy Air Defenses (SEAD): Assessing Future Needs*, Congressional Research Service Order Number RS21141, (11 May 2005): 2-3, http://www.fas.org/sgp/crs/weapons/RS21141.pdf.

[47] Fulghum, David A. and Barrie, Douglas, "Russia Sells SA-20 to Iran," *Aviation Week*, (12 December 2008), http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=awst&id=news/aw121508p2.xml.

[48] Maples, Michael D., Lieutenant General, U.S. Army, ANNUAL THREAT ASSESSMENT: Statement before The Committee On Armed Services, United States Senate, (10 March 2009): 2, http://armed-services.senate.gov/statemnt/2009/March/Maples%2003-10-09.pdf; U.S. Department of Defense, *Annual Report to Congress: Military Power of the People's Republic of China*, 2009, 50, 66; http://www.defense.gov/pubs/pdfs/China_Military_Power_Report_2009.pdf.

[49] "Venezuela buys powerful missiles with Russian loan," *Reuters*, (14 September 2009), http://www.reuters.com/article/idUSTRE58C1YR20090914; Kopp, Carlo, Dr., *Proliferation of Advanced Surface to Air Missiles*, Air Power Australia, (June 2009), http://www.ausairpower.net/APA-S-300-Proliferation.html; "Russia has assured Iran on missile delivery: diplomat," *Agence France Presse*, (27 November 2009), http://www.google.com/hostednews/afp/article/ALeqM5gMp9L77JriWEquReS9_u_UiXrzXQ; Ibid, Fulgham and Barrie.

[50] Chang, Andrei, "China exports new surface-to-air missile," *United Press International*, (18 March 2009), http://www.upi.com/Business_News/Security-Industry/2009/03/18/China-exports-new-surface-to-air-missile/UPI-30271237410000/.

[51] Kopp, Carlo, Dr., *Almaz S-300P/PT/PS/PMU/PMU1/PMU2, Almaz-Antey S-400 Triumf, SA-10/20/21 Grumble/Gargoyle: Technical Report APA-TR-2006-1201*, Air Power Australia, (December 2008), http://www.ausairpower.net/APA-Grumble-Gargoyle.html.

[52] Even against an adversary like Afghanistan that lacked any meaningful air force, the initial phases of the air campaign included strikes against nearly a dozen air bases. Rumsfeld, Donald and Myers, Richard, General, USAF, *Briefing on Enduring Freedom*, U.S. Department of Defense, (7 October 2001), http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2011, and associated briefing slide on air strikes at http://www.globalsecurity.org/military/ops/images/011009-d-6570c-002.jpg.

[53] For a summary of ballistic and cruise missile developments, see National Air and Space Intelligence Center, *Ballistic and Cruise Missile Threat*, NASIC-1031-0985-09, (April 2009); http://www.fas.org/irp/threat/missile/naic/NASIC2009.pdf.

[54] Gates, Robert M., *Speech to Air Force Association Convention*, National Harbor, MD, (16 September 2009); http://www.defense.gov/speeches/speech.aspx?speechid=1379.

[55] US Department of Defense, *Annual Report to Congress: Military Power of the People's Republic of China, 2009*, Figure 5, 23; http://www.defense.gov/pubs/pdfs/China_Military_Power_Report_2009.pdf.

[56] Office of Naval Intelligence, *The People's Liberation Army Navy: A Modern Navy with Chinese Characteristics*, (August 2009): 8; http://www.nmic.navy.mil/Intelligence_Community/docs/china_army_navy.pdf.

[57] For an assessment of how U.S. Air Force security forces have adapted to the mortar and rocket threat in Iraq, see Grant, Rebecca, "The Security Forces Rewrite," *Air Force Magazine*, (January 2006); http://www.airforce-magazine.com/MagazineArchive/Pages/2006/January%202006/0106security.aspx.

[58] Cordesman, Anthony H., *The Lessons of the Israeli-Lebanon War*, Washington, DC: Center for Strategic and International Studies, (March 2008): 17, http://csis.org/files/media/csis/pubs/080311_lessonleb-iswar.pdf.

[59] Ehrhard, Thomas P., *An Air Force Strategy for the Long Haul,* Washington, DC: Center for Strategic and Budgetary Assessments, (2009): 34, http://www.csbaonline.org/4Publications/PubLibrary/R.20090917.An_Air_Force_Strat/R.20090917.An_Air_Force_Strat.pdf; James Bonomo, et al., *Stealing the Sword,* Santa Monica, CA: RAND Corporation, (2008): 28-29 and 32-33, http://www.rand.org/pubs/monographs/2007/RAND_MG510.pdf.

[60] Motlagh, Jason, "U.S. to limit air power in Afghanistan," *Washington Times*, (24 June 2009), http://www.washingtontimes.com/news/2009/jun/24/us-to-limit-air-power-in-afghanistan.

[61] Both possess an unrefueled combat radius of about 600 miles. F-86 range found in Kamps, Charles Tustin, "The F-86 Sabre," Air & Space Power Journal, (Summer 2003): 78, http://www.airpower.maxwell.af.mil/airchronicles/apj/apj03/sum03/sum03.pdf; F-35 range found in Davis, Charles, Major General, USAF, *F-35 Lightning II Program Brief,* Joint Strike Fighter Program Office, (26 September 2006): 6, http://www.jsf.mil/downloads/documents/AFA%20Conf%20-%20JSF%20Program%20Brief%20-%2026%20Sept%2006.pdf.

CHAPTER IV:
BEYOND THE STALEMATE IN THE SPACE COMMONS

By Eric Sterner

JANUARY 2010

Contested Commons:
The Future of American Power in a Multipolar World

BEYOND THE STALEMATE IN THE SPACE COMMONS

By Eric Sterner

Introduction

The space commons are critical to the global economy and a key enabler of modern warfare. Satellite-based positioning information, overhead imagery and communications facilitate global coordination of commercial, scientific, and military activities with a degree of speed and precision that would be impossible without the use of outer space. Eight countries, plus the European Union, have the ability to independently place satellites into orbit, and any individual or country can utilize satellite technology by simply purchasing time on commercial satellites.

In general, space can be understood as a utility that lies at the heart of other international activities. Space enables other economic, social, political and cultural activities to take place, just as maritime transportation or telecommunications networks facilitate the distribution of energy, water, and food. Often, space capabilities are embedded in each of these other critical infrastructures.

The international community and the United States share a significant interest in maintaining the openness of space. Yet the fragility of space as a common, along with the emergence and proliferation of military anti-satellite technologies, will threaten the openness of the space commons in the coming decades. Moreover, policies toward space have not evolved to account for the role it plays in the international system, nor do they adequately protect the space commons from contemporary threats and challenges.

Debates have reached a stalemate due to disputes over "space weaponization." There are primarily two camps in this debate. To simplify, the realist camp views space as a zero-sum game in a self-help system in which the American ability to exert "space control" will preserve the peace. The realists fear cooperation that ultimately compromises the security of the United States and the global commons. On another side, the liberal camp focuses on a positive-sum game in which cooperation contributes to the achievement of mutual interests. Those on this side of the debate fear a scenario in which the fixation on self-interest compromises shared interests. This chapter will attempt to move beyond this stalemate by casting space as a global commons in which states can better identify their interests and use a combination of military capabilities, international agreements and regimes to maintain the commons.

This chapter will describe the nature of the space commons, exploring its role in the global economy and modern military operations while exploring contemporary international governance of the space commons. It will then identify enduring U.S. interests in space and potential threats, before concluding with recommendations to preserve the openness of the commons while maintaining the ability to respond to military threats in orbit.

The Space Commons and the International System

Space activity facilitates the smooth operation of the international economic and political system. Space-based telecommunications, global positioning, navigation, timing and remote sensing increase the frequency, speed, and reliability of cross-border transactions and contribute to a variety of economic, civic, and scientific endeavors.[1] In other words, space capabilities serve as a global "utility" that facilitates other activities. Signals from the Global Positioning Satellite (GPS) system not only help users navigate the surface of the planet, but they also can help to precisely time financial transactions around the world. Publicly available data from a network of government and privately owned remote sensing satellites is routinely utilized in land-use planning, monitoring, and disaster assessment. Spacecraft identify flood plains, track ocean circulation patterns, monitor volcanic events and earthquakes, assist in the identification of mineral resources, and guide farmers in the precise application of pesticides.

The economic value of commercial space activity is estimated to be several hundred billion dollars. The exact figure is difficult to assess in part because of globalization and in part because many space activities have indirect economic effects that are not well understood. The Space Foundation simplifies the problem by counting only the value of direct space activities, i.e., those commercial activities that derive the bulk of their value from their space components. Globally, these include infrastructure (81.97 billion dollars), infrastructure support industries (1.14 billion dollars), commercial satellite services (91.0 billion dollars), and commercial transportation services (40 million dollars).[2]

The indirect value of space is even more challenging to quantify.[3] Government-owned satellites (such as GPS) are utilized for commercial and civil activities worldwide, including financial-transaction timing, air, surface, and sea traffic management, construction-site surveying, agriculture, search and rescue, environmental management, scientific research, public safety and emergency management, and even recreation.[4]

The importance of science in national space activities is often overlooked. Yet, advances in science developed in space can change humanity's understanding of its place in the cosmos by revealing the nature of life in the universe and the kinds of life that may exist beyond Earth.[5] Scientific inquiry in space has often been an international pursuit—for example, NASA's 10 earth science missions currently in orbit involve partnerships with 14 countries.[6] Similarly, the 2002 World Summit on Sustainable Development called for the establishment of a monitoring initiative and led to the creation of the Group on Earth Observations (GEO) in 2005. The GEO coordinates the work of researchers from 79 governments, the European Commission, and 56 intergovernmental, international and regional organizations to build a virtual Global Earth Observation System of Systems (GEOSS).[7]

Table 1

U.S. GOVERNMENT SPACE SPENDING, 2008[8]	
AGENCY	AMOUNT (BILLIONS OF DOLLARS)
Department of Defense	25.95
National Reconnaissance Office	10.0
National Geospatial-Intelligence Agency	3.0
Missile Defense Agency	8.9
National Aeronautics and Space Administration	17.31
National Oceanic and Atmospheric Administration	0.95
Department of Energy	0.03
Federal Aviation Administration	0.01
National Science Foundation	0.48
Total	**66.63**

THE DISTRIBUTION OF SPACE CAPABILITIES

The United States is the world's leader in space, in civilian and government uses. The U.S. Government is the most active customer for space in the United States, and has the largest budget for it (Table 1).

The United States is also the world's leader in civilian space infrastructure and capabilities. In 2007, U.S. satellite manufacturers held contracts to produce 50 percent of commercial geosynchronous communications satellites on back-order, and the United States was scheduled to conduct 36 percent of back-ordered space launches for the world.[9] Of 21 new orders for geosynchronous communications satellites placed in 2008, U.S. manufacturers received 11 orders, followed by the Europeans with seven, and the Russians, Chinese and Japanese each won one order.[10]

Although the cost of designing, building, launching and maintaining satellites can be prohibitive, space is a global common, with several countries regularly accessing and using it (Table 2). Much of this activity is dominated by the major space powers: the United States, Russia, members of the European Space Agency (ESA), Japan, Ukraine, and China. Other countries have eschewed the development of a completely independent space system and instead partner with other states and focus on filling niche roles.[11] Canada's space agency, for example, usually conducts its science and exploration activities in partnership with NASA or the ESA. Many developing countries use space as a tool to address basic domestic issues. Indonesia, for example, has purchased foreign satellites in order to link its islands into a single communications network. Most other developing

Table 2

SUMMARY SAMPLE OF SPACE CAPABILITIES [12]

COUNTRY	LAUNCH	REMOTE SENSING	COMMUNICATIONS	SCIENCE/ ROBOTICS
Argentina		Yes	Yes	
Brazil	Developing	Yes	Yes	
Canada		Yes	Yes	Yes
China (PRC)	Yes	Yes	Yes	Yes
Egypt			Yes	
European Space Agency (1)	Yes	Yes	Yes	Yes
India	Yes	Yes	Yes	Yes
Indonesia			Yes	
Iran	Yes	Yes	Yes	
Israel	Yes	Yes	Yes	
Japan	Yes	Yes	Yes	
Kazakhstan (2)	Facilities		Failed	
Malaysia			Yes	
Mexico			Yes	
Nigeria			Failed	
North Korea	Developing	Developing		
Pakistan			Yes	
Philippines			Yes	
Russia	Yes	Yes	Yes	Yes
Singapore			Yes	
South Korea	Developing		Yes	Developing
Turkey			Yes	
Thailand			Yes	
Ukraine	Yes	Yes	Yes	
United States	Yes	Yes	Yes	Yes
Venezuela			Yes	
Vietnam			Yes	

*This table is not intended to be comprehensive.

(1) Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom are members. Canada, Hungary, Romania, Poland, Estonia, Slovenia, and Latvia each have cooperation agreements. Many of these countries have significant capabilities of their own. For example, France is a well-rounded space power, while Canada, Great Britain, and Germany have carved out capability niches.

(2) Russia now conducts space launches from facilities in Kazakh territory originally developed by the USSR. Kazakhstan does not have an indigenous space launch vehicle.

nations are content to "rent" space-based services such as weather imagery, remote sensing data, communications links, and positioning and timing data.

States, of course, are not the only actors capable of using space to their benefit. Private corporations, international nonprofits, international governmental organizations, and even individuals can, and do, use space for their own reasons. To the degree that they can acquire space capabilities through indigenous development, foreign acquisition, or even the leasing of foreign-flag space capabilities, any actor today has a modicum of potential space power.

Space Power

As a global common, space is a medium used by states for military activities and is a tremendous force multiplier. The U.S. Joint Chiefs of Staff define "space power" as "the total strength of a nation's capabilities to conduct and influence activities to, in, through, and from space to achieve its objectives."[13] Such a comprehensive definition includes physical assets (e.g., launch facilities, launch vehicles, satellites, command and control nodes, and communications links) as well as unquantifiable attributes, such as strong institutions and organizations, well-trained personnel, doctrine, knowledge, and experience.

Militarily, space provides the "strategic high ground" from which global communications and remote sensing can be quickly transmitted to militaries around the world. A military that can effectively use space has a tremendous advantage in terms of speed of communications, breadth of surveillance and intelligence, and accuracy of positioning and timing. Put in military terms, the space commons offers distinct and significant advantages in command, control, communications, intelligence, surveillance, and reconnaissance (C3ISR), maneuverability, and firepower. As the United States has been the world's leading innovator in the use of space for military purposes, this development is largely a story of American innovation.

> *A military that can effectively use space has a tremendous advantage in terms of speed of communications, breadth of surveillance and intelligence, and accuracy of positioning and timing.*

C3ISR

Space had an early impact on C3ISR capabilities, where its potential was first and most fully realized. The Cold War forced the American and Soviet militaries to develop the ability to support forces that may be operating around the globe. Line-of-sight communications limited the ability of national command authorities to control their military forces using terrestrial links. Space offered a natural solution: the higher the elevation, the broader the field of view. Thus, space became the new "high ground."

Today, advanced militaries are largely dependent on satellites for long-distance communications. Satellites offer reasonably reliable wireless connectivity and long-range mobile links that can be established in remote areas more quickly than terrestrial wire can be strung. One U.S. Army officer noted that 500,000 troops were able to communicate at a rate of 100 Megabytes per second (MBps) in 1990-1991 during Operation Desert Storm/Shield, compared to the smaller force of 235,000 troops connected at 2,400 MBps in the early days of Operation Iraqi Freedom in 2003.[14] This advance in technology is likely to continue. One Air Force officer predicts that the Defense Department's demand for worldwide satellite communications will jump from 13.6 Gigabytes per second (GBps) in 2006 to 160 Gbps by 2015, considerably more than existing military satellite communications systems can provide.[15]

The story is much the same in intelligence, surveillance and reconnaissance (ISR). Spacecraft watch the planet for a variety of national security purposes, ranging from detailed intelligence collection to detection of ballistic missile launches to real-time support of war operations. The United States regularly uses space ISR assets for targeting and battle-damage assessment. In Operation Iraqi Freedom, the American military has deployed space professionals at the Corps and Division levels to help integrate space capabilities with daily operations, giving forces on the ground the ability to more rapidly and fully exploit national space assets at the operational and tactical levels of war.[16]

MANEUVER

Space assets help military commanders plan for operations and maneuvers to a far greater degree of specificity and confidence. In Operation Desert Storm (1991), for example, remote sensing spacecraft aided coalition forces in developing useful maps and assessing desert terrain well west of the Saudi Arabian-Kuwaiti border, helping to determine whether conditions would support the movement of heavy armor and support vehicles. By creating maps, aiding navigation, and enhancing communications over vast territory, space played a significant part in moving the famous "left hook" from concept to reality.[17]

Today, GPS signals offer military commanders and war fighters an unprecedented level of accurate information on the location of friendly and hostile forces. In Operation Iraqi Freedom, space systems were integrated with maneuver elements in a system known as Blue Force Tracker, which vastly improved a commander's situational awareness about his own forces, enabling more rapid maneuvers.

FIREPOWER

Space assets are critical to the increased precision that has created a veritable revolution in firepower. Accurate knowledge of one's location — and, preferably, that of the target — has long been critical to a weapon's lethality. Following Operation Desert Storm, the Department of Defense developed low-cost kits for turning "dumb" bombs into "smart" bombs by equipping them with GPS capabilities to engage targets more precisely. Strike platforms became increasingly able to attack multiple targets in missions that had once taken multiple platforms and/or sorties. Former Secretary of the Air Force Michael Wynne explained, "In World War II, it took 1,500 B-17s dropping 9,000 bombs to destroy a given target. Today, on B-2 can strike and destroy 80 different targets on a single mission using weapons guided by space-based USAF global positioning system (GPS) signals."[18]

THE DISTRIBUTION OF MILITARY SPACE POWER

It is useful to summarize the capabilities of the major powers in space: the United States, China, Europe, Japan and India. Each has systems and interests that affect their positions in the global space commons.

The United States possesses advanced space capabilities far beyond those of other states and has integrated them into its war fighting capabilities more thoroughly and successfully than any other country. Space systems serve as a global infrastructure upon which deployed American military forces rely for critical functions. Unlike comparable terrestrial capabilities, space does not add significantly to the logistics trail of the deployed force, nor does it require foreign basing support, access agreements or overflight rights.

The United States possesses four space launch facilities on the coasts (Cape Canaveral and Wallops Island in the east and Vandenberg and Kodiak Island in the west). It boasts the Atlas and Delta families of large launch vehicles, plus

The International Space Station (ISS) is backdropped over Miami, Florida, in this 35mm frame photographed by STS-108 Commander DomInic Gorie aboard the Space Shuttle Endeavour.

(NASA)

vehicles capable of launching smaller spacecraft (Minotaur, Pegasus and Taurus). The United States also hosts innovative private-sector developments, most notably Space Exploration Technologies Corp.'s Falcon family of launch vehicles and Scaled Composites' ongoing work in suborbital spacecraft. The U.S. government operates several constellations of satellites, creating a robust global network of communications, remote sensing, positioning, navigation and timing capabilities, all of which are augmented by a comparably robust commercial sector possessing its own capabilities in communications and remote sensing. The U.S. Air Force and NASA both routinely conduct operations in space and manage contractors capable of designing, developing, and deploying space systems. The government space edifice is supported by a depth of contractor capabilities, personnel, and experience that is unmatched.

China is developing robust capabilities to operate in space and deny its adversaries the use of space during a time of crisis or conflict. After close analysis of U.S. and coalition war fighting practices, Chinese strategists identified space as central to enabling modern warfare, and have integrated space as a component of their campaign plans.[19] China has deployed multiple satellites to assist in reconnaissance, navigation and timing, and communications.[20] China has plans for a robust manned space program that would eventually land Chinese *taikonauts* on the moon. Moreover, China is developing multiple types of anti-satellite (ASAT) weapons, including jammers and direct-ascent missiles, such as the SC-17 tested in January 2007.[21]

The European Union adopted a multilateral approach in 2008 with a cooperative agreement among the European Commission, the ESA, and the European Defence Agency (EDA) to develop space technologies useful for national security, particularly in the area of space situational awareness and data relays, and possibly for military use of the burgeoning Galileo timing and navigation system. Member states, especially the United Kingdom and France, maintain robust space infrastructures that contribute to an impressive European space capability.

Japan in 2007 adopted a law that allows for the use of space for military purposes and emphasizes the need for commercial development in space. Japan maintains a robust civilian space capability with the ability to design and build satellites and rockets. Currently, Japan plans to develop additional remote-sensing satellites and launch missions to the moon.

India recently announced a greater interest in the military use of space and established a tri-service space cell in partnership with the Indian Space Research Organization.[22] India's indigenous space infrastructure is rather robust, with capabilities to design and build satellites and several advanced launch vehicles. India also plans to develop a manned space program over the long term.

"For All Mankind": Governance and Norms

Despite the international community's robust utilization of the space commons, governance of it is remarkably limited and out of date. The 1967 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies,* more commonly referred to as the Outer Space Treaty, declares, "The exploration and use of outer space, including the moon and other celestial bodies, shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and shall be the province of all mankind."[23] The signatories pledged not to station nuclear weapons or other weapons of mass destruction in space or on celestial bodies and accepted an intellectual framework recognizing space as a global common—an area that all countries may explore and exploit equally.[24]

With a legal foundation that is over 40 years old, space is in desperate need of a framework that reflects the role space plays in today's international system.

The United States led the way in promoting this principle. A decade before the Treaty, the United States consciously separated its civilian and national security space activities, explicitly giving NASA a peaceful mission.[25] When Neil Armstrong stepped from the lunar lander in 1969, he made a "giant leap for mankind," and when Gene Cernan became the last man to step off the surface of the moon in 1972, he remarked, "We leave as we came, and God willing, as we shall return, with peace and hope for all mankind."[26]

The United States strongly promoted the principle of "freedom of space," largely to secure the ability of U.S. reconnaissance satellites to overfly the Soviet Union. In doing so, it established the right for others to use space in such a manner.[27] More specifically, a decision memo forwarded to the president in 1955 noted, "A small scientific satellite will provide a test of the principle of 'Freedom of Space.' … Preliminary studies indicate that there is no obstacle under international law to the launching of such a satellite."[28] Despite having satellite programs of their own, the Soviets objected to the principle, charging that the United States was developing satellites for the purposes of spying, which they further argued signified America's intent to militarize space.[i]

Yet Soviet opposition to the freedom of space fell by the wayside as Moscow increasingly saw the benefit of launching Soviet satellites over American territory. By the time of the Outer Space Treaty, the Soviets had largely given up their objections. In 1972, the superpowers further enshrined the principle of noninterference with reconnaissance satellites in Article V of the Strategic Arms Limitation Treaty (SALT I) and Article XII of the Anti-Ballistic Missile (ABM) Treaty. Of course, the obligation only applied to the superpowers, but agreement between the two major space powers confirmed the creation of a meaningful international norm restricting the right of states to interfere with one another's peaceful use of space.

Nominally, international agreements continued to assert the principle of noninterference, largely

[i] These accusations turned out to be accurate, though they could have equally applied to the USSR.

in conjunction with technological developments. In 1979, several states signed the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (the Moon Treaty), which reasserted that the moon was the "province of all mankind, irrespective of their degree of economic or scientific development." It should be noted, however, that only a handful of states signed or ratified the treaty and none of them could be considered space powers. In 1982, signatories to the International Telecommunication Convention agreed to an update that governed the allocation of orbital slots for geosynchronous communications satellites and prohibited interference with non-military communications. Then, in 1986, the UN General Assembly adopted principles on remote sensing, which reaffirmed the right to collect imagery from space.[29]

MODERNIZING GOVERNANCE OF SPACE

With a legal foundation that is over 40 years old, space is in desperate need of a framework that reflects the role space plays in today's international system. To that end, several proposals have been made to update governance of the space commons. In general, these proposals focus on the regulation of ASAT weapons and the weaponization of space.

Some have argued that the United States should pursue an updated governance model built around a treaty on the Prevention of an Arms Race in Outer Space (PAROS).[30] In 2002, Russia and China jointly proposed such a treaty at the UN Conference on Disarmament. Article III of the draft text proposed obligating signatories "not to place in orbit around the Earth any objects carrying any kinds of weapons, not to install such weapons on celestial bodies, or not to station such weapons in outer space in any other manner," and "not to resort to the threat or use of force against outer space objects."[31] The proposal bans space-based systems but leaves signatories free to develop ground-based systems useful for attacking space-based elements. Both the Soviet Union and China have tested such ground-based systems. The draft treaty would further obligate parties to commit to benign intentions, which are neither verifiable nor enforceable.

Under their text, Russia and China would be free to continue developing—and deploying—counterspace systems capable of depriving the United States its space-derived conventional military capabilities. The text would not prevent war in space, and it would not reduce the threat posed to American space capabilities. In fact, the threat would continue to grow as potential adversaries continued to improve their terrestrially-based counterspace capabilities, even while promising not to use them. If Russia and China were truly concerned about space warfare, their proposals would likely extend to all weapons systems, whether based on sea, in air, on land or in space. Instead, they sought diplomatic constraints on potential U.S. strengths—space-based systems—while preserving their own capabilities to engage in space warfare.

Another proposal, from University of Maryland political scientists Nancy Gallagher and John Steinbruner, recommends upping the ante by proposing negotiations on a PAROS-like treaty that prohibits interference with space assets, including prohibitions on preparation for interference and a "robust" verification, monitoring, and inspection regime. They acknowledge that relying on nationally-controlled assets for verification, monitoring, and inspection would be inadequate. Instead, they suggest a combination of direct inspections, declarations of payloads, and a multilateral space surveillance capability. Unfortunately, they fail to acknowledge what an intelligence coup such an approach would be for other states seeking to close the gap between their space capabilities and those of the United States, how such a regimen might be used to more effectively target and attack U.S satellites, or how such a system might undermine the commercial uses of space. The proposed regulations would not prevent other space powers from maneuvering ostensibly peaceful satellites against military platforms simply by issuing new commands to platforms in orbit, or quickly and covertly giving peaceful high-power satellite transmitters extensive jamming capabilities. Therefore, there is still no reason to expect that such a treaty would adequately protect U.S. space assets or the openness of the space commons more generally.[33]

The U.S. military's reliance on space capabilities creates a unique and highly attractive vulnerability that any power contemplating conflict with the United States would be foolish to ignore.

A significant challenge for policymakers is that a legal framework that does not correspond to the distribution of power in the international system will always be under stress, in part because interests in such a regime are not aligned. To the degree that such a treaty levels the playing field, states that have invested substantial resources in space capabilities will be reluctant to sign. Indeed, the regime offered by Gallagher and Steinbruner would largely require the United States to reduce its relative advantages and increase its vulnerabilities in space, costing the United States lives and treasure in the event of a conflict with another space power. However, states that find themselves at a disadvantage in terms of space power are likely to seek a treaty that restrains more powerful states and creates a strategic opportunity to level the playing field and catch up. Thus, from the standpoint of U.S. interests, advocates of a PAROS regime are left arguing that the costs of surrendering U.S. advantages in space in the near- to mid-term will be offset by the benefit of maintaining parity in the future. This is a difficult sell.

Vulnerabilities and Threats in the Space Commons

While nations have made remarkable use of the commercial and military value provided by use of the space commons, it is not as clear whether such an accomplishment should serve as a source of pride or fear. Such reliance can also be seen as a tremendous vulnerability. If the use of space-based assets were denied, the international economy would at least temporarily collapse. Similarly, the U.S. military's reliance on space capabilities creates a unique and highly attractive vulnerability that any power contemplating conflict with the United States would be foolish to ignore.

VULNERABILITIES IN A FRAGILE COMMONS

Space systems are extraordinarily fragile. Satellites are vulnerable to kinetic and directed energy attacks. Even modest damage to subsystems, such as optics or solar arrays, may be functionally catastrophic to an entire satellite. In general, physical damage to space elements cannot be repaired and usually proves fatal, while even software failures can quickly become terminal because the margins for error aboard a spacecraft are so small. Communications links and ground-based command and control elements are also vulnerable and may be easier targets for a potential adversary. While it is possible to attack each space system, or its elements, individually, their location in orbit may also make them vulnerable as a class to a single strike that degrades or destroys multiple platforms. The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack noted that satellites in Low-Earth Orbit might be particularly susceptible to a nuclear-weapons-generated EMP attack that significantly increases radiation levels in the Earth's natural radiation belts.[34]

To make matters worse, the infrastructure that develops, launches, maintains, and operates spacecraft is similarly fragile and has multiple chokepoints. The United States possesses four launch sites, but only two are meant to handle large launch vehicles. Each has a limited number of launch pads and both are situated along coastlines that could be difficult to protect against a capable and well-resourced adversary. Some functions depend on civilian infrastructure which may itself be vulnerable to attacks, such as an effort to cripple power or transportation networks through cyberspace. In addition, the United States does not stockpile launch vehicles or significant numbers of spare satellites, nor does it develop systems with an eye towards surging new space assets in times of crisis.[35] Consequently, once degraded, American space capabilities would likely undergo a long and torturous reconstitution process that could prove impossible in the midst of an ongoing conflict in space with an adversary that had successfully seized the "high ground."

Taken together, these vulnerabilities make space an Achilles' heel for the United States and the international community. By successfully attacking and degrading U.S. space capabilities, an adversary could quickly eliminate the force-multiplying effects that boost the U.S. military, as well as threaten those critical infrastructures that rely upon space to function, presumably with highly adverse economic consequences.[36]

EMERGING ASAT CAPABILITIES

Several states appear to be developing capabilities to attack systems in space and deny the use of the space commons to potential adversaries. The U.S. Director of National Intelligence (DNI) recently noted in his annual report to Congress, "Potential foreign adversaries are aware of the increasing U.S. reliance on space systems and the advantages these systems provide to U.S. military and intelligence operations. Over the last decade, the rest of the world has made significant progress in developing counter-space capabilities."[37] The DNI offered no additional details in his unclassified testimony, directing Congress instead to classified material.

Typically, the purposes of an attack on space capabilities might be classified in several ways:

- Deception: manipulate, distort or falsify information.
- Disruption: temporary impairment of utility.
- Denial: temporary elimination of utility.
- Degradation: permanent impairment of utility.
- Destruction: permanent elimination of utility.

To accomplish these objectives, states may utilize the following means:[38]

- Attacks on or sabotage of ground segments.
- Attacks on space segments using a non-directed nuclear attack, such as the electromagnetic pulse generated by a nuclear detonation.
- A kinetic interception, which may involve space "mines" placed in similar orbits long before an attack and then maneuvered against a satellite, or a direct ascent attack combining launch and interception in a single act.
- Ground-based stand-off weapons, such as directed energy weapons, radio-frequency weapons, and particle beams.

Several states have well-developed counterspace capabilities, though the specifics of their capabilities remain shrouded in secrecy.

Russia has a high degree of space power, most of which it inherited from the Soviet Union.[39] Russia reportedly provided GPS jammers to Iraq that were used against the United States in 2003.[40] During the Cold War, the Soviet Union possessed co-orbital anti-satellite capabilities, which Russia presumably inherited.

China's counterspace capabilities and intentions are among the most frequently discussed by those concerned about U.S. national security vulnerabilities. China is a rising space power possessing extensive launch, communications, remote sensing, positioning, navigation, and timing capabilities.[41] Chinese military academics and professionals are clearly aware of America's advantages in space and the asymmetric vulnerabilities they provide.[42] Although U.S. officials confirmed in 2006 that China had "painted" a U.S. satellite with a laser, Western observers continued to debate the seriousness of China's interest in anti-satellite capabilities.[43] However, China's successful demonstration of a kinetic anti-satellite weapon in January 2007 confirmed that the interest was more than just "talk" among Chinese academics.[44] Gen. James E. Cartwright, then Commander of U.S. Strategic Command, testified to the Senate Armed Services Committee in 2007 that the Chinese "have undertaken what we would call a very disciplined and comprehensive continuum of capability against space—our space capabilities."[45]

Several actors have utilized jammers and cyber weapons to target satellites. Indonesia jammed a Chinese-owned satellite. Iran and Turkey both jammed satellite broadcasts of national dissidents.[46] In 2003, Iranians jammed satellite broadcasts of the Voice of America, and in March of that year Iraq jammed receipt of GPS signals. Libya has also frequently jammed mobile satellite communications links.[47] During summer 2003, Iran and Cuba reportedly colluded to jam broadcasts of Telstar 12, a satellite above the Atlantic that the Voice of America used to carry Persian-language programming.[48] In 1999, hackers even attacked a British satellite via cyberspace. In 2008, Brazilian hackers were arrested for using homemade communications dishes to "hijack" transponders on a U.S. Navy satellite.[49] In short, if threats are interpreted as a function of both intent and capability, multiple state and non-state actors have demonstrated ample intentions and capabilities to attack space systems. Thus, the United States and the global community face a wide range of threats to the space commons.

China's space mission.

U.S. Interests in Space

The United States requires the ability to militarily defend the freedom of space. Contemporary debates over American strategies in space tend to revolve around the issue of "space weapons," i.e., whether the United States should develop and deploy such weapons to enhance its national security. Yet, a single-minded focus on the preservation of U.S. military capabilities in space is insufficient; the United States must act to prevent kinetic strikes in orbit that create space debris. Moving past a debate over space weaponization and approaching space security as a "global commons" suggests a multi-pronged approach. It should be designed to preserve American freedom of action in space; offer new insights on how policymakers might move U.S. policy, strategy, and security programs out of stasis; and make substantive improvements that enhance U.S. national security.

PRESERVING U.S. FREEDOM OF ACTION

Since the 1950s, the United States has consistently supported the benign use of space by all countries. In 1996, the Clinton administration released its

National Space Policy, which reaffirmed a commitment to the exploration and use of outer space "by all nations for peaceful purposes and for the benefit of all humanity." It further determined that peaceful purposes included "defense and intelligence related activities in pursuit of national security and other goals."[50] Drafted at a time when a growing number of states were developing and deploying dual-use space systems, the Clinton administration went on to note, "National security space activities shall contribute to U.S. national security by … assuring that hostile forces cannot prevent our own use of space [and] countering, if necessary, space systems and services used for hostile purposes."[51]

The same year, the U.S. Space Command released "Vision for 2020," a planning document intended to guide the command's evolution and approach to future missions. The document more explicitly recognizes the range of space capabilities and predicts their use for national security purposes by other states. As a result, Space Command adopted a vision with two overriding themes: "dominating the space medium and integrating space power throughout military operations."[52] With that in mind, the Command adopted four operational concepts:

- **Control of Space:** The ability to assure access to space, freedom of operations within the space medium, and an ability to deny others the use of space, if required.
- **Global Engagement:** the application of precision force from, to, and through space.
- **Full Force Integration:** The integration of space forces and space-derived information with land, sea, and air forces and their information.
- **Global Partnerships:** Augments military space capabilities through the leveraging of civil, commercial, and international space systems.

This approach was mostly affirmed in the 2006 National Space Policy released by the George W. Bush administration. It reinforced an American commitment to the "exploration and use of outer space by all nations for peaceful purposes, and for the benefit of all humanity," rejected claims of national sovereignty, and reaffirmed the "rights of passage through and operations in space without interference." On the issue of space control, it was quite clear, asserting:

> The United States considers space capabilities—including the ground and space segments and supporting links—vital to its national interests. Consistent with this policy, the United States will: preserve its rights, capabilities, and freedom of action in space; dissuade or deter others from either impeding those rights or developing the capabilities intended to do so; take those actions necessary to protect its space capabilities; respond to interference; and deny, if necessary, adversaries the use of space capabilities hostile to U.S. national interests.[53]

Since the release of the 1996 National Space Policy and Vision 2020, the Department of Defense significantly improved its capabilities to undertake activities in all four operational areas noted in the Space Command's vision document. The Evolved Expendable Launch Vehicle program has created new launch capabilities to improve space access. As previously discussed, the Department also took the initial steps to exploit space for improved C3ISR, maneuverability, and firepower, demonstrating progress in global engagement and full force integration. Additionally, the Department and the intelligence community launched a series of ambitious programs to improve intelligence collection and communications. Finally, the Department successfully pursued a range of global partnerships with commercial firms, most notably in the communications and emerging remote-sensing industries.

However, for all the talk of "space control" a realistic analysis of the realities of international space power quickly demonstrates that the notion of establishing "control" of space is chimerical at best. Establishing command of space before a conflict is incompatible with existing international governance and the principle of the freedom of space that the United States has embraced since the beginning of the space age. Moreover, exercising space control in peacetime would likely be considered a hostile act by any number of space powers, including allies and friends of the United States. Lastly, the fragility of space-based systems and the threat of orbital debris would, in all likelihood, require the United States to engage in preemptive, if not preventive, war so as to deny an adversary the ability to threaten U.S. capabilities in space.

For all the talk of "space control" a realistic analysis of the realities of international space power quickly demonstrates that the notion of establishing "control" of space is chimerical at best.

Even a cursory review of the challenges of exercising and maintaining command of space suggest this may be more difficult than it sounds. Potential adversaries will always have at their disposal means of contesting such command. First, they can pursue programmatic means of deceiving, disrupting, denying, degrading or destroying U.S. space assets. Second, adversaries could utilize commercial communications satellites in order to tie their access to the space commons with that of the rest of the international community. Indeed, during the early days of Operation Enduring Freedom, al Qaeda made frequent use of Western satellite phones.[54]

Alternatively, an adversary could develop dominant capabilities that are employed only during conflicts, much in the way that U.S. forces only utilize their dominant capabilities in sea, air and land power when they are engaged in combat. Those capabilities, of course, need not be space-based, as the Russians and Chinese clearly recognize in their proposed texts on space weapons. Arguably, the United States currently possesses ample capabilities to destroy terrestrially-based weapons used against space assets, provided it can find them and is willing to attack them.

Rather than adopting the phraseology "command of space" and the intellectual heritage it carries from naval theorists such as Alfred Thayer Mahan, the United States should acknowledge that space will be a contested commons. This shift in thinking is not unprecedented — theories of sea power have similarly emphasized both "command of the seas" and the recognition of the limitations of such an approach. "Control" of space may be limited to specific battlefields for brief periods of time and, even then, may well require escalatory steps that the United States is unwilling to take. Even in limited battle conditions, control is unlikely to be perfect. Potential adversaries will still find ways to use space to their benefit and to the detriment of the U.S. Lt. Commander John Klein helpfully points in the direction of Sir Julian Corbett, a British strategist writing at the turn of the last century. Klein sums up Corbett's views on commanding the sea as a relative advantage, not an absolute: "It does not mean that an enemy cannot act, only that it cannot seriously interfere with one's actions. The normal state of affairs, Corbett observes, is not a commanded sea but an anarchic one — that is, command of the sea is normally in dispute."[55]

If it is accepted that space will be a contested common, command of space has less to do with weaponization or combat, and more to do with an adversary's overall ability to deceive, disrupt, deny, degrade, or destroy U.S. space capabilities, and vice versa. It is necessary to protect U.S. space capabilities and create the capability to deny others from using space for hostile purposes. Yet "command" of space, in the classic sense of the term, is unrealistic.

Recommendations for U.S. Space Policy

Approaching space security from the perspective of preserving the openness of the space commons offers new avenues for space policy, doctrine, and programs to move forward. By emphasizing the importance of the space commons to the international system, U.S. space policy and strategy could encourage actors to align their interests with America's and to perceive their interests in space as consistent with continued U.S. leadership. Rather than surrendering its freedom to act, the United States should use its considerable power and leadership in space to build an international infrastructure of interests and behavior that maximizes the benefits of space for the greatest number of actors while preserving American freedom of action. Potential American actions in this vein can be divided into four broad categories: providing public goods, setting the international agenda, modernizing international governance, and adjusting American hard power.

PROVIDE PUBLIC GOODS

The United States can create a win-win situation by becoming the most reliable provider of public goods in space, and serving the interests of other space actors. This puts the United States in a dominant position—so long as it is prepared to bear the burdens of providing the public goods. The United States can build on its tradition of protecting the space commons by proactively and consciously seeking to meet global demand for goods and services and partnering with parties willing to contribute to the creation or maintenance of such a public good. Doing so will help reduce the incentives for others to act against the openness of the space commons.

It is necessary to protect U.S. space capabilities and create the capability to deny others from using space for hostile purposes. Yet "command" of space, in the classic sense of the term, is unrealistic.

Since the 1950s, the United States has been an extraordinarily good international steward of the space commons. Since the first launch of an American weather satellite, the Television and Infrared Observation System (TIROS) in 1960, the United States has routinely made space-derived weather data available to all. This act marked the inauguration of a policy of openness that continues to this day. By the 1970s, the United States had made LANDSAT data, a historical archive of remote-sensing data of the Earth, widely available at cost, creating a boon for remote sensing applications. The United States has also involved a range of countries in its scientific efforts. Maintaining and expanding these efforts will enlarge the number of actors who have a self-interest in the continued success of U.S. space systems.

GPS: The Global Positioning System is, perhaps, the best example of U.S. leadership in providing a space-derived public good. As mentioned earlier, the GPS signal is available worldwide to all users, free of charge. During the course of the past two-plus decades, since the United States decided to make GPS available, it has maintained and modernized the program, all the while progressively making more advanced services available to the world's people. GPS remains the gold standard against which global users measure other systems. Modernizing GPS to better serve the non-military needs of those global users can help it remain the global standard and make other positioning, navigation, and timing (PNT) systems commercially less attractive and financially less viable to finance ministries looking for budget savings. More often than not, initiatives to add such capabilities to GPS die on the vine over funding fights, and the Department of Defense is largely expected to cover the added costs of such modernization. Yet the budget process does not provide additional resources for such a task. It is time for civilian agencies to meet their responsibilities and provide the fiscal resources to support GPS as the national and international resource that it is.

Second, the United States can more aggressively develop GPS-related applications that serve the widest possible user community. For example, the Federal Aviation Administration's Next Generation Air Transportation Control System, which would shift from ground-based navigation and traffic control to satellite-based traffic management, has been in development for years. Accelerating development and roll-out of the system and providing support for its adoption overseas would help maintain GPS as the global standard, again, making other systems less attractive and reducing any potential return that their sponsors anticipate on their investments. As part of such a strategy, the United States may also want to consider greater support for the private development of GPS applications, which, ultimately, have driven global adoption of the system.

Third, the United States can pursue modernization of GPS with close allies that remain committed to it as a global standard. By engaging new partners and giving them a substantial role in the system, the United States can create a *de facto* alliance in which an attack on U.S. space systems constitutes an attack on those partners as well. Japan, which has an advanced aerospace industry and can contribute productively, would be a logical place to start.

Space Surveillance Network: Space surveillance is a critical capability for U.S. national security that is also crucial in avoiding accidental collisions. The existing Space Surveillance Network (SSN) tracks 19,000 objects in space as small as 10 centimeters across, including 1,300 active payloads and 7,500 pieces of debris.[56] With so many objects in orbit, traveling at such high speeds, collisions are quite common. Of course, they are not always catastrophic, but even a millimeter-sized piece of debris traveling about 10,000 miles per hour can cause the catastrophic loss of a spacecraft. Consequently, spacecraft are frequently maneuvered to avoid debris, burning up fuel and shortening their lifetimes. In 2008, for example, U.S. and French officials admitted moving spacecraft eight times just to avoid debris.[57] China's 2007 test of a kinetic anti-satellite weapon produced about 2,400 pieces of known debris and a 2009 collision between an Iridium communications satellite and a defunct Russian communications satellite produced more than 870 pieces of cataloged debris.[58] To make matters worse, collisions geometrically increase the amount of debris over time, as each collision produces multiple pieces that can then collide with other objects, creating more debris.

The SSN creates an opportunity to improve cooperation among space actors who all have an interest in avoiding collisions. The Department of Defense currently provides some tracking information to approved operators on a reimbursable basis.[59] In recent years, the Department sought greater public-private coordination in order to improve the utility of its space tracking capabilities and make those capabilities more useful for owners and operators of spacecraft.

However, the system has several flaws and much more can be done to address them. The SSN does not continually track every orbiting object or those below a certain size; it is not a "staring eye" that examining the population of objects in orbit. Instead, it tracks objects by taking frequent snapshots that are analyzed by a computer, which predicts the location of each object between snapshots and attempts to correlate the data sets. Moreover, it has coverage gaps. The Northern Hemisphere is monitored more readily than the Southern Hemisphere, higher orbits are more difficult to assess, and non-U.S. government spacecraft owners and operators can be reluctant to share data. Thus, observers do not have perfect situational awareness in the debris cloud, only a scientific model backed by empirical evidence.

Improving the system and its utility requires higher-quality data and modeling capabilities. Better sensors and more frequent sharing of information with the U.S. Air Force can help improve data. Modeling is largely a function of computing power, therefore including more actors can help advance modeling capabilities. Providing the Department of Defense with adequate resources to improve its data sets and crunch numbers will elevate both U.S. space situational awareness and the ability to support others seeking to protect their investments in space hardware. It may be necessary to consider new kinds of public-private relationships, particularly with foreign companies, that would allow the Department to make data more widely available and encourage other countries with some space surveillance capabilities to feed their data into the U.S. system. In particular, the United States should examine partnerships between its network and other data collection systems, most notably those operated by Japan, France, and the European Space Agency.

The United States should consider similar activities related to space weather, which routinely affects the operation of spacecraft and has been known to affect telecommunications and power lines on Earth. Currently, the U.S. Air Force and National Oceanic and Atmospheric Administration dedicate resources to monitoring space weather, while NASA operates several scientific spacecraft useful in studying space weather phenomena.

While greater overseas cooperation can benefit U.S. interests, it also carries risks. To the degree that improved space situational awareness becomes more publicly available, it may provide potential adversaries with greater information that can be used to target U.S. spacecraft. Similarly, it will give them insight into the information that the United States possesses about their space capabilities. Nevertheless, the benefits may outweigh the potential costs: The likelihood of future collisions can be reduced, and other space actors can become attuned to, and dependent upon, improved U.S. space situational awareness. In other words, a win-win scenario is within the realm of possibility.

SET THE GLOBAL SPACE AGENDA

The United States must set the agenda for globally beneficial space activity, such as scientific research, orbital maintenance and exploration. Doing so will affect decision-making in other countries. By itself, the United States will not likely be sufficient to dissuade others from threatening U.S. space capabilities. But it may affect their long-term conceptions regarding which space activities are legitimate, lead them to find greater value in peaceful activities, and increase their willingness to accept benign U.S. leadership in space.

In the 1950s and 1960s, space played a significant role in a Cold War competition of soft power, in which both sides' capabilities were seen as a sign of national strength and technological prowess. As the world's leading space power with a history of undertaking multilateral space projects, the United

States has the ability to set a global agenda in civil space activity. With that in mind, the United States should undertake space activities that appeal to others with an eye towards influencing their choices about program priorities and resource allocation. Quite simply, it serves U.S. national interests for other states to pursue non-threatening space activities, such as space-based research and exploration, as opposed to activities with greater potential military purposes. By offering opportunities for others to join the story of humanity's quest to expand its proverbial horizons, it may be possible to build coalitions of states who define their space interests in terms of following the U.S. lead.

The United States has already pursued this course of action, to demonstrable good effect. The process of turning the U.S. Space Station into the International Space Station, for example, began with a decision to seek multiple partners in 1984, and it continues to guide human spaceflight programs and decisions in the United States, Europe, and Japan a quarter-century later. The Bush administration did not, and the Obama administration has not yet, committed to the International Space Station beyond 2015, but America's partners have expressed a strong desire to continue the program through at least 2020. An expert panel has essentially endorsed that desire and such an outcome appears likely.[60] Thus, a single decision, backed by sustained programmatic, fiscal and management actions, will have affected programmatic, policy, and budget decisions of other countries for at least 36 years.

Fortunately, the United States has the opportunity to set a similar agenda, involving a larger number of countries, for an even longer period of time. In 2004, in the wake of the space shuttle Columbia accident, the Bush administration initiated the Vision for Space Exploration, which sought to "extend a human presence across our solar system." The initiative sought to complete the International Space Station and retire the space shuttle by 2010, build new space vehicles for human spaceflight, return to the moon by 2020, and, eventually, move on to Mars.[61] In 2005, NASA Administrator Michael Griffin argued, "Leadership in the world of the 21st century and beyond will go to the nation that seeks to fulfill the dreams of mankind. … What the United States gains from a robust, focused program of human and robotic space exploration is the opportunity to define the course along which this human imperative will carry us."[62]

The Bush administration explicitly sought international participation and NASA sponsored several multilateral conferences to establish guiding exploration principles and a process to coordinate the extension of human presence across the solar system. On behalf of their governments, 14 space agencies agreed to a global exploration strategy with four principles:

- Open and Inclusive (open to any agency with a vested interest in space exploration)
- Flexible and Evolutionary (to meet changing needs and circumstances)
- Effective (work to an agreed plan with deliverables useful to all stakeholders)
- Mutual Interest (meet the needs of all stakeholders)[63]

Those agencies then established the International Space Exploration Coordination Group (ISECG) "to provide a forum for space agencies to discuss their interests, objectives and plans in space exploration with the view to working collectively towards the further development and implementation of the entire scope of the Global Exploration Strategy."[64]

In short, by defining a multilateral future in space, the Bush administration created an opportunity to lead other nations down a path of peaceful and mutually beneficial space exploration. Foreign interest demonstrates that the United States still has the ability to set a global agenda in space programs.

Unfortunately, U.S. pursuit of its own agenda has been anemic. Unlike the Reagan and Clinton administrations, in which the president or vice president was personally involved in the diplomacy needed to set a multilateral agenda for the International Space Station, the Bush administration's senior political leaders largely bowed out. At the same time, the administration and Congress failed to adequately fund such an ambitious agenda. Those two actions signaled to others that the United States might not be committed to executing its own ambitious plans, eroding other countries' willingness to follow America's lead. As of this writing, the Obama administration and Congress are heading down the same path at a quicker pace, further reducing projected available resources for civil space programs in general, and exploration in particular.

Of course, leading a multinational effort involves risks. Unless carefully designed, it may lead to illicit technology transfers that could put United States space advantages at risk. Rather than redirecting space investments from military and into civil pursuits, it may lead states to increase their total investments in space capabilities and strengthen the domestic industrial base upon which their national security space programs rely. This may be a welcome development among close U.S. allies, but the same effect might occur among states whose relationship to the United States is more ambiguous. Finally, there is a risk of creating dependencies on foreign capabilities that may prove unacceptable to the United States over the long run. Many of these risks are manageable but should prompt careful forethought by policymakers concerned about, and attuned to, U.S. national security interests as well as mobilizing broad international space efforts.

Nevertheless, leading a multilateral space exploration program offers the potential for the United States to engage other powers in peaceful activities that help define their perceptions of the importance of space and appropriate space priorities. Patterns of peaceful behavior, regularized interaction and informal rules for cooperation have the potential to influence senior political leaders' views on space activity and prioritization of space spending. While such an "institutional" approach to space as a global common may not overcome power differences as a primary driver of international behavior, it can reinforce measures taken elsewhere to dissuade others from choosing a path of confrontation.

MODERNIZE INTERNATIONAL GOVERNANCE OF THE SPACE COMMONS

The United States can more aggressively build an international structure that enables space commerce to flourish, creating more private goods and services from which all may benefit, while increasing the risks to other parties of engaging in a space conflict. Building a framework of international rules can help moderate international behavior.[65]

The United States routinely engages in technical discussions and agreements meant to facilitate national and multilateral space activities and ensure that space actors minimize interference with one another. Discussions of space security tend to disregard such discussions as low politics. Interestingly, the fact that such discussions and agreements are low politics may make them useful for building coalitions disposed to appreciate and value U.S. space leadership. They may, in fact, help to build coalitions of actors ill-disposed toward those who threaten rules that the United States led efforts to build.

For over a century, the International Telecommunication Union (ITU) has coordinated efforts to set common standards and minimize interference among telecommunications systems.

Wireless communications, in particular, are vulnerable to inadvertent interference with one another's signals. Thus, some form of coordination has long been necessary. Every two or three years, the ITU hosts the World Radio Communications Conference (WRC), which reviews and revises radio communications rules and allocates communications satellite orbits/orbital slots. Even though tens of billions of dollars are at stake and competition among states is intensely political, WRC events rarely rise to the level of "high politics" as a matter of conflict between states, in part because ITU functions are perceived as technical. Yet, the ITU and WRC have been relatively successful in establishing rules that enable satellite communications to flourish. Without them, building the military, civil and commercial space communications capabilities upon which the United States relies would have been eminently more difficult.

The United States should consider diplomatic initiatives in two similar areas with an eye toward making it more difficult to develop counter-space capabilities. The growth of space debris and the threat it presents to all spacecraft has risen in importance on the international agenda. In 1980, only 10 countries operated spacecraft and the Air Force tracked 4,700 objects in space. By 2009, over 50 actors owned or operated spacecraft and the U.S. Space Surveillance Network was tracking about 19,000 objects in orbit, straining resources and creating problems for space operations.[66] Trends indicate that problems will continue to grow.[67] Concerns about debris led NASA to adopt and promulgate standards for debris creation in 1995. Other U.S. agencies adopted those standards in 2001, and the major space-faring countries followed suit in 2002.[68] U.S. leadership in this area heightened international interest and concern about debris, widening interest in the global consequences of China's 2007 ASAT test and contributing to the number of actors willing to condemn it.

Debris agreements are voluntary and largely unenforceable. Still, debris represents a classic "tragedy of the commons" problem in which strong leadership can make a difference. Nearly a half century ago, American economist Mancur Olson argued that small groups could cooperate to provide public goods when each member of the group benefited from doing so, even if the group was not comprehensive.[69] Fortunately, the number of countries launching spacecraft is considerably smaller than the number of countries that own them. The dominant space launch entities include the United States, Russia, China, ESA, Japan, and India. Israel and Iran have also conducted space launches, and North Korea has attempted them. By themselves, the six dominant space-launching countries could share information to reduce debris created by their launch vehicles and seek agreement to require that payload providers demonstrate that they meet certain debris standards before being accepted for launch. Doing so would emphasize the importance of debris mitigation—an area in which the United States leads—and, possibly, increase the diplomatic penalties for testing kinetic anti-satellite systems. To the degree such a regime were honored, it would improve the long-term operational environment for all space actors, whether civil, military, or commercial.

There are additional areas in which more technically-focused rule-making might contribute to a stable regime that supports space commerce and advances U.S. interests. These areas include liability for accidents, PNT coordination (given the continuing proliferation of such systems), scientific data standards (particularly in the area of Earth observation), information-sharing associated with space situational awareness, and proximity operations around foreign spacecraft. The seeds for these activities have already been planted.

Pursuing such agreements has risks. Agreements tied to commercial activities may lead to a cartel-like environment in which any single actor could advance its commercial interests by defecting from the rules and offering services at a lower cost. Similarly, negotiations to reach and monitor agreements could involve transfers of sensitive information, which some actors might use to improve their capabilities to the detriment of U.S. national security and commercial interests. Finally, other space actors could attempt to grow such negotiations into broader discussions of a PAROS-like treaty, shifting the focus from modest, but practical, technical goals into broader, political goals aimed at curtailing U.S. advantages. Avoiding such pitfalls would require close coordination and cooperation in the interagency process and a domestic strategic consensus about the purpose, and limitations, of these kinds of discussions.

Nevertheless, a diplomatic approach that placed a higher priority on rule-making would help advance U.S. interests by:

1. Enabling the United States to set the global space agenda.
2. More clearly defining what constitutes "good" and "bad" behavior in space.
3. Building coalitions of actors prepared to condemn bad behavior, such as intentional interference with one another's satellites, unnecessary debris creation, or intrusive maneuvers.
4. Reducing economic externalities imposed on the global commons by any single actor's disregard for the common interest.

ADJUST AMERICAN HARD POWER IN SPACE

Pursuing the three main courses of action identified so far may dissuade others from contesting U.S. space capabilities and even help define the environment in which such a contest takes place. However, they cannot, by themselves, determine the outcome of a conflict. At the end of day, U.S. space security still depends on the results of the contest between offense and defense. With that in mind, the United States must act quickly to improve its space security posture.

Multilateralism: The United States should integrate its space capabilities with those of other responsible space-faring nations with an interest in maintaining the openness of the space commons. The United States is not the only country that depends upon its space security for relative military advantage. For better, and worse, the United States and its allies have made great strides in recent years incorporating space into their conventional military capabilities. Multilateralism could expose American policymakers to programmatic opportunities to leverage the space capabilities of close allies, either as a substitute for low-priority U.S. space capabilities, an enhancement for existing capabilities, or a hedge against the loss of existing and planned U.S. capabilities. By incorporating allied capabilities into U.S. space architectures and encouraging those allies to contribute to the creation of U.S. capabilities, the United States can begin to more closely align their interests with its own in preserving U.S. leadership. Such integration has already occurred in programs such as the Joint Strike Fighter and, increasingly, ballistic missile defense. Military space should not be far behind.

Deterrence: Deterring attacks on space assets is a difficult task. Some in the United States assume that an attack on U.S. space capabilities, upon which the United States depends for its national security and economic vitality, would automatically result in retaliation. However, it is not at all clear that potential adversaries share this view. They may believe that destroying space assets may not automatically trigger a U.S response because an attack would not take place on the territory of the United States or its allies, or kill anyone.

Clarifying U.S. intentions may have been the objective of the Bush administration's 2006 National Space Policy, which asserted, "The United

States considers space capabilities — including the ground and space segments and supporting links — vital to its national interests."[70] Yet this statement falls far short of a definitive declaratory statement establishing clear red lines that should not be crossed. The Obama administration should ensure that, privately and publicly, statements on deterrence in space are clear and explicit.

In cases where diplomacy or sanctions fail, other means will be necessary.

Denial: U.S. space-based weapons remain the most controversial aspect of the U.S. space posture, even though the United States is not developing space-based weapons. Even preserving the option to develop space-based weapons at some future date is viewed as provocative. Nonetheless, as this paper has argued, the issue of space-based weapons is largely a distraction from the central issues of space security. The simple fact is that space warfare does not require space-based weapons. Indeed, such space-based systems play to American strengths, and not those of the United States' potential space adversaries, who may find it more technically and fiscally feasible to attack U.S. space capabilities, including ground segments and communications links, from the surface of the Earth. Consequently, banning space-based weapons would do little to secure American space capabilities while potentially precluding the development of capabilities that play to American technical strengths in space operations.

Setting aside the question of space-based weapons, it should be clear that the United States will require the ability to deny potential adversaries the use of space for hostile purposes during armed conflicts, just as the United States possesses the ability to deny adversaries the use of the sea or air at such times. Currently, the United States possesses a range of tools to seek such denial, or at least to contest an adversary's use of space sufficiently to minimize the threat.

Diplomacy and sanction can be effective tools to deny an adversary's ability to use space during a conflict. During the 1991 Persian Gulf War, the United States worked with other space-faring actors to deny Iraq use of certain space capabilities, including space-derived imagery available on the global market. With that in mind, the United States can seek to deprive potential adversaries of the benefits of space with sanctions and embargos, just as it seeks to restrict trade with adversaries during times of conflict. It will serve U.S. interests to ensure that commercially available space-derived services, such as imagery and communications, can be legitimately denied to potential adversaries when necessary.

In cases where diplomacy or sanctions fail, other means will be necessary. America's global conventional capabilities give it the ability to kinetically attack ground segments and communications links during an armed conflict. Satellite command and control networks tend to be large and easily identifiable. The large radio uplinks are fixed and difficult to hide. They may be more difficult to attack, however, to the degree that doing so requires one to penetrate a defended battlespace.

This naturally turns one's attention to attacking space elements. As discussed earlier, there are many ways to do so. Jamming may be the most common. Other forms of "soft kill," which disable or disrupt satellites only temporarily, include such tactics as interrupting the power supply. Alternatively, a spacecraft could be maneuvered into position between the target satellite and the sun, close enough to interfere with the satellite's solar cells and force it into "safe" mode, during which it is unlikely to perform its assigned functions. When appropriate, the shielding spacecraft can move away, enabling the target satellite to collect energy and its operators to restore its functions. A third option might be to penetrate the satellite's command and control link with enough fidelity to issue false commands, again causing the satellite to shut down or otherwise corrupt its operations.

When soft-kill options fail or are otherwise inappropriate, the United States may face the need to destroy a satellite kinetically. During the 1980s, it conducted successful tests of a direct-ascent anti-satellite weapon launched from an F-15. Although successful, the program was discontinued. In 2008, the United States reconfigured anti-ballistic missile systems aboard a naval vessel in order to destroy a malfunctioning spacecraft on its way to re-enter Earth's atmosphere. U.S. officials were quite clear that the intercept was undertaken as a special circumstance, though there is no reason to believe that the United States could not repeat the feat with greater margins for success as ballistic missile defense capabilities improve.[71] Thus, the United States has the technical wherewithal to develop, deploy and operate anti-satellite capabilities, but has, to date, not done so, making it dependent on other means of space control. The other means—sanctions, embargo, radio-frequency and kinetic attacks on communication links and ground elements—may be sufficient against states with limited space capability, for now. However, as capabilities proliferate, become more advanced, and involve a growing number of cross-border relationships, the utility of such tools is likely to decline. With that in mind, it serves U.S. interests to develop better means of denying hostile actors of space systems at their most vulnerable point: the space-based elements.

Recalling that control of space will be contested, and that the United States only requires such control during times of conflict, the United States need not pursue permanent solutions. Moreover, physics makes space a global battlefield. Filling orbital bands with debris, as China's 2007 ASAT test did, will have adverse global consequences long after a conflict ends. Therefore, the United States should focus its efforts on "soft kill" effects that persist only so long as the United States needs them to.

Defense: One of the least controversial space security issues concerns defensive measures. Unfortunately, they also tend to be among the most expensive aspects of space security and may require wholesale bureaucratic, cultural, and procurement changes.

On individual satellites, these alterations might include hardening against electromagnetic pulse, frequency-hopping transmitters and receivers to help defeat jamming, maneuverability against kinetic weapons, and stealth to complicate detection and targeting. Of course, all such measures are expensive and tend to decrease the mission-relevant aspects of a spacecraft. They add weight and cost. While military systems should place mission performance and survivability ahead of economic efficiency, the commercial systems upon which the United States increasingly relies have responsibilities to shareholders that preclude hardening their systems against a military aggressor. To address these shortfalls, the United States should consider options that improve the rates of return on investment, making it more financially attractive for commercial service providers to design for, and meet, government needs. Such options might include government guarantees of a revenue stream to a commercial provider to offset added demands on a commercial satellite. They might include outright financing of some commercial systems with low-cost loans or subsidies for launch and operating costs.

Policymakers should also more aggressively explore alternate space architecture options. Today, most space actors build satellites, launch them,

An alternative space architecture would explore the development and deployment of satellite systems that exploit the architectural advantages of networking, in which the loss of an individual spacecraft would be damaging, but the network as a whole could work around such losses.

and operate them in a relatively predictable manner as long as the satellites' life spans will allow. It has been financially efficient to do so, and the use of space has not been routinely contested. Because orbital slots are limited, launches are expensive, and procurement cycles are extraordinarily long, the tendency has been to pack as much performance into a spacecraft as possible. As a result, spacecraft are as vulnerable to bad actors as unarmed merchant ships have been to Somali pirates. Adding individual defensive capabilities reduces performance, thus there is a reluctance to transform spacecraft into the 21st century equivalent of a 16th or 17th century armed merchantman capable of taking modest care of itself.

An alternative space architecture would explore the development and deployment of satellite systems that exploit the architectural advantages of networking, in which the individual nodes on the network are not highly-advanced and expensive spacecraft, but the entire network performs more capably because of the larger number of nodes. In such an architecture, the loss of an individual spacecraft would be damaging, but the network as a whole could work around such losses.

Such an approach would be highly expensive and require the development of new technologies, but the Department of Defense has begun exploring it. In the 1980s, the Strategic Defense Initiative Organization considered such an approach for space-based missile interceptors. Known as Brilliant Pebbles, the concept sought to exploit advances in information technology, microelectronics, propulsion systems, principles of mass production, and sensor capabilities to build a fleet of small satellites that would collectively defeat ICBMs. The program died with the Cold War, but the architecture survived in the form of the Iridium satellite communications network.

More recently, the Defense Department experimented with improved communications and remote sensing capabilities and networking architectures. The Department, for example, initiated the IRIS program in partnership with Cisco to experiment with Internet routers in space, providing orbital routing capabilities, reducing the number of times a spacecraft must communicate with the ground in order to manage communications traffic, and beginning the process of building an "Internet" in orbit.[72] Other, less successful attempts include the Transformational Satellite Communications System (TSAT), and Future Imagery Architecture (FIA), both of which were canceled.

In addition to networking architectures, the Department should examine mechanisms for addressing infrastructure constraints. As mentioned earlier, the U.S. infrastructure for creating and launching spacecraft is not very responsive and has multiple chokepoints at which a determined adversary could seek to degrade U.S. space capabilities over time. Funding already-established programs, such as the Force Application and Launch from CONUS (FALCON) and the Operationally Responsive Space (ORS) Office, move the U.S. toward a space architecture that is more readily surged, modified on relatively short notice, flexible in the face of a changing environment, and more readily reconstituted in the face of sustained attack.[73] FALCON petered out because of a lack of funding, and ORS faces a struggle between those who want to use it to make better use of existing assets and those who want to use it to develop better capabilities. But these and programs like them reflect an awareness that the United States needs to be able to access space more quickly, with greater flexibility and responsiveness to quickly changing national security needs than existing space architectures generally allow.

Taking these capabilities to the next level and changing space power in the way that information technologies changed sea, air, and land power requires new technology and sustained funding. Pursuing this path, however, would have multiple benefits for U.S. space posture. First, such capabilities would improve deterrence in space by establishing in fact and perception that attacks on U.S. space systems will fail to achieve their objectives.[74] Second, they may reduce the need for offensive space warfare to the degree that protecting U.S. space advantages does not require attacks on an adversary's counter-space capabilities, which may be militarily and politically difficult in a variety of scenarios. Third, they increase operational flexibility and would accelerate integration of space capabilities into U.S. military capabilities, ultimately increasing the options available to U.S. commanders, the military effectiveness of U.S. forces, and, in the end, helping secure U.S. security interests while putting fewer U.S. personnel at risk.

Conclusion

America's space posture is at a turning point. The United States depends on its space capabilities to maintain its 21st century economy and relative military advantages around the planet. However, changes to antiquated space policy have stalled over debates about space weaponization that largely miss the point. Potential adversaries recognize the military benefits of space and American dependence upon it. As their capabilities to use space for military purposes improve, whether through the development of indigenous capabilities or the acquisition of space-related goods and services on the global marketplace, the potential for a space conflict increases. Quite simply, potential adversaries cannot afford to ignore the asymmetric advantages and vulnerabilities that space creates for the United States. They do not require space-based weapons in order to level the playing field.

U.S. policymakers must not remain stuck in a stale debate. Instead, they should develop a space strategy that reflects developments around the world. Such a strategy will take the full range of space capabilities into account, acknowledge the limitations of both a "command of space" and a governance approach to securing the space commons, and move forward more creatively on multiple diplomatic, political, commercial, and military fronts to enhance U.S. space security.

American policymakers can begin on this course by using U.S. leadership to dissuade others from challenging U.S. interests. To do this, they will need to demonstrate the benefit others derive from depending on U.S. space capabilities and supporting a U.S.-led civil space agenda. By refining rules that enable all parties to use space to their benefit, the United States can promote standards of "good stewardship" of a commons for all space actors. By integrating allies into its national security space capabilities, the United States will also build *de facto* alliances of space actors, helping ensure that any actor contemplating hostile acts against the United States must also consider the adverse consequences of those hostile acts on third parties. Finally, by focusing its space control efforts on “soft kill” capabilities and conducting a significantly stronger effort to build defensive capabilities, the United States may be able to deter attacks on space capabilities altogether and, failing that, ensure that attacks on its space systems do not result in a catastrophic space “Pearl Harbor” as feared by so many experts.

ENDNOTES

[1] See Ithiel de Sola Pool, *Technologies without Boundaries: On Telecommunications in a Global Age,* (Cambridge, MA: Harvard University Press, 1990).

[2] *The Space Report, 2009,* op. cit, 5.

[3] See the government's GPS website at http://www.gps.gov/index.html. (Accessed 27 August 2009).

[4] See the government's GPS website at http://www.gps.gov/index.html. (Accessed 27 August 2009).

[5] These questions drive the bulk of NASA's Science Mission Directorate's activities. http://nasascience.nasa.gov/about-us. (Accessed 10 August 2009).

[6] NASA, *FY2010 Budget Estimate, Earth Science*. Available at http://www.nasa.gov/pdf/345950main_3_Earth%20Science_FY_2010_UPDATED_final.pdf. Accessed (17 August 2009).

[7] http://earthobservations.org/index.html. (Accessed 18 August 2009).

[8] *The Space Report, 2009,* op. cit., 122.

[9] *Aerospace Facts & Figures, 56th edition,* op. cit., 74. It should be noted that the U.S. space launch industry largely exists to launch U.S. government payloads and is no longer the provider of first choice for truly commercial customers. While the United States may be "first among equals" in commercial space activities, the market share of its manufacturers has declined precipitously, generally attributed to U.S. reluctance to freely transfer advanced space technology across national borders and the continuing entry of other capable spacecraft manufacturers into a profitable market.

[10] Satellite Industry Association, *State of the Satellite Industry Report, June 2009,* http://www.sia.org/.

[11] For a brief overview of trends in the global space economy, see *The Space Report, 2009,* op. cit., and Richard Kaufman, Henry Hertzfeld, Jeffrey Lewis, *Space, Security and the Economy*, Economists for Peace and Security, (September 2008): 22-29.

[12] Sources include: *The Space Report, 2009,* op. cit., passim; Lt. Col. Robert D. Newberry, USAF, "Latin American Countries with Space Programs: Colleagues or Competitors?" *Air & Space Power Journal,* (Fall 2003). The James Martin Center for Nonproliferation Studies (CNS) at the Monterey Institute of International Studies also maintains a useful website summarizing some foreign capabilities at http://cns.miis.edu/pubs/missiles.htm. (Accessed 11 September 2009), as does the online space reference site, SpacePolicyOnline (http://www.spacepolicyonline.com/pages/). A more detailed and rigorous survey would likely find that each of these states possesses some ability to utilize remote sensing and communications applications and had participated in some form of space-related research, because anyone can purchase on the commercial market satellite phones and terminals and remote sensing data.

[13] Cited in Department of Defense, *Joint Publication 3-14*, Space Operations, (6 January 2009): GL-9.

[14] Patrick Rayermann, "Exploiting Commercial SATCOM: A Better Way," *Parameters*, (Winter 2003-2004): 55.

[15] Rory D. Welch, "Satellite Communications and the Future of American Expeditionary Warfare," *High Frontier: The Journal for Space and Missile Professionals*, Vol. 2, No. 1, 61.

[16] See, for a useful discussion, Lt Gen Gary L. North and Col John Riordan, "The Role of Space in Military Operations: Integrating and Synchronizing Space in Today's Fight," *High Frontier*, Vol. 4, No. 2, February 2008, pp. 3-6; Maj John Thomas and Maj Richard Operhall, "Space, the ACCE, and the Joint Fight," *High Frontier*, Vol. 4, No. 2, (February 2008): 29-33.

[17] See, for example, Sir Peter Anson and Dennis Cummings, "The First Space War: The Contribution of Satellites to the Gulf War," in Alan D. Campen, ed., *The First Information War*, (Fairfax, VA: AFCEA International Press, 1992): 121-135; James Winnefeld, Preston Niblack, and Dana Johnson, *A League of Airmen: U.S. Airpower in the Gulf War*, (Santa Monica, CA: RAND Corporation, 1994), pp. 200-203; Brig. Gen. Robert H. Scales, J.R., *Certain Victory: The U.S. Army in the Gulf War*, (Washington, DC: Brassey's, 1993): 160-164. To be sure, space assets did not provide definitive intelligence during Operation Desert Storm and were often found wanting by coalition commanders. Rather, Desert Storm hinted strongly at the potential of space for combatant commanders, helping drive more rapid integration in the 1990s.

[18] Michael Wynne, "Space: The Ultimate High Ground Creating Strategic and Tactical Conditions for Victory," *High Frontier*, Vol. 3, No. 4, (August 2007): 4.

[19] Department of Defense, *Annual Report to Congress: Military Power of the People's Republic of China*, (2009): 13, 52.

[20] Department of Defense, *Annual Report to Congress: Military Power of the People's Republic of China*, (2009): 26-27.

[21] Department of Defense, *Annual Report to Congress: Military Power of the People's Republic of China*, (2009): 27.

[22] *The Space Report*, op. cit., 112-114; Jessica Guiney, India's Space Ambitions: Headed Toward Space War? Center for Defense Information Policy Brief, (April 2008).

[23] Article I, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, (27 January 1967). Available at: http://www.state.gov/www/global/arms/treaties/space1.html#1. (Accessed August 4, 2009).

[24] John Hickman argues that this "res communis" approach, as opposed to a "terra nullius" approach that would have viewed space as unclaimed territory, has retarded the development and use of space by making it more difficult for any party to secure benefit from that party's development activities. He offers a fascinating argument, but one that remains outside the scope of this essay. See, John Hickman, "Still crazy after four decades: The case for withdrawing from the 1967 Outer Space Treaty," *The Space Review*, (24 September 2007). http://www.thespacereview.com/article/960/1. Accessed August 10 2009.

[25] The National Aeronautics and Space Act of 1958, Public Law 85-568, Section 102(a). http://www.nasa.gov/offices/ogc/about/space_act1.html. (Accessed August 4, 2009).

[26] See, Eugene Cernan with Don Davis, *The Last Man on the Moon,* (New York: St. Martin's Press, 1999): 337.

[27] Walter A. McDougall, . . .*the Heavens and the Earth: A Political History of the Space Age,* (New York: Basic Books, 1985): 118-121; Peter Hays, *United States Military Space: Into the Twenty-First Century,* INSS Occasional Paper 42, (Maxwell AFB, AL: Air University Press, September 2002): 64-65.

[28] *NSC 5520, Draft Statement of Policy on U.S. Scientific Satellite Program, General Considerations*, (20 May 1955), contained in Presidential Decisions: NSC Documents, (Washington, DC: George C. Marshall Institute, n.d.,): 10.

[29] See the website of the United Nations Office for Outer Space Affairs, which maintains a repository of major international space agreements. http://www.oosa.unvienna.org/oosa/index.html; Nancy Gallagher and John D. Steinbruner, *Reconsidering the Rules for Space Security,* (Cambridge, MA: American Academy of Arts and Sciences, 2008): 15.

[30] Helen Caldicott & Craig Eisendrath, *War in Heaven: The Arms Race in Outer Space,* (New York: The New Press, 2007): Chapter 5.

[31] Working Paper Presented By The Delegations Of China, The Russian Federation, Vietnam, Indonesia, Belarus, Zimbabwe And Syrian Arab Republic, United Nations Conference on Disarmament, CD/1679, (28 June 2002). http://www.unog.ch/80256EE600585943/(httpPages)/D4C4FE00A7302FB2C12575E4002DED85?OpenDocument. (Accessed 14 September 2009).

[32] Gallagher and Steinbruner, *Reconsidering the Rules for Space Security,* op. cit., 75-83.

[33] For a discussion of the challenges of monitoring and verifying such a treaty, see Paula DeSutter, *Is an Outer Space Arms Control Treaty Verifiable?,* (Washington, DC: George C. Marshall Institute, Roundtable on Science and Public Policy, March 2008.) DeSutter, then Assistant Secretary of State for Verification, Compliance, and Implementation, answered her own question in the negative.

[34] *Report of the Commission to Assess the Threat to the United Chapter from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures*, (April 2008): Chapter 10.

[35] The United States has demonstrated the ability to "surge" space capabilities into crisis areas by moving satellites already in orbit, which burns fuel and may shorten their life spans, possibly accelerating the launch of spacecraft already in the launch queue, and leasing increased capacity on commercial assets.

[36] *Report of the Commission to Assess United States National Security Space Management and Organization*, (11 January 2001): viii.

[37] J. Michael McConnell, *Annual Threat Assessment of the Intelligence Community for the House Permanent Select Committee on Intelligence*, (7 February 2008): 33.

[38] For an excellent survey of offensive counterspace capabilities, see, Tom Wilson, *Threats to United States Space Capabilities*, Background Paper Prepared for the Commission to Assess United States National Security Space Management and Organization. Available at: http://www.fas.org/spp/eprint/article05.html#8. (Accessed September 11, 2009).

[39] Pavel Podvig, "Russia and Military Uses of Space," in *Russian and Chinese Responses to U.S. Military Plans in Space,* (Cambridge, MA: American Academy of Arts and Sciences, 2008): 1-29.

[40] Maj Scott Weston, USAF, "Examining Space Warfare: Scenarios, Risks, and U.S. Policy Implications," *Air & Space Power Journal*, (Spring 2009).

[41] Kevin Pollpeter, *Building For The Future: China's Progress In Space Technology During The Tenth 5-Year Plan And The U.S. Response*, (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, March 2008).

[42] See, for example, Michael Pillsbury, *An Assessment Of China's Anti-Satellite And Space Warfare Programs, Policies And Doctrines*, Report Prepared for the U.S.-China Economic and Security Review Commission, (19 January 2007); Larry M. Wortzel, *China's Nuclear Forces: Operations, Training, Doctrine, Command, Control, and Campaign Planning*, (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, May 2007); Larry M. Wortzel, *The Chinese People's Liberation Army and Space Warfare*, (Washington, DC: American Enterprise Institute, n.d.); Department of Defense, *Annual Report to Congress: Military Power of the People's Republic of China*, (2009): 13-14.

[43] Reuters, "China jamming test sparks U.S. satellite concerns," *USA Today*, (5 October 2006). http://www.usatoday.com/tech/news/2006-10-05-satellite-laser_x.htm. (Accessed September 6, 2009).

[44] For general discussions of China's ASAT test, see: Ian Easton, "The Great Game in Space," (Washington, DC: Project 2049 Institute, n.d.); Phillip C. Saunders and Charles D. Lutes, "China's ASAT Test: Motivations and Implications," *Joint Forces Quarterly*, Issue 46, (3rd Quarter 2007): 39-45; and, Ashley Tellis, "China's Military Space Strategy," *Survival*, (September 2007).

[45] Transcript of the testimony of Gen James E. Cartwright, Commander, U.S. Strategic Command, before the Strategic Forces Subcommittee of the Senate Armed Services Committee, Russell Senate Office Building, Washington DC, (28 March 2007).

[46] *Report of the Commission to Assess United States National Security Space Management and Organization,* (11 January 2001): 20.

[47] See, Lorraine Martin, "Preparing for Conflict in Space: A New Perspective of the Joint Fight," *High Frontier*, Vol. 4, No. (2 February 2008): 20.

[48] J. Michael Waller, "Iran and Cuba Zap U.S. Satellites," *Insight on the News*, (19 August 2003). http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&folder=141&paper=1108. (Accessed 11 September 2009).

[49] Marcelo Soares, "The Great Brazilian Sat-Hack Crackdown," *Wired.com*, (20 April 2009). http://www.wired.com/politics/security/news/2009/04/fleetcom?currentPage=all. (Accessed 6 September 2009).

[50] PDD/NSTC 8, National Space Policy, (14 September 1996) in R. Cargill Hall, *Presidential Decisions: NSC Documents, Supplement: Newly Declassified Excerpts*, (Washington, DC: George C. Marshall Institute, April 2006): 23.

[51] *Ibid.*, 24.

[52] *Vision 2020*, op. cit.

[53] *National Space Policy*, (31 August 2006).

[54] Stephen Grey, "Death of Bin Laden's deputy: How the U.S. killed Al-Qaeda leaders by remote control," *The London Times*, (18 November 2001); James Martin Center

for Nonproliferation Studies, Al Qaida Profile, n.d. Available from archives at http://cns.miis.edu/archive/wtc01/alqaida.htm. (Accessed September 24, 2009).

[55] Lt Commander John Klein, USN, "Corbett in Orbit: A Maritime Model for Strategic Space Theory," *Naval War College Review*, Vol. LVII, No. 1, (Winter 2004): 64.

[56] Lt Gen Larry James, Commander, Joint Functional Component Command for Space, Statement before the Subcommittee on Space and Aeronautics, Committee on Science and Technology, U.S. House of Representatives, Hearing on "Keeping the Space Environment Safe for Civil and Commercial Users," (28 April 2009).

[57] Robert Lee Hotz, "Harmless Debris on Earth is Devastating in Orbit," *The Wall Street Journal*, (27 February 2009). http://online.wsj.com/article/SB123568403874486701.html. (Accessed 25 September 2009.)

[58] James, op. cit.

[59] The Center for Space Standards and Innovation offers something known as the SOCRATES-GEO service, which provides preventive notices of possible conjunctions to subscribers. http://www.centerforspace.com/. (Accessed 25 September 2009.)

[60] U.S. Human Space Flight Plans Review Committee, Summary Report of the Review, n.d. Available at http://www.nasa.gov/pdf/384767main_SUMMARY%20REPORT%20-%20FINAL.pdf. (Accessed 29 September 2009). The Committee is generally referred to as the Augustine Committee, after its chairman, former Lockheed Martin CEO Norm Augustine. Technically, the panel made no recommendations, but six of the eight options it identified for consideration involved extending the program through 2020.

[61] Remarks by the president on U.S. Space Policy, NASA Headquarters, (14 January 2004). http://history.nasa.gov/Bush%20SEP.htm. (Accessed 30 September 2009).

[62] Michael Griffin, "Leadership in Space: Address to the California Space Authority, December 2, 2005," in Michael Griffin, *Leadership in Space*, (Washington DC: National Aeronautics and Space Administration, 2008): 7.

[63] The fourteen space agencies were as follows: ASI (Italy), BNSC (United Kingdom), CNES (France), CNSA (China), CSA (Canada), CSIRO (Australia), DLR (Germany), ESA (European Space Agency), ISRO (India), JAXA (Japan), KARI (Republic of Korea), NASA (United States of America), NSAU (Ukraine), Roscosmos (Russia).

[64] *The 2008 Annual Report of the International Space Exploration Coordination Group*, (March 2009).

[65] The author benefited greatly from conversations with Dr. Scott Pace, a veteran space policymaker and current director of George Washington University's Space Policy Institute, for extended discussions of this approach over the years.

[66] James, op. cit., 2-3.

[67] Subcommittee on Space and Aeronautics, Committee on Science and Technology, U.S. House of Representatives, Hearing Charter on "Keeping the Space Environment Safe for Civil and Commercial Users," (28 April 2009).

[68] Nicholas Johnson, Chief Scientist for Orbital Debris, National Aeronautics and Space Administration, Statement before the Subcommittee on Space and Aeronautics, Committee on Science and Technology, U.S. House of Representatives, Hearing on "Keeping the Space Environment Safe for Civil and Commercial Users," (28 April 2009).

[69] Mancur Olson, *The Logic of Collective Action*, (Cambridge, MA: Harvard University Press, 1971 ed.): 36-43.

[70] PDD/NSC-49/NSTC-8, *National Space Policy*, (31 August 2006).

[71] Brian Weeden, "The space security implications of missile defense," *The Space Review*, (28 September 2009). http://www.thespacereview.com/article/1474/1. (Accessed 30 September 2009).

[72] See the Cisco website at: http://cisco.com/web/strategy/government/space-routing.html. (Accessed 5 October 2009).

[73] Hon. Terry Everett, "Arguing for a Comprehensive Space Protection Strategy," *Strategic Studies Quarterly*, (Fall 2007): 30; and Geoffrey Little, "Mach 20 or Bust," *Air & Space Magazine*, (1 September 2007).

[74] See, for example, Robert Butterworth and John Sheldon, "Deterrence in Space: Responding to Challenges to the U.S. in Outer Space," (Washington, DC: George C. Marshall Institute, 13 November 2008).

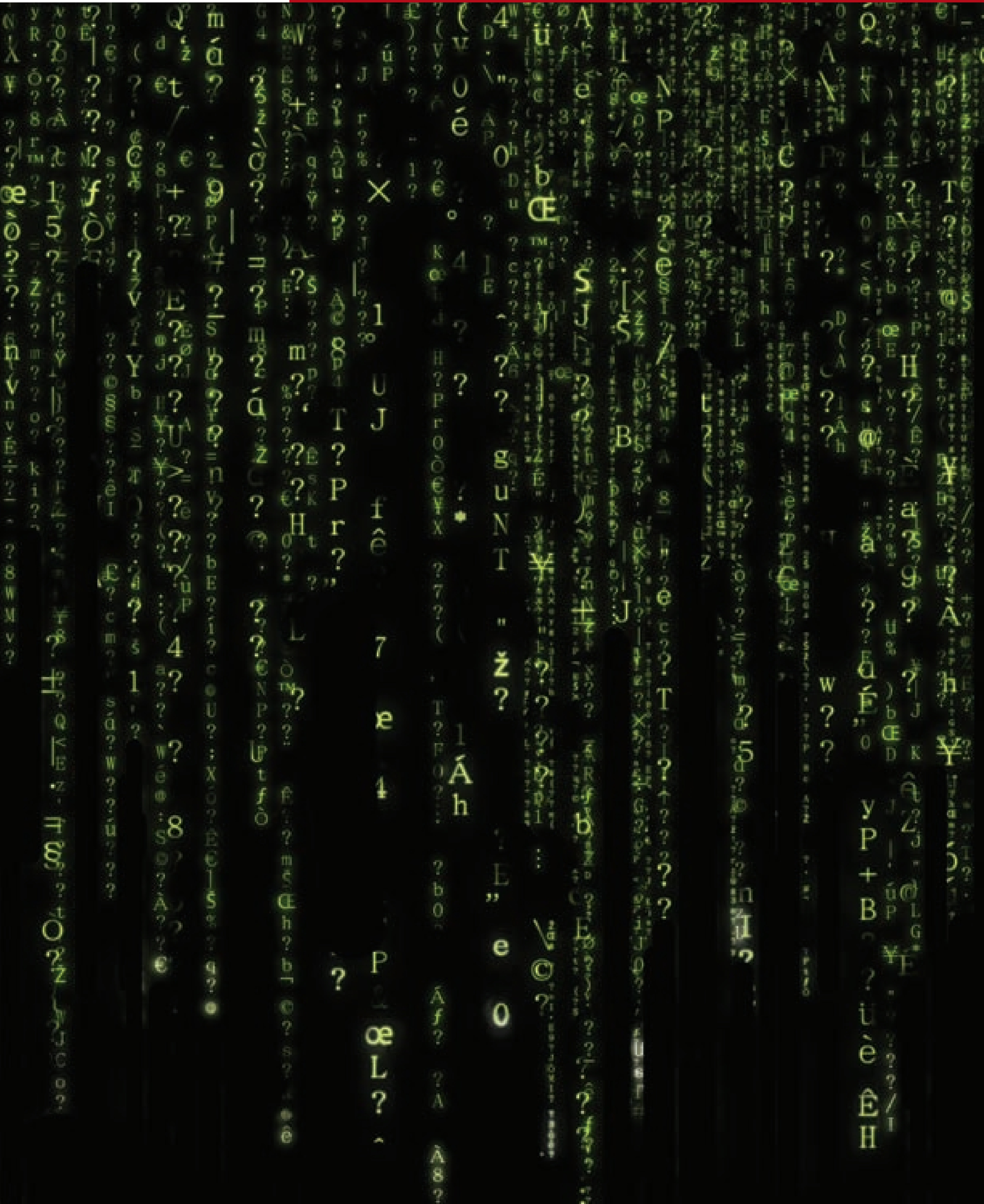
CHAPTER V:
AMERICAN SECURITY IN THE CYBER COMMONS

By Dr. Greg Rattray, Chris Evans, Jason Healey

JANUARY 2010

Contested Commons:

The Future of American Power in a Multipolar World



AMERICAN SECURITY IN THE CYBER COMMONS

By Dr. Greg Rattray, Chris Evans, Jason Healey

Introduction

Cyberspace is now an integral part of modern life. People around the world interact, cooperate and compete through a series of networked linkages that span the world. This unique system has evolved into a truly global commons. Through a combination of simple web-based communications and more complex infrastructure networks, the cyber commons enables private and public institutions to provide essential services such as energy, food and water. Banks and asset traders use the Internet to shift billions of dollars within seconds. Modern militaries—especially the U.S. military—employ the cyber commons as a key enabler of military operations, using commercial and private networks for everything from command and control to logistics support.

Because of the fundamental importance of cyberspace to modern society, the international community has a significant interest in preserving the openness and stability of the cyber commons. However, the cyber commons are under threat as U.S. adversaries continue to develop capabilities to contest its free use and security. The cyber commons have become a medium for conflict, involving state and non-state actors.

The 2005 U.S. National Defense Strategy identified cyberspace as “a new theater of operations,” asserting the need to secure strategic access and retain global freedom of action, particularly through the control of the global commons in order to deal with traditional, irregular, catastrophic or disruptive threats.[1] Despite much progress in addressing the issue of cyber security, governments and militaries cannot agree on how to think about cyberspace, let alone how to defend and operate within it. International cooperation is similarly hampered. In many ways, the international community’s thinking on cyberspace is similar to thinking on nuclear weapons in the late 1940s. It was widely accepted that a new dimension of warfare had emerged and that it was significant, but foundational concepts such as deterrence and mutual assured destruction had yet to be defined and promulgated.

The 2005 U.S. National Security Strategy established four strategic defense objectives: "Secure the U.S. from direct attack. … Secure strategic access and retain global freedom of action. … Strengthen alliances and partnerships. … Establish favorable security conditions."[2] To accomplish these goals in the cyber commons, the United States must develop a new strategy toward cyberspace, improve funding for research and orchestrate all elements of national power.

Toward that end, this chapter will first describe the nature of the cyber commons and compare it with other commons. It will then discuss the meaning of power in cyberspace and how the openness of the cyber commons has become contested. Ultimately, this chapter describes a theoretical model — cyber public health — to promote a better understanding of the nature of the cyber commons. By describing the cyber commons in this way, this chapter highlights the imperative for the United States to focus on fostering a "cleaner, healthier" cyber environment in order to secure a broad range of United States and international interests. Finally, this chapter recommends collaborative and unilateral approaches designed to promote and protect the openness of the cyber commons and achieve American and international objectives.

Nature of the Cyber Commons

Cyberspace, a concept coined in the 1980s, was viewed initially as a space fundamentally separate from the physical world.[3] Some theorists went so far as to assert that cyberspace transcends geographic and national boundaries, and therefore strains traditional notions of sovereignty and security. Yet cyberspace is fundamentally a physical environment, created by connecting physical systems and networks, and managed by rules set in software and communications protocols — all of which are located in the sovereign boundaries of nation-states.[4]

Cyberspace comprises physical and logical systems and infrastructures that are governed by the laws of physics and the logic of computer code. The principal physical laws governing cyberspace are those related to electro-magnetism. The speed at which waves propagate and electrons move creates advantages and challenges: communication across cyberspace is nearly instantaneous and vast amounts of data can be transferred over vast distances, unimpeded by physical barriers or political boundaries. This speed and freedom of movement across the global cyber commons creates advantages, but dependence on the global cyber commons also creates vulnerabilities that adversaries can exploit.

In cyberspace, as in the other global commons, almost all activities involve the use of technology. Cyberspace is unique in that the interactions are governed by hardware and software that is man-made, so the "geography" of cyberspace is more mutable than other environments. Mountains and oceans are hard to move, but elements of cyberspace can be turned on and off with the flick of a switch. They also can be created, deleted or "moved" by programming new instructions for a router or switch. Cyberspace is not, however, infinitely malleable: Limits on the pace and scope of change are governed by physical laws, logical properties of code and the capacities of organizations and people.

Increasingly, researchers are discovering that the strategic geography of the physical and logical components of cyberspace share the rules of physics with countless complex self-organizing systems, called scale-free networks. These networks include cellular metabolism, protein regulatory networks and even social interactions (like the popular "six degrees of separation" games). These scale-free networks have the same immunity to random attacks, however they share a significant vulnerability to targeted attacks perpetrated against the most highly connected hubs.[5]

But is cyberspace a global commons? Cyberspace appears to fit the standard definition of a commons because it is a "type of good, a resource, which can have either public or private ownership but which is managed and used jointly by a group."[6] Yet, unlike the oceans, cyberspace is a diverse accumulation of networks—a network of networks. Moreover, while much of the information in cyberspace is considered public, the physical elements of the cyber commons—the desktops, the laptops, the servers, the Internet-enabled refrigerators, the routers, the telephones, the mobile phones, the LAN cables, the fiber optic cables—have clear owners.

Critically, though, the backbone "cloud" networks are almost like an ocean—vast and open to navigation by all. The cloud is public, despite being privately owned, because it is publicly used. The owners of the infrastructure comprising the cloud rarely are able to choose who transits their networks or for what use. Indeed this is built into key Internet design premises like network neutrality and open, universal access; the infrastructure is shared by all. The national borders, true owners, and even actual hardware used are so abstract that they are indeed truly common.

Power in the Cyber Commons

Two distinctive features of the cyber commons merit attention: offense-dominance and the rapid changeability of the cyberspace environment. Offense-dominance is characteristic of some other realms, but it has different implications in cyberspace. The weaknesses in the technological foundations, and the economic incentives for openness between networks and systems, make many key networks highly vulnerable to exploitation, manipulation and disruption by digital attack. Even non-state actors derive large advantages from the ability to focus on niche objectives, utilize anonymous access, rapidly leverage expertise and make decisions more rapidly. Offense is easy and defense is very difficult.

National security organizations cannot defend the environment simply by increasing the size of their military cyber forces.

In cyberspace, the tried and true method of limiting damage through preemptive first strikes or retaliatory strikes is largely irrelevant. It is easy to deploy attacking forces stealthily, and attributing the source and intent of attackers is difficult. Thus, an actor would have little confidence in trying to strike preemptively to remove the cyber attack forces of an even moderately sophisticated adversary. Similarly, trying to use cyber counter-attacks to disable attacks in progress is complicated by issues of identifying and discretely targeting the complex web of electronic points of origin of the attacker, the culpability of the networks and systems from which attacks appear to originate, and the fundamental fact that disrupting these points in cyberspace may have only a limited effect.

As a result, national security organizations cannot defend the environment simply by increasing the size of their military cyber forces. If the attacker has a high probability of rapid success, pursuing current information-security approaches with more vigor is fruitless. A robust, defensible infrastructure will depend on shaping the technologies employed, the obligations of operators of key networks and infrastructures, and the ability to coordinate government-private sector investment and responses to attacks.

Cyber defense will also require new thinking. Most attention in the national security community has focused on risks from espionage or a single, time-limited strategic cyber blow from a major adversary. Counter-strategies for states or terrorist non-state actors conducting an economic guerilla campaign in cyberspace remain underdeveloped. A unique characteristic of cyberspace is its rapid pace of change. Although nations have long competed in the sea and air, thanks to advantages derived through technological innovation, the fundamental physical forces and terrain of those environments do not change. Scientists and technologists have understood them better over time, developing technologies that could

Table 1

COMPARING THE GLOBAL COMMONS

	MARITIME	AIR	SPACE	CYBER
Strategic Advantages	Enables global power projection	Allows direct strikes against enemy forces and centers of gravity	Creates a new high ground; enables global imaging and communications	Enables fast transfer of information; finely coordinated military operations; force multiplier, especially for non-state actors
Speed and Scope of Operations	Slow transit over long distances; enables global strikes	Fast, global transit. Scope dependent on sortie rates close to targets	Allows for continuous global operations; detailed C4ISR; precision strike	Extremely fast global operations; automation of command and control
Examples of Key Features	Sea lanes, straits, canals, sea ports	Airports, air ceilings, English language commercial standard, basing and overflight access	Orbit slots, Lagrange points, space ports	**Physical:** submarine cables and their landing stations, Internet exchange points, corporate data centers, infrastructure nodes; **Logical:** TCP/IP standard, highly-connected web nodes
National Mobilization	Ensure cadre of professionals; link to private sector	Ensure cadre of professionals; link to private sector	Ensure cadre of professionals; link to private sector	Ensure cadre of professionals; link to private sector

measure altitude or longitude. By contrast, the man-made environment of cyberspace can change its key characteristics and dominant operating modes very rapidly. For example, as the World Wide Web expands, bandwidth capacities and memory capacities also increase, while new devices become ubiquitous. Software updates and additions to networks change the ability to defend and attack many networks on a daily basis. Changing standards, access and legal regimes, plus the accelerating deployment of new technologies, alter the landscape of technological choices, operational procedures and risks for all users, both attackers and defenders.

Understanding the rapidly evolving nature of the cyber commons means recognizing that its dynamics are those of complex adaptive systems, rather than those of classical physics. The mobilization of resources in this space will require leadership, strategies and decision-making processes that put a premium on learning and flexibility. Management and acquisition processes will need to support rapid implementation of changes to systems and networks, as well as agility in the adoption of rapidly changing rules governing access to outside networks and mission partners that balance usability and security. Leaders at all levels must be able to think with the proper mental constructs and analogies that match the nature of the environment. The conduct of military and other operations will place a premium on trusting individuals to understand the changes they see in the cyber tactical environment and adjust the execution of their operations quickly.

COMPARING THE CYBER COMMONS

To understand the nature of the cyber commons and the national security threats to open access, it helps to examine how strategic theorists have addressed questions of national power on land and the seas, in air and outer space.[7] Environmental theories of power highlight four common threads: technological advances, speed and scope of operations, control of key features, and national mobilization. Examining these factors provides insights into the way that the environmental characteristics of cyberspace will shape efforts to wield influence in the cyber commons.

Technological advances: The rise of digital connectivity has transformed the nature of conflict and international competition. Just as the telegraph and railroads brought about major shifts in the age-old struggle to dominate landmasses, technological advances in the cyber commons will transform the landscape of conflict and competition in the future.

A major imperative for strategic theorists is to predict the political-military impact of technological advances within a given common. For Halford Mackinder, the advent of rail transportation and telegraph communication meant that the nation or nations controlling the heartland would be in position to assert global rule.[8] For Alfred Thayer Mahan, the advent of steam meant that global trade and presence through maritime power would be the primary path to success for nations that could develop such capacities.[9] The air-power theorists thought that the rise of unstoppable strategic bombers meant direct strikes at the enemy centers of gravity would decide future conflicts.[10] The ability of man to move into space led theorists such as Colin Gray, Geoffrey Sloan, and Mark Harter to argue that sustained space presence is an essential enabler of military operations and control over the global information infrastructure.[11]

The advent of the Internet and the opportunities for information exchange and social dialogue created by it, along with the ubiquity of wireless and digital connectivity, have similarly profound implications for the nature of political, economic and military interactions. Competition to control the use of the electromagnetic spectrum can be traced to the 19th century, when the telegraph had a major impact on economic affairs, political reporting, and the conduct of diplomatic and military operations in the American Civil War and the Crimean War. Today, the electromagnetic spectrum plays an integral role in the application of military power. Special-forces units mounted on horseback operating against Taliban positions in Afghanistan in late 2001 called down GPS-guided precision air strikes from B-52s.[12] New U.S. fighter aircraft, such as the F-22, carry sensor systems that allow them to share data in real time. Crucial advantages accrue to those capable of creating information-enhanced forms of traditional military operations that leverage the global cyber commons, but most require very deep pockets.

Yet, leveraging the cyber commons is a two-edged sword. It is a significant force-multiplier, but reliance on cyberspace now creates crucial risk-management decisions for governments, corporations and other actors as they grapple with issues of control over sensitive information and network availability. Advanced weapons systems conducting net-centric warfare leverage commercial IT systems and global cyber infrastructures to reduce costs in design and production, to enhance support logistics, and to fuse sensor and intelligence information in the conduct of mission planning and targeting. However, this reliance on commercial IT systems beyond the direct control of the U.S. military creates new vulnerabilities. The capacity to evaluate tradeoffs related to operational value, connectivity, costs, vulnerabilities and threats—and to strike an effective balance—will become a core cyber-related military capability.

Technological advances in other environments are also changing the terms of competition, in a manner similar to the rise of steam propulsion. In that time, advantages went to those who could establish colonies and coaling stations to conduct global trade. Today, economic and military competitors of the United States have explicitly adopted such strategies in cyberspace. In the late 1990s, the Japanese set out national plans to establish the world's most advanced networks and promote the construction of ultra-high-speed Internet access for its businesses and its citizens.[13] The People's Republic of China has engaged in a multi-front approach: controlling public Internet access, developing proprietary operating systems for national use, and endeavoring to influence global standards evolution, especially for Internet Protocol version 6 (IPv6). Appropriately then, the 2005 U.S. National Defense Strategy explicitly acknowledges that "disruptive challenges may come from adversaries who develop and use breakthrough technologies to negate current U.S. advantages in key operational domains."[14] These fears were realized in the spring of 2007, when dissidents with ethnic Russian sympathies organized a disruptive series of cyber attacks that affected the Estonian government, banking and other sectors.[15] These attacks utilized botnets that were controlled across the global commons and utilized that commons to conduct acts. Similarly, cyberspace played a major role in Russia's 2008 territorial dispute with Georgia, as Russian-affiliated hackers blacked out most of Georgia's telecommunications and broadband

Matt Inaki, a computer network defender coach/trainer of SPAWAR Systems Center San Diego, shows U.S. Air Force Staff Sgt. Daryl Graham and Navy Information Systems Technician 1st Class Martin MacLorrain how to monitor the activity of a network during a cyber war training course at the Space and Naval Warfare Systems Center in Pearl City, Hawaii, July 12, 2007.

(MC3 MICHAEL A. LANTRON/U.S. Navy)

networks during the opening phases of the military operations.[16] Because of these fast-moving technological trends, cyberspace may represent the operational domain of highest risk for the United States in the early 21st century.

Speed and scope of operations: The rapidity of connections offered by modern communications and information systems to the cyber commons creates challenges and opportunities. Cyberspace can almost instantly make information on political, economic or military developments available across the globe. Commercial companies are tightening global supply chains by means of radio-frequency identification (RFID) systems linked to point-of-sale electronic inventories, increasing efficiencies and lowering costs. Militarily, complex logistics chains and new forms of rapidly-adaptive operations are made possible by the use of these systems. Actionable intelligence can be rapidly pushed to war fighters, allowing engagement of high-value targets across wide areas, as in the strike that killed al Qaeda in Iraq leader Abu Musab Al-Zarqawi.[17] Broadly speaking, advanced militaries can more tightly orchestrate joint operations.

Conflict in cyberspace will accelerate the pace of war. Key events and disruptive threats can rapidly emerge and shift in seconds. National leaders will face tighter timelines for decisions, even as it becomes increasingly imperative to orchestrate action across wider distances.

The requirement for rapid response in cyberspace can mean higher levels of automated decisions for states and other entities. However, this comes with profound implications for the role of human decision-making in wartime. Fusing sensor and communications systems enable the engagement of targets that emerge rapidly but offer very limited time periods in which to take action. Rules of engagement often call for high-confidence identification of potential targets, but a commander may not fully trust automated systems to make the call regarding weapons employment. Unfortunately, cyberspace presents myriad opportunities for adversaries to subvert automated systems and turn them against their operators, or against third parties.

Control of key features: Military strategists often focus on the importance of controlling key features, especially logistics and lines of communication. Mackinder focused on the centrality of telegraph communication to the success of land forces, while Mahan emphasized the importance of coaling stations and repair facilities in supporting dominant naval forces.[18] Similarly, activities from financial transactions to complex military communications require the ability to access crucial assets in cyberspace, such as undersea fiber-optic cables, communications satellites, and major interconnection points for large global networks (Table 1). Such key features in cyberspace are rather limited in number, meaning they represent vulnerabilities, the loss of which could significantly disrupt the functioning of the commons overall. For example, American fiber-optic networks were severely disrupted by the attacks of Sept. 11.[19] In March 2007, authorities in the United Kingdom arrested individuals accused of planning terrorist attacks against key Internet infrastructure locations on the two U.S. coasts (known as MAE East and MAE West).[20]

These key features may be held in the private sector or may be owned and operated by the state, yet this ownership can change rapidly given corporate maneuvers or the advance of technology. Standard-setting for communications systems can be in the hands of governments, as with traditional telephone systems through the International Telecommunication Union (ITU), or largely outside government control, as with much of Internet governance, in which stakeholders include governments, business, technical groups and civil-society organizations. Large actors such as national governments, militaries and multi-national corporations have choices about which systems to emphasize — such as open, Internet-based communications or closed, proprietary systems — and about the pace of adoption of new standards. In this context, it is important to remember that American firms currently dominate cyberspace's topography, and therefore copious amounts of global Internet traffic transits through the United States, putting it potentially in a dominant position.

National mobilization: The national mobilization of essential resources, including deliberate government efforts to coordinate military and commercial activities, is a central concern of military strategy. Naval, air and space-power theories focus on the potential synergy between a nation's commercial and military activities and the development of professionals dedicated to securing the nation's interests.

Human capital is an even more crucial resource in the cyber environment, which rewards pioneers. Risks in cyberspace are less physical than they were for previous explorers. The premium is on brainpower, creativity and ability to manage complexity. Historical U.S. strengths — advanced education, systems integration, and intellectual property development and management — should offer advantages in cyberspace competition. However, the lack of requirement for major resource investments and the ease of leveraging global access to networks will provide more advantages to non-state actors in cyberspace than in other environments.

In Western nations, expertise resides mainly in the commercial sector; the government and its military and national security establishments must effectively leverage this pool. This contrasts with the other environments related to national security. Non-state actors can leverage fairly small cadres of skilled personnel to use cyberspace for specific purposes, whether to mobilize large numbers of people for a demonstration against globalization, or to hire a botnet for disruptive attacks on infrastructure. The military will face significant challenges is this area, as the vibrant commercial sector cultivates talented cyber professionals with the cutting-edge technological challenges and significantly higher financial compensation in recognition of their expertise.

The centrality of human expertise requires the United States, like other major actors, to compete globally to cultivate, recruit and retain the human capital needed to successfully engage in cyberspace. These personnel must be capable of analyzing the ever-changing opportunities and risks present in the environment, operating and protecting the large enterprises and infrastructures that sustain cyberspace, and performing other tasks ranging from developing new modes of sharing information to developing the capacity for preventing or deterring disruptive attack. For the U.S. military, the challenge is to nurture a strong cadre of cyber experts, similar to the naval, air and space expertise that has enabled its success in other environments. This requires the vision and the will to divert resources from traditional military missions and instead invest in the core capabilities necessary for the cyber environment.

The Pentagon has recognized the vulnerability created by its leveraging of commercial networks. The 2005 National Defense Strategy states, "Successful military operations depend on the ability to protect information infrastructure and data. Increased dependence on information networks creates new vulnerabilities that adversaries may seek to exploit."[21] It is unclear whether the Department of Defense has yet to sufficiently address this vulnerability, but recent efforts to develop a new cyber security strategy and the creation of U.S. Cyber Command suggest efforts are ongoing.[22]

U.S. Government Efforts to Protect the Cyber Commons

For more than a decade, the United States aggressively approached cyber space as a national security issue, with a focus on defensive measures:

- The Clinton administration's Presidential Decision Directive 63, Critical Infrastructure Protection, put protection of key U.S. assets against cyber attack on par with defense against physical strikes.
- The Bush administration extended this effort in its 2003 National Strategy to Secure Cyberspace, which outlined the efforts necessary to reduce U.S. vulnerabilities and ensure disruptions to the nation's critical infrastructures are infrequent, of minimal duration, manageable and cause the least damage possible.[i] In January 2008, NSPD-54/HSPD-23 formulated and launched a Comprehensive National Cyber Security Initiative (CNCI) to protect federal government systems from cyber espionage threats.
- In November 2008, the Commission on Cyber Security for the 44th Presidency identified "America's failure to protect cyberspace [as] one of the most urgent national security problems facing the new administration." It called for White House leadership, development of national-level strategy, public-private cooperation and international engagement.[ii] Early in the Obama administration, a White House-led cyberspace policy review stressed similar themes, emphasizing national communications and information infrastructure.[iii]

The U.S. government has officially distributed responsibility for cyber security across several agencies:

- The **Department of Homeland Security** is charged with protecting the .gov communications and information infrastructures against attacks in cyberspace.
- The **Department of Defense** is charged with information assurance, and with protecting the security of all aspects of the IT infrastructure that affect critical military infrastructures, including private-sector infrastructures on which the war fighter relies. With the establishment of a Cyber Command, the United States has more publicly recognized an offensive component of its approach to the cyber commons.
- The **Department of Justice** has dedicated capabilities for combating cyber crime, countering cyber espionage and supporting cyber counter-terrorism efforts.
- The **Department of Treasury** is the first line of protection for cyber infrastructure related to banking and finance.
- The **Department of Energy** is charged with protecting America's energy infrastructure.

[i] The White House, "The National Strategy to Secure Cyberspace," February 2003, http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf.

[ii] James A. Lewis et al, "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies, December 2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.

[iii] The White House, "Cyberspace Policy Review," May 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

THREATS AND VULNERABILITIES IN CYBER SPACE

The cyber commons today is a complex and anarchic environment lacking effective international agreements. Currently state and non-state actors are able to hack, intrude, corrupt and destroy data with relative impunity. While economic and technological necessity have allowed for the creation of standards and protocols to enable consistent communication, security in the cyber commons is often self-provided by users rather than by a central authority.

State and non-state actors are able to hack, intrude, corrupt and destroy data with relative impunity.

At the same time, the increasing use of the Internet and other aspects of the cyber commons by advanced states to manage domestic infrastructure creates new strategic vulnerabilities that adversaries cannot ignore. For example, sustained power outages or catastrophic breakdowns in transportation systems could result in significant physical damage and casualties, not to mention severely disrupting crucial economic, military and social activities. More disturbingly, attacks against these systems are technologically feasible.[23]

The distributed and interactive nature of cyberspace, combined with the low cost of computing devices, has lowered the threshold for actors to operate with great effect in cyberspace. Actors do not necessarily have to build complex weapons systems, like the Joint Strike Fighter, in order to leverage the benefits of cyberspace. Instead, accessibility and anonymity have created an environment in which smaller organizations and political actors, especially those who seek to hide from retribution in other environments, can achieve a disproportional increase in capabilities to conduct their operations and disrupt those of adversaries. The ease of achieving anonymity on the Internet also facilitates the rapid orchestration of operations across wide geographic areas with less chance of tipping off adversaries that disruptive attacks are imminent. The Madrid bombers, for example, reportedly used "a program downloaded from the Internet by which text messages could activate mobile phones simultaneously" to set off multiple explosions.[24] A 2005 *Washington Post* article noted that al Qaeda "has become the first guerrilla movement in history to migrate from physical space to cyberspace."[25]

Cyberspace has changed the dynamic of political and military competition, as states may be able to compete aggressively in cyberspace while still being deficient in other measurements of national power. Weak adversaries can use cyberspace to exploit vulnerabilities of their more powerful adversaries and, for instance, steal intellectual property from advanced states. Just as the expansion of global maritime trade required the development of colonies, naval fleets and their supporting infrastructures, cyberspace will require political and military measures to protect economic and informational interests. The United States will have to learn how to protect its cyberspace presence in a cost-effective fashion.

Indeed, using the cyber commons to achieve rapid strategic impact has become a tool for non-state actors. Organized criminal activity, Internet posting of terrorist videos of beheadings and malicious disruption on a global scale can all spread rapidly.[26] Cyberspace has multiplied opportunities for small groups to achieve large effects by getting their message to a global audience. This increases their geographic base for acquiring resources, whether through voluntary contributions or illicit activity. In the future, these groups will use cyberspace as a place where guerilla campaigns, orchestrated dispersal and surreptitious disruption can occur. The challenge for the United States is to create a recognizable signature in cyberspace that renders such nefarious groups vulnerable to retaliation and future deterrence.

Cyberspace offers opportunities for disrupting and crippling even the largest state opponents through new methods of attack. The disruptive attacks against U.S. and South Korean government and economic sites in early July 2009 illustrate this. While the actors behind the attack remain unknown, it is known that they utilized a bot-net of tens of thousands of computers based on a long-known vulnerability to network security protocols.[27]

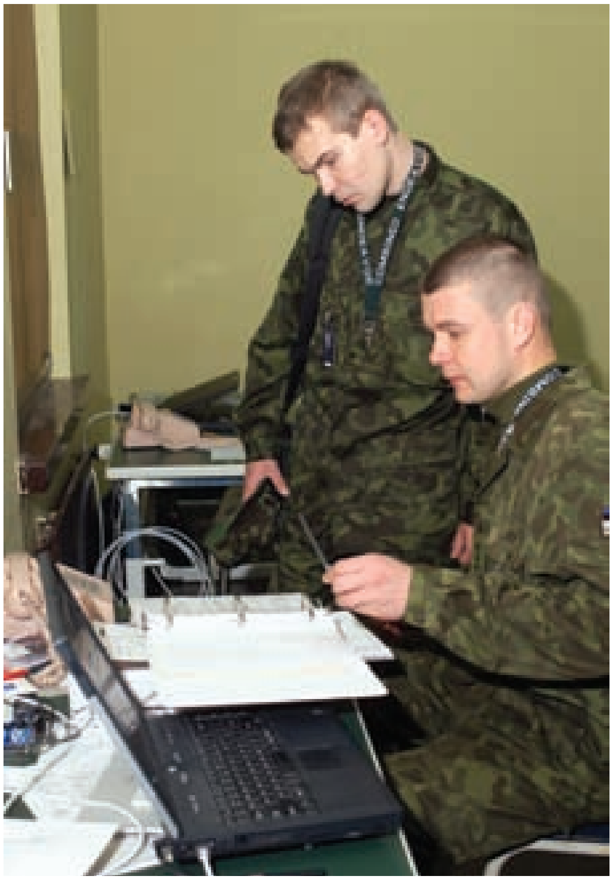
Although the major threat to the openness of the global commons stems from its anarchic and decentralized nature, several state and non-state actors are developing the capability to challenge U.S. and international access to the cyberspace.

- **Russia** reportedly has developed a robust ability to deny its adversaries access to cyberspace.[28] In April 2007, during an imbroglio surrounding the removal of a Soviet-era monument, the websites of the Estonian Parliament, ministries, media outlets, and banks were attacked and defaced. While the Estonian government immediately blamed Russia for the attack, they could not definitively link it to Moscow.[29] Georgia faced similar attacks during its war with Russia over South Ossetia in 2008.[30]
- **China** reportedly has developed several types of computer network operations. According to a Pentagon report, China's military has "established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks."[31] Indeed, according to the Pentagon, China's military has integrated these sorts of strikes into its exercises, using them as first strikes against enemy networks.
- **Al Qaeda** apparently has developed plans to target key businesses, government agencies, financial markets and civil infrastructure using cyberspace.[32]

In many respects, governance in cyberspace resembles the American Wild West of the 1870s and 1880s, with limited governmental authority and engagement.

GOVERNING THE CYBER COMMONS

To date, the United States and the international community have had little success in governing the cyber commons. In many respects, governance in cyberspace resembles the American Wild West of the 1870s and 1880s, with limited governmental authority and engagement. Users—whether organizations or individuals—must typically provide for their own security. Much of cyberspace operates outside the strict controls of any hierarchical organizations. No one individual or entity is in charge. Internet traffic is routed through peer arrangements between Internet Service Providers (ISPs), without central authority or control. The resolution of domain names fundamental to web browsing and e-mail is strictly based on an agreed set of protocols, loosely coordinated by a nongovernmental organization referred to as the Internet Corporation for Assigned Names and Numbers (ICANN).



Estonia Army Technical Specialists Captain (CPT) Daniel Meltsas (foreground) and CPT Andres Hairk, assign computer network passwords, during the U.S. European Command (USEUCOM) sponsored Exercise Combined Endeavor, held at Lager Aulenbach, Germany. The Exercise is the largest information and communications systems exercise in the world.

(SSGT KIMBERLY DRAKE/U.S. Air Force)

Further challenging any effort to govern or control the cyber commons is the complexity of its ownership — the physical infrastructure of the cyber commons is largely owned and controlled by the private sector. States do not, and cannot, command the cyber commons to the same degree as the sea or air, or even to the extent that they controlled communications technologies in the past. Today, there are myriad providers of devices, connectivity and services in loosely woven networks with open standards. Many governments, especially in the western world, have a limited ability to control cyber activities that originate within their borders. To date, the American approach to cyberspace has been supportive of a cyber commons that is open and market-based.

Yet, this condition of anarchy is not absolute. Economic imperatives and the desire to widen and standardize communication networks have led to the creation of relatively public and transparent nongovernmental operations of the Internet Engineering Task Force (IETF), ICANN and numerous other organizations for standardization, governance and regulation of cyberspace. States and other organizations can also establish boundaries by making choices in how to employ hardware, software and standards. For example, it has been over 100 years since the governments who set up the ITU required the principle of compulsory intercommunication between vessels at sea and the land . . . the first regulations governing wireless telegraphy.[33] Thus, states are able to exert some authority over their telephony systems, giving them the capacity to govern the economics of international calling and to monitor the communications of their citizens. Just as governments may jam "undesirable" radio and television broadcasts from outside their geographic borders, many authoritarian regimes employ software filters and other techniques to limit where their citizens can traverse within the Internet.[34]

Today, governance of the cyber commons is a messy amalgamation of international, national, and non-state protocols and agreements — all of which are sufficient for cyberspace to flourish but insufficient to make it safe.

International governance: Traditional international agreements, such as the Council of Europe Cybercrime Convention signed in late 2001, suffer from a lack of wide acceptance, adequate enforcement and an inability to conclusively identify the source of cyber attacks and intrusions.

National governance: National policy influences international, organizational and individual access to and use of cyberspace. China, for example, focuses on tighter control of individual rights in cyberspace, and seeks to establish a somewhat separate national cyberspace with controlled access to foster political control and improve its ability to defend national cyber assets. By contrast, the United States takes a *laissez-faire* approach and loosely manages the Internet and other cyberspace media to reap economic benefits of innovation and access to services. The impact of the different approaches on the ability to manage strategic conflict in cyberspace is not yet clear. However, a loosely controlled, diverse but robust network infrastructure may fare better than a centrally managed infrastructure with mandated barriers and defenses, if the latter is burdened with a limited capacity for rapid adaptation in the face of new threats.

Non-state governance: Non-traditional governance structures exist for certain aspects—IETF for technical standards and ICANN for domain names—but these are multi-stakeholder organizations in which governments have limited influence. Properly engaging and utilizing these mechanisms must increasingly play a central role in cyber security strategy.

New Perspectives on the Cyber Commons

As the statistician George Box famously noted, "All models are wrong; some models are useful."[35] Although models for cyber security are often discussed, the dominant model in the national security arena currently is the simple, binary and military model of offense versus defense. Conceiving of the challenge in terms of cyber public health offers a new and more useful model for securing the cyber commons. Public health is not completely compatible as a model for cyber security, yet the parallels between public health and cyber security make it an effective and insightful way to conceptualize challenges and solutions.

THE ENVIRONMENTAL MODEL: A COMPREHENSIVE APPROACH TO CYBER PUBLIC HEALTH

Public health, with its focus on sanitization and incident response, should be familiar to cyber defenders who worry about insecure systems being attacked by malware and rapidly spreading to their neighbors. Computer security expert and biostatistician Dan Geer cogently argues that as in cybersecurity, public health professionals worry about "macro scale effects due to micro scale events."[36] Epidemiologists are not worried about a disease per se, but rather about the spread of that disease. Their response does not necessarily require an understanding of causality; they focus on practical interventions to stop the disease.[37] In other words, epidemiologists concentrate on questions such as, "Where are the hot spots?" and "How many of event X is too many?"[38]

It must be stated from the outset that the public health model is not as useful in a wartime scenario, but it applies well in a range of peacetime scenarios in which cyber security involves defense against the spread of malware and botnet attacks—the cyber equivalent of "preventive medicine." Thus to understand the logic of interventions made in the interest of the "health" of the components of cyberspace (and collectively, of cyberspace as a whole), epidemiology and public health are good places to start.

Each entity in the cyber commons shares bandwidth and access to interconnected systems, just as organisms share an ecosystem. The symbiotic relationship between the cyber commons and its users induces competition between users for access to online applications, use of bandwidth and shared access to systems reaching through the core infrastructure of the Internet. Competition also exists, intangibly, between users needing privacy and security for conducting online activity; malicious users who seek to operate under the guise of privacy and defeat security; and the security community that promotes transparency to differentiate between malicious and benign activity and attempts to thwart malicious activity. Users — whether operating for good or bad, or as individuals, organizations or states — must work, play and survive in the same commons.

Malicious actors, be they nation states, criminal groups, terrorists or rogue hackers, rely on the inherent ease of entry provided by the Internet to mask their activity. The sheer size of the Internet produces a noise level,[39] beneath which much activity cannot be efficiently tracked, leading sophisticated attackers to try a "low and slow" approach.[40] When the interconnected systems that compose the cyber ecosystem are overloaded by malicious traffic, response times for time-critical applications decline and performance slows. As an ecosystem, cyberspace more resembles a swamp than other, more transparent environments. The Internet, in particular, promotes global connectivity, enabling global reach and presence to anyone with a connection.

THE DISEASE OF MALICIOUS ACTIVITY

The Internet is evolving. New technologies and techniques are blossoming within the ecosystem. Benign users are adapting these technologies to serve new purposes. However, lurking within the ecosystem are malicious users who also seek to evolve, adding to the compendium of viruses, worms, data compromises and debilitating attacks that are analogous to disease in the biologic world.

In biological ecosystems, a significant disease event can occur when the natural balance is disrupted. For example, something nonindigenous may be introduced, such as the influenza virus in the human body, or something offsets the balance, such as HIV infection that reduces the effectiveness of the human immune system. Or, something indigenous to the system multiplies until it becomes a hazard, such as the case when bacteria normally present in the small intestine overgrows and causes negative effects.[41] Major upsets in the natural balance have the potential for widely destructive effects. In the cyber commons, the same holds true. However, global disease propagation and infection that can be measured in days or weeks in biologic systems can be measured in seconds and minutes across the global cyber commons.

Epidemiology has two primary measurements to determine the level of disease in a population — and therefore identify which diseases require "practical intervention."[42] Both of these measurements are applicable to malware and computer vulnerabilities, and with this model, U.S. priorities for intervention in the cyber commons can be determined. The first measurement, incidence, is the "rate at which new cases occur in a population during a specified period."[43] For example, there are X new phishing attackers per week, or Y new botnets created per day. The second measurement, prevalence, is the "proportion of a population that are cases at a point in time."[44] For example, X percent of all e-mail today is spam or Y percent of all computers are part of botnets.

The key properties of infections are just as important for cyber security as they are for public health:[45]

1. Prevalence: The number of infected compared to the number of those exposed.
2. Interval from the time of infection to becoming infectious oneself.
3. Duration of infectiousness.
4. Interval from infection to display of symptoms.
5. Duration of acquired immunity.

For example, in looking at over 500 incidents of compromised cyber security, Verizon found that in 11 percent of the cases, it only took minutes for a computer to go from being infected to becoming infectious.[46] In 64 percent of the cases, it was months before the symptoms were discovered. The symptoms were apparent before that, but as with biological diseases, symptoms are not always recognized, or recognized for what they are.

METHODS OF TRANSMISSION

In the biological world, infections typically can be attributed to three transmission methods: direct contact, indirect contact and airborne transmission.[47] In the cyber realm, infections similarly occur via direct and indirect contact. An unprotected computer with a newly installed, unpatched operating system has no resistance to the malware that is present on the Internet. Such a computer can be directly infected within minutes of being introduced to the Internet via direct contact.[48]

In both the biologic and cyber worlds, infections due to indirect contact do not spread as rapidly as those due to direct contact because an extra step is involved, usually contact with an intermediary object on which the disease is present. Such an occurrence is facilitated by poor hygiene in the biological world; in the cyber realm, poor hygiene consists of a computer being infected by removable media (e.g., USB pen drives, media cards), bad browsing habits (e.g., contracting malware via surfing malicious websites), and faulty security practices (e.g., opening email attachments in message from unknown senders).[49]

Even “secure” networks are not immune. The defense industrial base in the United States has been targeted by indirect attacks via sophisticated phishing messages that contained malware intended to compromise a computer and turn over control, remotely, to the attacker.[50] Government projects are not alone; automated teller machines at banks have been targeted and infected with malware that compromise a user’s bank account information and PIN.[51] The implications to national security are severe. Not only are systems that contain research and development data at risk, but also closed and well-protected networks are vulnerable to indirect infection. The issue is not limited to the government’s domain; civil livelihood is also at risk, as the United States is heavily dependent on technology.

Long periods between infection and pandemic are less common in cyberspace than in the biologic world, but they do happen. For example, the Michelangelo computer virus was built to trigger on March 6, 1992 and erase the hard drives of infected computers.[52] The event created public hysteria up to and on the trigger date with media reports wildly speculating on the virus’ potential impact.[53] Unrelated events (e.g., an ATM network affected by a power outage) were attributed to the virus, increasing its hysterical effect on the public. In these cases, the crisis communication strategies, such as those for public health pioneered and promulgated by Peter Sandman, can be similarly helpful for cyberspace.[54]

Outwardly healthy people can be carriers of disease, spreading the disease to others, without showing signs of the disease itself. As an example, Typhoid Mary was colonized by the typhoid bacillus bacterium, but showed no signs of the disease.[55] She was responsible for propagating typhoid until health officials determined that she was the source of the infection. Similarly, computers carrying a virus are often responsible for also propagating the disease, with few recognizable symptoms, and until the sources are detected and treated, may continue to propagate the disease. The colonized computer systems seen in early strains of the Conficker worm outbreak in late 2008 to mid-2009. These systems exhibited no outward signs of infection, but were the sole propagation vector.[56] Effectively, a large number of computers could be remotely controlled, with the resulting implication that malicious functions could be “switched on” at the whim of the actors behind the malware.

ADAPTION AND COUNTER-ADAPTATION

An action-counteraction dynamic exists in both cyberspace and the biologic world. In biology, as noted by Dan Geer,

> Were one to introduce a new predator species, the prey who had never before seen it are ripe for slaughter, whether we are talking about rabbits harvesting Australian grasslands or the African Clawed Frog harvesting the ponds of Golden Gate Park. It is predators that force prey to diversify.[57]

But predators must also diversify themselves in turn. This evolutionary arms race is called the Red Queen Effect from the Red Queen's race in Lewis Carroll's *Through the Looking Glass:* "It takes all the running you can do, to keep in the same place."[58] In biology, the only way that a species involved in a competition can maintain its fitness relative to the others is by improving its design.

This process of adaptation and counter-adaptation can be clearly seen in cyberspace. Early malware was characterized by rudimentary propagation methods, such as removable media, and no resistance to anti-virus programs simply because there were no anti-virus programs at the time.[59] As malware adapted to detection, stealth methods were introduced to hide from casual inspection, then polymorphic code was developed to hide from intense scrutiny. Today's malware has learned from its predecessors and now commonly exhibits traits seen in previous outbreaks. The Storm worm outbreak of 2007 saw several smaller outbreaks of variants as defenses were constructed and the worm adapted.[60] Such adaptation results in a never-ending Red Queen Effect: Malware authors introduce tactics and techniques, which are then countered and integrated into security products, forcing malware authors to once again develop tactics and techniques.

Building a Healthier, Cleaner Cyber Commons

If a public health model is a means to understand the challenge of cyber security, what would a cyber-public health response look like? In biological ecosystems, the standard course of action during an outbreak is to determine how the disease propagates, identify control points, establish control measures, and evaluate and follow up with any changes to the control points or measures as needed until the outbreak is contained.[82] This section looks at various measures used by epidemiologists—including sanitization, diagnosis, treatment, inoculation, quarantine and early warning—then concludes with lessons for the public health of cyberspace.

Universal sanitization precautions are typically the first step in combating sickness or pandemic. The public is encouraged to follow a set of rules to decrease their chances of contracting the disease. Precautions range from simple hand-washing to wearing protective clothing to special handling instructions for contaminated objects. In the cyber realm, precautions include installing the latest patches, uploading current anti-virus signatures and firewall rules, browsing safe websites, and scanning files for virus detection. Most governments and private corporations worry predominantly about ingress filtering on their networks, looking for cyberspace pathogens coming at them. In fact, from a public cyber-health perspective, egress filtering for cyber pathogens and malicious activity is far more important, and can drastically slow transmission rates.

Detection and diagnosis is critical to affect a treatment protocol. Detection of biologic agents is conducted primarily by medical practitioners (through testing or analysis of symptoms), the patient (through onset of symptoms), through public health surveillance data, or through the local media, with most detection being done by medical practitioners and patients.[83] Within the computer world, public awareness of malware, its causes, symptoms, and effects is not nearly as comprehensive. People generally know when they are ill or are experiencing atypical symptoms, but most users are oblivious to the fact that their computer systems have been compromised. According to Verizon, fully 75 percent of the intrusions they investigated were discovered by people other than the victims and 66 percent of victims did not even know an intrusion occurred on the system. Perhaps most worrying, 83 percent of intrusions were not discovered for weeks, months, or even years.[84] Correct diagnosis depends on testing and analysis of symptoms. In both cases, a sample of the biologic or cyber disease must be taken and analyzed, which usually occurs after the outbreak. It is simply not efficient to attempt to do this proactively.

Treatment follows diagnosis. Removal tools can be used to treat the malware, but the cyber realm has a key advantage. Unlike infected humans, computers can simply be "wiped clean" and their operating systems reloaded so as to remove the infection, provided that the time is available to reload the system, suitable data backups exist, and the original vector is patched (so the newly cleaned system cannot be re-infected).

Inoculation can help prevent computers from becoming infected with a disease. In biological terms, immunity can be natural (the effect of previous exposure) or acquired (perhaps with a vaccination).[85] In the cyber commons, users can choose malware-resistant operating systems or simply not connect to the Internet, but they acquire immunity most easily by patching their systems with the most up-to-date anti-virus signatures.[86] More important to the public health of cyberspace, though, is herd immunity. In this scenario, the majority is inoculated, but a few remain susceptible to the disease. However, a diseased member of the herd cannot spread the illness to the rest; the herd will survive.

83 percent of intrusions were not discovered for weeks, months, or even years.

Herd immunity in cyberspace can be achieved when enough systems are immunized through patches and other defenses. Although individuals may lose data, there would be no successful widespread botnet attacks or pandemic dissemination of malware throughout the herd, or network in this case.

Public health professionals have a choice when offering immunization shots. They can vaccinate against impact or vaccinate against transmission.[87] Vaccinating against impact is designed to minimize the harm. In this case, the worst failures get first protection.[88] In the recent swine flu pandemic, for example, doctors prioritized health care workers, children, the elderly, and pregnant women. In cyberspace, this means patching the most important machines first. The other immunization method, vaccinating against transmission, is designed to improve herd immunity. By giving priority of immunization to doctors and nurses (the front line of public-health defenses) and other individuals who are likely to encounter a great number of people (such as transit workers), the spread of the disease can be greatly diminished. In cyberspace, this would mean immunizing security devices and systems that have a high degree of interconnectedness. Individual organizations

Case Study: Combating the Conficker Worm and Swine Flu

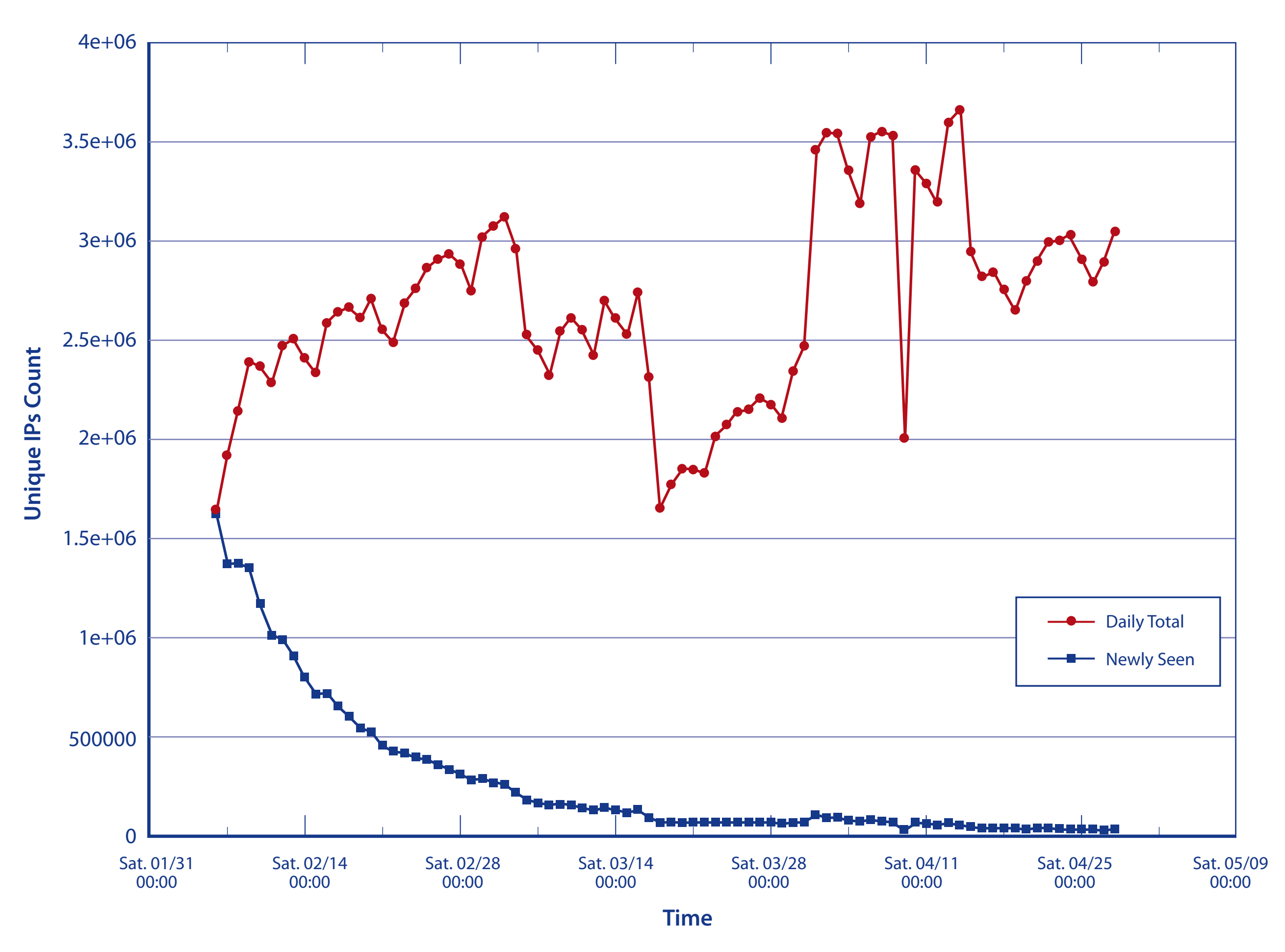
Comparing the Conficker worm outbreak on the Internet in late 2008 with the H1N1 swine flu pandemic of 2009 provides insight into how responses to future Conficker-like events could improve if they use the public health system as a model.

DISCOVERY AND MALWARE/DISEASE CHARACTERISTICS

In September 2008, a Chinese hacker introduced a proof of concept exploit that formed the nucleus of the Conficker worm, which installed itself and propagated to vulnerable computers, infecting a wide swath of the Internet user populace.[61] Defenses at the time, based on anti-virus signatures, were inadequate to stop Conficker as it formed one of the largest BotNets in the history of the Internet.

The first outbreak of H1N1 flu was in Mexico City and spread from person to person through direct or indirect methods.[62] Just like Conficker, existing defenses generally were not able to defend against it, as the swine flu was sufficiently different from the seasonal flu against which people had been vaccinated.

Figure 1: Conficker A/B Unique IP Addresses vs. Time (Sinkhole Data from Shadowserver.org).



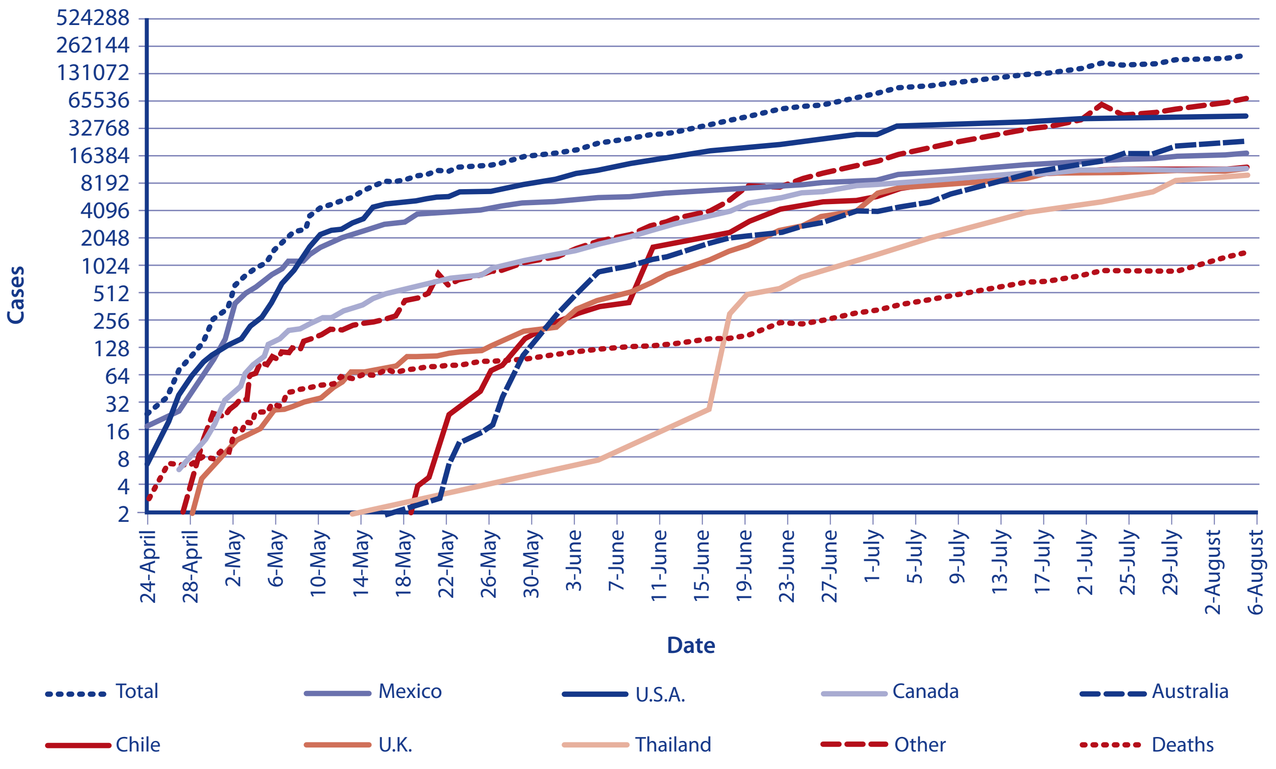
RAPID DEVELOPMENT OF THE OUTBREAKS

The original strains of the Conficker malware were detected by "honeypots," networks created for the purposes of capturing malware.[63] The rate of infection was enormous and estimates by San Diego Supercomputing Center at the University of California in San Diego place the number of infections increased by nearly half a million hosts in the span of 24 hours.[64]

The figure on the previous page shows the number of Conficker-infected computers, as both a total number (red line) and number of new infections (blue line) from February to May 2009. The near-vertical movements represent February 20, 2009, when Symantec released updated anti-virus signatures for Conficker.B variant, and March 31, 2009, with the increase in media coverage, release of network intrusion detection signatures, and remote scanning tools.[65]

The H1N1 flu spread fast similarly to Conficker. The chart below shows in more detail that, like Conficker, the flu started quickly before leveling off slightly after a few months. The rate of new infections slowed, but the number of infected continued to rise inexorably. For the swine flu, important dates were April 25, 2009, when the World Health Organization (WHO) convened its Emergency Committee for the first time; April 29, 2009, when the WHO raised the pandemic alert level to 5, the second highest, meaning pandemic is imminent; and June 11, 2009, when the WHO moved to the highest alert, 6, meaning a global pandemic.[66]

Figure 2: Influenza H1N1 Cases in 2009 Pandemic.



Source: WHO (http://www.who.int/csr/)

MUTATIONS SO FAR

Conficker's authors released a new mutation every four to eight weeks, thwarting the security community's efforts to detect and contain the worm. As its binary files were reverse engineered (equivalent to determining its digital DNA), Conficker responded to this Red Queen race with obfuscated code, anti-debugging features, and suicide routines, resulting in a more resilient strain.[67]

The first variant of the Conficker worm, Conficker.A, spread by directly exploiting computers that were not patched to fix the Microsoft Windows vulnerability Conficker used to propagate.[68] To receive instructions and updates, Conficker.A relied on the Domain Name System (the DNS, which maps domain names, such as "www.example.com" to a unique computer address, such as "208.77.188.166") to receive instructions and updates. The next mutation, Conficker.B, featured additional propagation methods and expanded use of the DNS to spread more quickly and defeat defenses which had been hastily erected to block it. Conficker.C further increased its use of the DNS, and added the ability to receive updates and instructions from other infected computer via a peer-to-peer network.[69]

On the other hand, researchers now believe the H1N1 swine flu "strain has been circulating among pigs for many years prior to its transmission to humans… [and] derived from several viruses circulating in swine."[70] In a similar way, the current strain is likely to mix with seasonal flu to become either more transmissible or more hazardous. A bleak reminder is that the 1918 Spanish flu started mildly before returning the following seasons to kill an estimated 20 million to 100 million.[71]

COLLABORATIVE RESPONSES

The responses to both Conficker and H1N1 showed a tremendous amount of global coordination. The table below summarizes the similarities and differences in response methods.

Initial responses to Conficker belied its potential. Microsoft released a patch for the infection vector via its "Automatic Updates" feature. In addition, the US-CERT released an advisory on the vulnerability; however, both it and the patch proved to be ineffective in preventing the outbreak.[76] By late December of 2008, security experts realized Conficker was using the DNS as a method of command and control and individuals attempted to preemptively register the domain names it was using to prevent Conficker from spreading.[77] In early February of 2009, as Conficker spread around the world, Microsoft announced the formation of a Conficker Working Group (a.k.a., the Conficker Cabal).[78] The working group brought together Internet organizations, companies, service providers, security experts, and academia to set a course of action in response to the growing threat. The working group focused promoting awareness and developing detection and eradication tools.[79] In comparison to the public health system, these responses were entirely ad hoc.

The public health system had existing monitoring systems and formal international mechanisms to share information and actual viruses. The WHO used years of pandemic preparation to convene a newly created Emergency Committee for the first time, which reported changes in the progress of the H1N1 epidemic using a well-tested pandemic alert level system to which governments and companies executed trigger-based action plans.[80]

The Internet connects people and systems around the globe without regard to their intent, and its openness and non-jurisdictional nature now provides "murk" for malicious actors to mask their activity. Public/private relationships to detect and stop malicious Internet activity are not present as they are for the public

Table 2

SIMILARITIES IN RESPONSE FOR CONFICKER AND H1N1

MEANS TO STOP SPREAD	CONFICKER	H1N1
Sanitization	Don't open unknown attachments or click on unknown links	Basic hygiene like washing hands and covering mouths
Coordination	Ad hoc Conficker Working Group with Microsoft, ICANN, CERTS, researchers, universities	Established coordination between UN (WHO), CDC (US), and other nations, laboratories
Immunization	Microsoft released patch MS08-067 to fix original Windows vulnerability	WHO launching largest immunization since 1955
Diagnosis	Researchers reverse engineered malware and examine behavior	Researchers examine virus DNA and behavior
Treatment	Remove trapdoors and control software after infection such as with Windows Malicious Software Removal Tool	Reduce symptoms, also Relenza® and Tamiflu®
Ingress Detection and Filtering	Signature updates were released for popular scanning tools like NMap and Nessus	Nations stopped inbound travelers from infected countries or who showed flu-like symptoms[72]
Egress Filtering and Quarantine	Many infected networks were taken offline, including in France[73] where the measure meant fighter bases could not access flight plans so their missions were scrubbed	Travelers dissuaded from going to infected countries.[74] Those infected were quarantined until it was clear they had no symptoms[75]

health community. Further, governments do not have (or use) sufficient authority to stop malicious Internet traffic, yet they do stop global travel during a biologic pandemic. For cyber outbreaks, there is no systemic, collaborative effort to manage the "swamp," but the public health model has such a system, originating shortly after the United Nations was founded over 60 years ago.[81]

The lesson from Conficker is that the ecosystem is at least partially defensible. Approaches limited to only one government, industry sector, or company to combat malicious activity are prone to failure in the face of a malware pandemic. Instead, cyberspace needs global collaborative and enabling approaches to clean the global cyber commons to constrain Conficker-like threats of the future.

will routinely choose to minimize harm, but governments have a responsibility to minimize transmission and improve herd immunity.

A 1998 study of the World Wide Web estimated that if one started arbitrarily from any of the then-800 million nodes, or documents, it would only take about 19 clicks to reach any other document.[89] While convenient, there is a dark side to this interconnectivity:

> …the Internet makes casual transmission of pathogens the norm as you are in close quarters with every other species and organism.… As children have fewer rights and share more fluids, we simply mandate their immunization. An analogy at the level of the Internet and national infrastructure is dauntingly obvious—should ISPs, the analog of public schools, be required to demand proof of immunization before permitting client entry into their networks?[90]

Quarantine and isolation are measures used to minimize disease propagation, and "There is a long history of quarantine powers being reserved to the state."[91] This method is susceptible to the risk of failing to isolate every infected person because of lack of detection or long incubation periods. Fortunately, in the cyber world, isolating infected computers is straightforward if a computer is determined to be infected. However, control methods do have downsides: Operations can be disrupted by isolation procedures, and universal precautions can be applied but are typically are not enforced. For example:

> When the (2004) Witty Worm was imminent, U Cal Berkeley and Lawrence Berkeley Labs [LBL] took different approaches. UCB warned systems administrators to administer a patch. LBL scanned their networks and only those who had taken the patch were allowed on the network. UCB had 800 infections. LBL had one. Quarantine works if there are diagnostic tests.[92]

At the level of cyberspace as a whole, quarantining implies the ability and will to isolate an Autonomous System Number (ASN) network from the rest of the Internet. Conducting this kind of quarantine requires a control strategy and, more important, the ability to enforce it. Lawrence Berkeley labs had the capability to scan for the presence of the patch and the ability to keep those compromised systems off the network. Plus, system managers had the fortitude to keep those compromised systems offline. While LBL's costs were probably lower in the long run, quarantining can be seen as a heavy-handed and expensive approach. Quarantining is certainly difficult, but not doing so highlights the risks in an environment in which it is inherently difficult to contain outbreaks.

If overdone, measures like quarantines can be worse than simply waiting for a cure. For example, the H1N1 (swine flu) outbreak in late 2008 caused considerable overreaction as evidenced by the slaughtering of pigs in Egypt, mostly attributed to lack of information.[93] In the cyber commons, carefully calibrating responses is similarly difficult, with the typical response being to issue a patch to close the initial compromising vector, and then hope for the best.

Consider the Blaster worm outbreak in 2003.[94] In a rush to stop propagation of the worm, network administrators disabled Internet Control Message Protocol (ICMP) capabilities. This action not only stopped the propagation of the Blaster worm, but it also rendered many of the network management, monitoring and assessment tools unusable. Such measures often make sense in a crisis but do not make sense as a long-term solution, and they can push network users to bypass security to be efficient or avoid inconvenience. In such cases, administrators and management need a strategy that defines a plan of action to preclude the unintended consequences.

Early warning is crucial. Indeed, "the mandatory reporting of communicable diseases" is the "lynchpin for public health."[95] However, the reporting of cyber infections has never fully taken root. Information-sharing and analysis centers, and cyber centers of excellence, have their place, but none match the power of centralized national and international reporting. The strength of international disease reporting and cooperation compels even authoritarian nations to participate. After being roundly criticized, both domestically and internationally, for a slow and secretive response to SARS, the Chinese government was significantly more active in international efforts to fight avian and swine flu.[96]

Corporations and governments, however, do not share adverse cyberspace information eagerly, for a number of understandable reasons. Reporting adverse information may cause a corporation to lose shareholder confidence or market share value. The information may be classified, or a government may feel sharing information would undermine its sense of national sovereignty. There is, however, good information to be found in the work of volunteer groups (such as the Internet Storm Center or the Shadowserver Foundation) and companies that collect information and share it with the community (such as the Verizon Data Breach Investigations Report or ESET's virus radar).[97]

Information on public health threats are combined to alert users about incidents of widespread concern. Each nation typically has its own system, for example Singapore uses the DORSCON system, but nations use common criteria and look to the WHO as the global coordinator.[98] In the cyber defense community, there are a multitude of alert systems, each run by a particular company or for a specific industry or government sector, all using varying criteria. There is far more confusion than in the public health system, largely because each group is pushing a system for its particular needs, its customers, or its financial gain. A system similar to the WHO pandemic alert phases makes sense for malware that spreads like a biological virus but may not be appropriate for alerting the Department of Defense to a cyber attack (for an alert comparison, see table 3).

Common criteria for reporting cyber attacks would work best mainly for home users, interested merely in protecting their desktops, and large companies that are part of the critical infrastructure sectors. Even here, commonality might be difficult to pinpoint as companies in the Defense Industrial Base may have different concerns than banks or electrical companies.

Following an outbreak in the biologic world, the medical community uses data to learn appropriate lessons to prevent future outbreaks. The medical community seeks to learn about the disease, reassure the public and contain hysteria, mitigate economic and social disruption, and teach identification, prevention, control and treatment of the disease.[103] In the cyber commons, there is difficulty in cleaning the environment as no single entity coordinates these functions. The world does not have a cyber-equivalent of the WHO, and the United States lacks a cyber Centers for Disease Control and Prevention (CDC).

ORGANIZATIONAL RESPONSES AND SIMILARITIES

Using the analogy of the cyber commons as a biological system, it is illuminating to study the organizational structure of the global public health world as a model for how the international community could better promote the health of the cyber commons. Response organizations are organized at the international, national, state and local levels, and they are chartered to proactively address health matters and respond to health crises such as outbreaks or bioterrorism as they occur.

At the **international** level, the WHO prescribes International Health Regulations, promotes information sharing, tracks volunteer reporting

Table 3

COMPARISONS OF ALERT "PHASE" SYSTEMS

WORLD HEALTH ORGANIZATION[99] "PANDEMIC ALERT PHASES"	MULTI-STATE ISAC[100] "CYBER ALERT INDICATOR"	SYMANTEC[101] "THREATCON LEVEL"	SANS INTERNET STORM CENTER[102] "INFOCON"
Changes declared by Director General, WHO	Changes declared by chair, MS-ISAC	Changes declared by Symantec security response centers	Changes declared by head of ISC
Phase 1. No viruses circulating among animals have been reported to cause infections in humans.	**Green, low risk.** No unusual activity exists beyond the normal concern for known hacking activities, known viruses or other malicious activity.	**Level 1, Low, Basic network posture.** This condition applies when there is no discernible network incident activity and no malicious code activity with a moderate or severe risk rating.	**Green. Everything is normal.** No significant new threat known.
Phase 2. An animal influenza virus circulating among domesticated or wild animals is known to have caused infection in humans.	**Blue, Guarded.** Indicates a general risk of increased hacking, virus or other malicious activity.	**Level 2, Medium, Increased alertness.** This condition applies when knowledge or the expectation of attack activity is present, without specific events occurring or when malicious code reaches a moderate risk rating.	**Yellow.** We are currently tracking a **significant new threat.** The impact is either unknown or expected to be minor to the infrastructure. However, local impact could be significant. Users are advised to take immediate specific action to contain the impact.
Phase 3. An animal or human-animal influenza reassortant virus has caused sporadic cases or small clusters of disease in people, but has not resulted in human-to-human transmission sufficient to sustain community-level outbreaks.	**Yellow, Elevated.** Indicates a significant risk due to increased hacking, virus or other malicious activity which compromises systems or diminishes service.	**Level 3, High, Known threat.** This condition applies when an isolated threat to the computing infrastructure is currently underway or when malicious code reaches a severe risk rating.	**Orange.** A **major disruption** in connectivity is imminent or in progress. Examples: Code Red on its return, and SQL Slammer worm during its first half day.

continues

Table 3 continued

COMPARISONS OF ALERT "PHASE" SYSTEMS			
WORLD HEALTH ORGANIZATION[99] "PANDEMIC ALERT PHASES"	MULTI-STATE ISAC[100] "CYBER ALERT INDICATOR"	SYMANTEC[101] "THREATCON LEVEL"	SANS INTERNET STORM CENTER[102] "INFOCON"
Phase 4. Characterized by verified human-to-human transmission of an animal or human-animal influenza reassortant virus able to cause "community-level outbreaks."	**Orange, High.** Indicates a high risk of increased hacking, virus or other malicious cyber activity which targets or compromises core infrastructure, causes multiple service outages, multiple system compromises or compromises critical infrastructure.	**Level 4, Extreme, Full alert.** This condition applies when extreme global network incident activity is in progress.	**Red. Loss of connectivity across a large part of the Internet.**
Phase 5, Pre-pandemic. Characterized by human-to-human spread of the virus into at least two countries in one WHO region.	**Red, Severe.** Severe risk of hacking, virus or other malicious activity resulting in wide-spread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.	None	None
Phase 6, Human-to-human pandemic.	None	None	None

of diseases and trends, and performs monitoring, alert and response operations.[104] The WHO's global perspective allows it to shape a research agenda and widely disseminate information. It establishes standards and guidance on promotion and implementation of evidence-based policy options. Further, the WHO manages Alert and Response Operations to track acute outbreaks, as part of the Global Outbreak and Alert Response Network (GOARN), through its JW Lee Centre for Strategic Health Operations.[105] The GOARN is a collaborative effort that provides rapid identification, confirmation and response to outbreaks at the international level.[106]

At the **national** level, the U.S. Department of Health and Human Services implements the federal public health system and operates the CDC. The CDC functions similarly to the WHO, providing centralized monitoring and guidelines for acute response, as well as supporting state and local programs through funding and assessment tools. The CDC also encourages research and development efforts in detection and response, which has led to the development of planning guides, models and recommendations for responding to outbreaks.[107] Examples include bioterrorism planning guides created by the Health and Human Services' Agency for Healthcare Research and Quality, and specific guidance for smallpox outbreaks.[108] While not directive in nature, the CDC guidelines are followed by state and local health departments, as the repercussions of disease outbreaks are well understood.

At the **state and local** level, public health departments are responsible for developing response procedures, establishing collaborative efforts with external partners such as the U.S. Office of Preparedness and Emergency Operations, emergency responder groups, professional societies, health care providers and researchers. The California Public Health Department, as an example, maintains a Center for Infectious Diseases, an Emergency Preparedness Office, and an office for Health Information and Strategic Planning.[109] All three contribute to the salient functions of monitoring, detecting, controlling and responding to outbreaks.

Public health operations exist at two levels: proactive and reactive. Proactively, each organization promotes collaboration to monitor and track ongoing diseases, develop response procedures and increase understanding of threats and risks.[110] Reactively, each organization responds according to its plans based on the National Response Framework (NRF), and implemented through the National Incident Management System (NIMS). The NRF defines a structure in which organizations at multiple echelons collaborate to develop response procedures. The NRF is based on five over-arching principles:

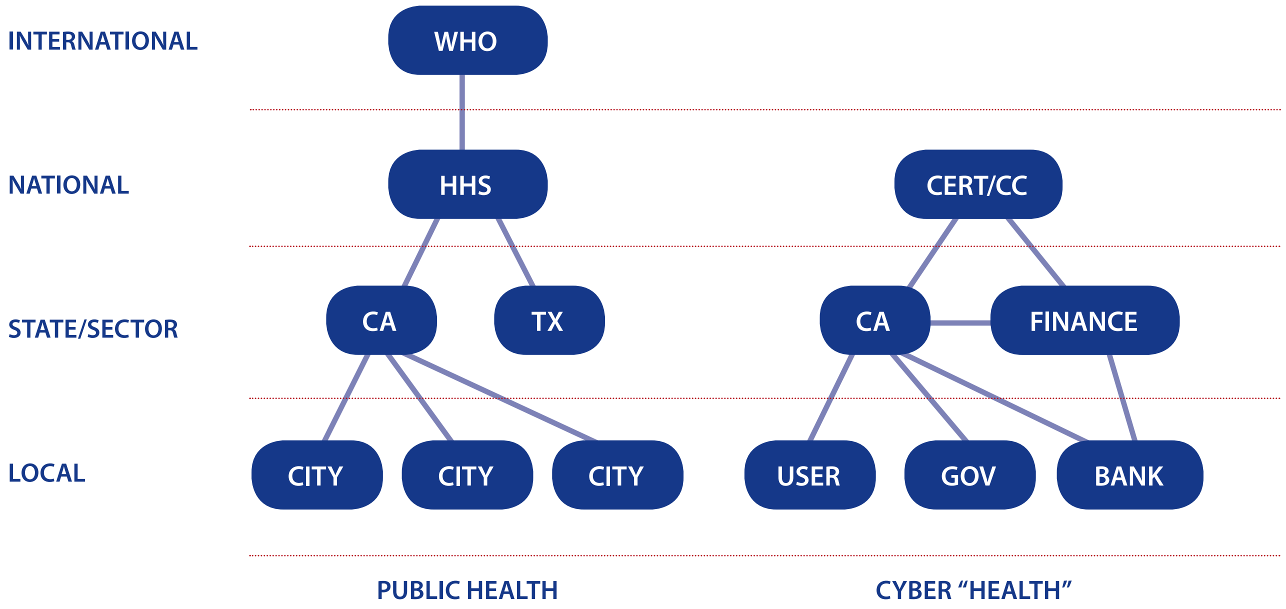
1. Engaged partnership.
2. Tiered response.
3. Scalable, flexible and adaptable operations capabilities.
4. Unity of effort through unity of command.
5. Readiness to act.[111]

The NIMS standardizes the response, defining a set of roles, responsibilities and structure during a crisis.[112] The NRF and the NIMS follow an "all-hazard" approach that has traditionally been defined as accidents, natural disasters and attacks. While the approach needed for cyber incidents is similar, neither the NRF nor the NIMS has addressed the specific needs of the cyber commons.

ORGANIZING FOR A CLEAN AND HEALTHY CYBER COMMONS

The public health model suggests methods for organizing proactive and reactive cyber response functions (Figure 3). A national cyber health organization would carry out functions similar to the WHO and CDC. State and local organizations

Figure 3: Public Health Organizational Relationships vs. Notional Relationships for Cyber Health.



(governments, businesses, security researchers, academia and even end users) could implement collaborative monitoring, detection and coordinated response functions. The key to successful implementation is a national strategy based on decentralized execution with the national organization enabling state, sector-specific, and local organizations to plan, train, exercise and conduct cyber defense actions. Implementation of such a strategy would require participation of key stakeholders, including those in security research, academia, private industry and civic organizations. The Conficker Work Group, created in response to the Conficker worm outbreak of 2008–2009, demonstrates how successful these collaborative efforts can be.[113] Although this working group was in response to a particular threat, collaborative efforts should be ongoing and threat-agnostic, focusing on an "all-hazards" approach similar to that used by the NIMS and the NRF.

The public-health structure also provides a model for international cooperation. Public health agencies are able to cut across political boundaries in times of crisis, something that is lacking in the cyber domain. Currently, the nation-centric nature of cyber communities breeds an inability for global collaboration, focus and response. Further, the proactive and reactive cyber defense methods in use are disjointed and ad-hoc, resulting in unnecessarily large impacts to all users of the cyber commons when outbreaks occur. Each entity, be it public, private, national or local, has some resources to enact cyber defense within its organization. However, coordinated monitoring, alerting, response and recovery functions like those in the public health domain is lacking. The WHO's GOARN shares outbreak information worldwide, but the cyber commons has smaller, competing organizations which monitor portions of the Internet, some offering access to "threat data" for a price. While individual response procedures exist, coordinated response on a national or global scale hasn't been seen before. Some business sector-specific relationships exist (e.g., the Financial Services—Information Sharing and Analysis Center) and enable collaboration, but they are operated on a voluntary membership basis. Without such functions, entities are left to their own devices for implementing cyber security, resulting in a broad spectrum of effectiveness, from nonexistent to superb.

Currently, the nation-centric nature of cyber communities breeds an inability for global collaboration, focus and response.

At the national level, a cyber health organization should focus on monitoring, detection, trend analysis, future outlook and developing a common response framework. The U.S. Computer Emergency Response Team/Coordination Center (US-CERT/CC), other national CERTs, and international organizations such as the Forum of Incident Response and Security Teams (FIRST) perform some of the same functions as the WHO and CDC, but they are not nearly as comprehensive. The US-CERT/CC provides risk management and threat awareness at the system and software levels, assists in vulnerability reporting to vendors and facilitates information-sharing.[114] While US-CERT/CC's information is publicly available on its website, the cyber defense community does not always take advantage of this resource, thus leaving a gap between the local and national level. A comprehensive cyber defense strategy at the national level, similar to the NIMS and the NRF, should be initiated. A collaborative national response to cyber threats could then be linked to the global community, just as the CDC is linked to other nations' public health programs via the WHO. Such a move would also establish the United States as a key player on the world cyber stage.

Organizations at the state level must enable information exchange between local and national organizations, while sector-specific organizations (such as banking and finance, or energy) would work on these issues for their companies. Collecting and publishing best practices from constituent organizations, sharing monitoring data, championing research efforts and assisting response activities during times of crisis are all activities these cyber health organizations should undertake.

At the local level, entities should plan for cyber outbreaks, coordinate response procedures and share information, in addition to implementing guidance from state and national levels. Such entities should include businesses, network security experts, academics, local governments and even end users. Each entity features different architectures and capabilities, and as such, are best positioned to determine specific implementations. This collaborative approach would provide a vast sensor network for state and national monitoring and detection programs. In a decentralized execution model, local organizations must be enabled and encouraged by the state and national entities to implement and conduct responses. Simply directing implementation from the national level will not be effective.

A Strategy to Protect the Cyber Commons

Managing the cyber commons is evolving into one of the most challenging national security issues of this era. Access to and control of the cyber commons is required for defense, economic growth and international engagement. To protect the commons effectively, the United States must be willing to address cyberspace's unique features by working for a healthier commons, ensuring the United States can work through disruptions and attacks, and understanding the limits of deterrence.

ENABLE DEFENSE, DETERRENCE AND OPERATIONS THROUGH A HEALTHIER COMMONS

The United States should lead global efforts to clean up the cyber environment. A healthy cyber commons serves broad strategic objectives by promoting democracy, economic markets and global dialogues. A clean, healthy cyber commons serves national security purposes, making it easier to identify the source of attacks and reducing the spread of botnets and other threats used by malicious actors that seek to harm the United States and its allies. A cleaner cyber environment would also reduce risks to U.S. military systems and operations that require cyberspace to conduct network-centric warfare and to project U.S. power globally.

Any effort to clean up the cyber environment will require international engagement for success. As in other commons, the Internet is too interconnected to make standalone national defenses effective. The United States cannot fight global issues like pollution or overfishing alone, just as the United States cannot be a steward of orbital space if other nations are going to destroy its satellites within that realm. The sanctuaries where malicious adversaries lurk in cyberspace, just as in the other commons, must be reduced. The number of vulnerable computers and networks must be reduced. And the ability of nations and Internet organizations to respond to threats must be improved.

In cyberspace, the State, Defense and Justice Departments' programs to build the capacity of national CERTs is helping establish legal frameworks and contact networks, as well as foster a culture of cyber security. This will help partners play roles in effective protection of the cyber commons. The United States must move beyond working with governments to engage and support global multi-stakeholder organizations such as the IETF or ICANN. In addition, it must encourage network operator groups to play active roles in ensuring the technological systems and operations of the cyber commons are more resistant to abuse by malicious actors and resilient in the face of attacks. In making the commons a better place for all users, these organizations can reach across political boundaries and remain outside the interplay of day-to-day political struggles.

Finally, the United States should take lessons from public health efforts at national and global levels. Specifically, the federal government should support public-private collaboration that enables the early warning of new threats, the rapid response to contain the spread of malware, and the long-term commitment to eradicating malicious activity that often thrives in the cyber commons. The fundamental strength of such efforts will come from private-sector technology vendors, network operators and security providers who have the expertise in cyberspace. The government should be an enabler and in some situations a coordinator, rather than the guardian and the controller of cyberspace.

To exercise leadership, the United States must be perceived as acting within a broader global agenda and not merely looking for advantage and dominance. The Internet was spawned from a DoD-funded experiment, however it grew into a wholly new environment for human interaction. As this experiment in sharing research developed into a global commons, the United States had the vision to facilitate its global interoperable use and to cooperate broadly in the diffusion of the technology. Internet governance structures include people, groups and governments around the world. As U.S. reliance on the cyber commons grows, challenges to U.S. security mount. Therefore, the United States must continue to leverage its place on the high ground to mobilize international and global action. It must collaborate in seeking norms for proper behavior through declaratory statements, as well as promotion of efforts such as the Convention on Cyber Crime. While competition in the cyber commons continues, the United States must understand the utility of a cooperative strategy to advance its interests.

If attacks are targeted smartly and selectively against the most highly connected nodes, then destroying as few as 5 percent can isolate great parts of the network.

DEFEND KEY FEATURES OF CYBERSPACE

Defenders in cyberspace do not need to be everywhere at once. Cyberspace has its own key features, including the equivalent of the "high ground." This "high ground" consists of highly connected physical nodes (such as cable landing stations, DNS root servers, and Internet Exchange Points) and logical features — such as Google or the BGP routing protocol. Defending a mountain pass has been a successful strategy in land warfare for millennia. A pass is highly defensible, and there are usually a limited number of them, so commanding one means the enemy can be forced through a chokepoint, or diverted to lesser goals.

A small number of highly connected nodes form cyberspace's "high ground," and they should be a central part of a defense strategy, similar to the "vaccinate against transmission" strategy in public health. Research by physicist Albert-Laszlo Barabasi and others have shown that in a scale-free network like the Internet, up to 80 percent of nodes can be attacked without destroying the system as a whole — but only if the nodes are attacked randomly.[115] If attacks are targeted smartly and selectively against the most highly connected nodes, then destroying as few as 5 percent can isolate great parts of the network. Some of this high ground is controlled by the government, but most is owned by the private sector. Accordingly, the U.S. government must prioritize infrastructure protection and information-sharing efforts on the commanding heights with lower emphasis on less-connected nodes. This idea matches recommendations made by the Center for Strategic and International Studies' Commission on Cyber Security for the 44th President.[116]

The United States still commands a great — but diminishing — number of these physical and logical passes of the cyber commons. None of these chokepoints have yet been used to improve the global cyber commons. The United States may be losing comparative advantage because of the growing diffusion of control over cyber assets and privacy concerns about intelligence collection.[117] Regardless of the reasons for this decline, improving the state of cyberspace not only reduces the number of attacks against the United States, but also can influence allies through the use of soft power.

DEFENSE THROUGH RESILIENCE AND AGILITY

Attackers typically have superior freedom to maneuver in cyberspace. Development of botnets increases attack mobility by creating fluidity in launch sites through decentralized control of botnet armies, with little time and effort required for preparation. The attacker does not face the challenge of synchronizing a large physical force, and the victim is limited in its capabilities to determine the location or size of attacking forces.

Despite plans for information dominance, it is more likely that the adversary's offensive capabilities will overpower those of the United States than vice versa, because of heavy reliance on information technology and vulnerable critical infrastructure. As the United States moves to global sourcing of information technology products and services such as smart grids, wireless control systems within critical infrastructure, and Voice-over-Internet Protocol (VoIP), it presents adversaries with additional access to, and insight into vulnerabilities within, strategic target sets.

Therefore, a major focus of cyber defense should be on resilience and agility across all national assets — far different than implementing a specific set of federal standards and reporting as currently required under the Federal Information Security Management Act. Resilience and flexibility come from a commitment to work through and around Internet disruptions, just as militaries have trained and learned over the centuries to fight through deception, nighttime, fog, clouds and electronic jamming. Apart from individual technicians and system administrators, few observers would argue that American cyber fighting forces have much nimbleness. The flexibility and ingenuity that American kinetic forces are known for must be emulated in its cyber forces.

Cyber training must be done in a realistic manner. During exercises, U.S. Air Force pilots learn to find and kill the enemy despite jamming.[118] Interestingly, U.S. Air Force cyber exploitation and denial professionals, commonly referred to as Red Teams, are rarely allowed, if ever, to conduct similar attacks during large games against critical command and control nodes. In other words, cyber operations teams are unable to train in the manner they may be expected to fight. But, if the air tasking order (ATO) is not delivered accurately and securely because the network is successfully degraded, critical air war-fighting capabilities are neutralized. Although this is an Air Force-specific example, this training scenario failure occurs at nearly every level in every service, department and agency. By thinking about and developing options that allow users to work through Internet disruptions, users would be able to improve their understanding of the network, as well as their critical information requirements. In addition to planning for and practicing within a degraded system, users would improve the command and control system's resiliency as well as gain confidence in their own abilities. Knowing how information, IT systems, and communications relate to operational functions and mission effectiveness are essential to achieving more resilience to cyber attack and disruption.

Going forward, the U.S. national cyber security effort must also change the conception of public-private partnerships. Instead of seeking centralized means to detect and respond, the federal government should build flexibility and trust as an enabler for operational defense and resilience to occur at the points of contact between attacker and defender. While public-private sharing is essential, the nation's defense is served not by a Maginot cyber line operated by the military or other national security agencies. The national security focus should engage the operators of cyberspace, critical infrastructures and other national assets with cyberspace dependencies, to improve their own defenses and resilience. Federal cyber security efforts should stress mutual sharing of observed threat activity, effective countermeasures, best practices for resilient operations and joint cyber defense contingency planning and exercises. The government should encourage active cyber defense collaboration between private sector parties, even in those situations where barriers of law, policy and trust limit governmental involvement.

At the end of the day, improving resilience and flexibility will not be easy. National security strategists must consider whether efforts to improve the health of the cyber commons might be one of the more cost-effective strategies. Furthermore, national security strategists must determine if a well-orchestrated and transparent program of national cyber resiliency deters adversaries who consider cyber attacks against the United States. The situational awareness underpinning defense, risk management, resilience, and even deterrence, is cheaper if the system is healthier and more transparent, and such measures will reduce the day-to-day costs of fighting threats emerging from cyberspace commons.

UNDERSTAND LIMITATIONS OF CYBER DETERRENCE

There is a strong need to develop strategies for cyber deterrence.[119] However, the difficulty of attributing responsibility for attacks provides fundamental challenges to credibly respond, whether in cyberspace or through other means. The inability to determine responsibility for behavior creates further challenges of justifying a response. During the Cold War, the United States and the Soviet Union took decades to establish basic ground rules for behavior, and there were many tripwires that could initiate armed conflict. In cyber deterrence, shared norms and a means of signaling intent do not yet exist.

Additionally, the cyber commons is home not only to government actors with strong, centralized decision-making, but also to a range of non-state actors ranging from criminal groups to the politically disenfranchised. These actors can conduct disruptive activities that challenge the United States through access to, and attacks from, the cyber commons without having to place their own assets at risk in cyberspace. Moreover, these groups may have no geographic home, complicating responses outside of cyberspace.

Two key elements have been lacking in the U.S. dialogue about cyber deterrence. First is the degree to which the cyber commons presents opportunities to constrain U.S. actions. U.S. strategic assets such as financial systems, power grids and telecommunications networks are subject to disruptive cyber attack and are operated by sectors that are more susceptible to coercion than the U.S. government. For example, if the president were to choose a course of action perceived as benefiting Taiwan to the detriment of the People's Republic of China, a subsequent strategic attack on America's cyber infrastructure could lead the U.S. private sector to lobby the administration to pursue a different foreign policy.

Second, for national security purposes, technical attribution is not needed. Attribution is still useful to help prosecute and stop individual attackers, but fussing about attribution restrains the national security community as much as it helps. Instead, the national security community needs to understand the responsibility of an attack, not the attribution, is most often what is needed to respond. "Who is to blame?" is more to the point than "Who did it?"

For instance, in 1999, NATO aircraft mistakenly bombed the Chinese embassy in Belgrade, Serbia during airstrikes designed to compel Yugoslav troops to withdraw from Kosovo. The U.S. embassy in Beijing (as well as other embassies and consulates) were targeted by angry Chinese protestors who tore up the roads for stones to throw, smashing windows and trapping the ambassador and others in the compound, which looked like a "war zone."[120] Yet, the U.S. intelligence community and National Security Council staff did not spend much time watching video and backtracking trajectories to identify the individual stone throwers. Such attribution was not a priority, because the Chinese government clearly encouraged the response.[121]

In 2007, Estonia was deluged by cyber attacks. All signs pointed to Russian involvement: Many of the cyber attacks themselves were traced to Russia;[122] many of the attack tools were written in Russian;[123] many of the corrupted Estonian websites were polluted with strong nationalist Russian reactions;[124] numerous Russian politicians openly supported the attacks;[125] and the Russian government refused to stop or even investigate the attacks. Russian police simply remained on the sidelines.[126]

But in analyzing this case, too many analysts have been back-tracking the trajectory of the cyber stones, in a "keyboard-versus-keyboard or geek-versus-geek approach."[127] In the end, this approach has led to the single prosecution of one student.[128] If, however, we look instead for national responsibility, Russian leadership clearly encouraged and abetted the attacks against Estonia, just as the Chinese government did for its protesters against the United States.

This national responsibility is often missed because of a fixation on attribution inherited from law enforcement methods and cyberspace's technical roots. "Who did it?" can be found in system logs, and that information can lead to prosecution. Attribution of individual attacks is critical for many reasons—not the least of which is to seek prosecution or uncover evidence to determine national responsibility.[129] Determining responsibility re-establishes some state-to-state symmetry and enables deterrence, as well as a wider range of options open to sovereign nations: diplomatic, intelligence, military and/or economic responses. Accordingly, the national security community needs to shift resources from the "attribution problem" to the "accountability problem."

CLEAN THE CYBER COMMONS

Although burning coal or oil has been essential to becoming an industrial society, pollution in cyberspace is not a necessary byproduct of becoming an information society. Nations retain sovereign rights to pollute in order to improve the prosperity of their citizens. This good is then balanced against the global harm to the commons. Nations do not have good reasons to pollute cyberspace, however. Unpatched personal computers are unlikely to boost a nation's gross domestic product. Furthermore, botnet armies conducting cross-border attacks are not contributing to the public wealth of the nation hosting the infected host computers.

As with environmental pollution, nations must take some level of responsibility for every attack in cyberspace. For attacks emanating from the United States, this responsibility is overwhelmingly passive; as a matter of policy, the U.S. government does not encourage, condone or support cyber attacks.[130] However, the United States has too many uncontrolled, insecure systems that are used to attack others—for which it bears some responsibility. Comparatively, more accountability falls to Russia for the cyber attacks against Estonia and Georgia in 2007 and 2008.[131]

A national security goal for the United States should be to hold other nations accountable for attacks coming from their geographic parts of cyberspace. New norms and cooperative agreements could present nations polluting cyberspace with two choices: Clean up or be cleaned. If the nation hosting the malicious activity does not or cannot stop the illegal and nefarious activity, the international community needs agreed-upon protocols (training, education, funding, access to technology) to assist. If these agreed-upon protocols do not stop the attacks, certain agreed-upon procedures might allow aggrieved parties to take action by externally patching systems or by disabling botnets. Accountability is, of course, a dual-edged sword. In return, the United States must work diligently to reduce its own passive responsibility, lest it be open to criticism or action from other nations who receive cyber attacks from U.S. cyber soil.

Conclusion

The international community must preserve the benefits of innovation and connectivity that have made the cyberspace commons so valuable. Defense and economic institutions depend on cyberspace and cannot allow a regression toward a Wild West of continuous malicious activity. Thus, it is in America's long-term commercial and national security interest to ensure the cyber commons is clean, in order to prevent the spread of dangerous outbreaks, and to respond appropriately when required.

The strategic features of the cyber commons are becoming more apparent. Nations can, and will, vie for control of the commons in pursuit of national interests. However, current limitations exist in monitoring, detecting, coordinating responses and sharing information in times of national crisis. From a national defense standpoint, this situation makes the cyber commons hard to control.

The evolving cyber environment requires substantially different national security approaches than other commons. Because of the more mutable, human-driven characteristics of cyberspace, the United States must look for ways to embed flexibility and mechanisms for rapid change in policy, institutions, technology choices and human capital plans. Insights from public health serve as useful guides to developing innovative approaches to achieve a cleaner cyber commons. The fundamental lesson of biology is that survival and success is not necessarily the reward for the biggest, strongest or meanest, but rather for the most adaptable. The ability to learn, cooperate when fruitful, and compete when necessary will strengthen U.S. efforts to ensure access, use, and control over the cyber commons.

ENDNOTES

[1] U.S. Department of Defense, *National Defense Strategy*, (March 2005): 1 & 3.

[2] *National Defense Strategy*, iv.

[3] The first use of the term “cyberspace” was in William Gibson’s cyberpunk novel Neuromancer in 1984.

[4] See Dr. Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge MA: MIT Press, 2001): 11–12.

[5] Researchers have proven the “scale free” nature of both the physical interconnections of the Internet as well as the information linked on the Web. See, Albert-Laszlo Barabasi and Eric Bonabeau, “Scale-Free Networks,” *Scientific American*, (May 2003); and Albert-Laszlo Barabasi’s, *Linked*, (Perseus Publishing, April 2002).

[6] Charlotte Hess, “Untangling the Web: The Internet as a Commons.” Workshop in Political Theory and Policy Analysis, Indiana University, (1996): 3.

[7] This framework was initially developed and published as part of the NDU Cyberpower project, resulting in the book, *Cyberpower and National Security* (Washington, DC: NDU Press and Potomac Books, 2009).

[8] Halford John Mackinder, “The Geographical Pivot of History,” *The Geographical Journal* (Royal Geographical Society, London), Vol. 23, No. 4 (1904).

[9] Alfred Thayer Mahan, *The Influence of Seapower Upon History*, 1660–1783 (Boston: Little Brown, 1890).

[10] Key works include Giulio Douhet, *Command of the Air*, trans. Dino Ferrari (New York: Coward-McCann], 1942); William Mitchell, *Winged Defense: The Development and Possibilities of Modern Airpower — Economic and Military* (New York: G.P. Putnam’s Sons, 1925); Maj. Gen. Sir H.M. Trenchard, “Report on the Independent Air Force,” (1 January 1919).

[11] See Colin S. Gray and Geoffrey Sloan, Geopolitics, Geography and Strategy (London: Frank Cass, 1999) and Mark E. Harter, “Ten Propositions Regarding Space Power: The Dawn of a Space Force,” *Air and Space Power Journal*, special issue on space power (Summer 2006).

[12] Max Boot,“Special forces and horses” excerpted from “War Made New,” *Armed Forces Journal* (November 2006).

[13] Japanese Ministry of Information, *Basic Guidelines on the Promotion of an Advanced Information and Telecommunications Society*, (9 November 1998), www.kantei.go.jp/foreign/it_e.html.

[14] *National Defense Strategy*, 5.

[15] Larry Greenemeier, “Estonian Attacks Raise Concern Over Cyber ‘Nuclear Winter’,” www.informationweek.com/news/showArticle.jhtml?articleID=199701774, (Accessed 24 May 2007).

[16] Siobhan Gorman, “Cyber attacks on Georgia used Facebook, Twitter,” Total Telecom, (17 August 2009), http://www.totaltele.com/view.aspx?C=0&ID=448132.

[17] Ellen Knickmeyer and Jonathan Finer, “Insurgent Leader Al-Zarqawi Killed in Iraq,” *Washington Post*, (8 June 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/06/08/AR2006060800114.html.

[18] Halford John Mackinder, “The Geographical Pivot of History,” *The Geographical Journal* (Royal Geographical Society, London), Vol. 23, No. 4 (1904); Alfred Thayer Mahan, *The Influence of Seapower Upon History, 1660–1783* (Boston: Little Brown, 1890).

[19] Committee on the Internet Under Crisis Conditions: Learning from the Impact of September 11 et al., *The Internet Under Crisis Conditions: Learning from September 11* (Washington, DC: National Academy Press, January 2003).

[20] David Leppard, “Al-Qaeda plot to bring down UK Internet,” *The Sunday Times*, http://www.timesonline.co.uk/tol/news/uk/crime/article1496831.ece, (11 March 2007).

[21] *National Defense Strategy 2005*, 13.

[22] Donna Miles, “Gates Establishes New Cyber Subcommand,” *American Forces Press Service*, (24 June 2009).

[23] Tim Wilson, “Experts: U.S. Not Prepared for Cyber Attack,” describing Congressional testimony, www.darkreading.com/document.asp?doc_id=122732, (Accessed 26 April 2007).

[24] Kathryn Westcott, “Transport systems as terror targets,” *BBC News*, (7 July 2005), http://news.bbc.co.uk/1/hi/world/europe/4659547.stm.

[25] Steve Coll and Susan B. Glasser, “Terrorists Turn to the Web as Base of Operations,” *Washington Post*, (7 August 2005): A01.

[26] The Slammer worm in 2003 caused major disruption across the Internet in a period of less than 15 minutes. Paul Boutin, “Slammed! An inside view of the worm that crashed the Internet,” *Wired*, (July 2003), http://www.wired.com/wired/archive/11.07/slammer.html.

[27] See Wikipedia for a summary of these attacks, http://en.wikipedia.org/wiki/July_2009_cyber_attacks.

[28] For example, see Tim Thomas, “Nation-state Cyber Strategies,” in *Cyberpower and National Security*.

[29] Arthur Bright, “Estonia accuses Russia of ‘cyberattack,” *The Christian Science Monitor*, (17 May 2007).

[30] John Markoff, “Before the Gunfire, Cyberattacks,” *New York Times*, (12 August 2008).

[31] U.S. Department of Defense, “Annual Report to Congress on the Military Power of the People’s Republic of China,” (2009): 27-28.

[32] “Al Qaeda planning cyber war against Britain, warns Lord West,” *The Telegraph*, (25 June 2009).

[33] International Telecommunication Union, “100 Years of ITU Radio Regulation,” http://www.itu.int/ITU-R/information/promotion/100-years/index.html.

[34] See, for example, Seth Mydans, "Monks are Silenced, and for Now, Internet is, Too," *New York Times*, (4 October 2007), www.nytimes.com/2007/10/04/world/asia/04info.html?emc=eta1.

[35] Box, George E. P.; Norman R. Draper (1987). *Empirical Model-Building and Response Surfaces*. (New Jersey: Wiley, 1987): 424.

[36] Dan Geer, "Measuring Security," 167, http://geer.tinho.net/usenix/measuringsecurity.tutorialv2.pdf.

[37] Geer, "Measuring Security," 129.

[38] Geer, "Measuring Security," 167.

[39] For a good example of Internet attack "noise" see Kaspersky Security Bulletin 2006 by Kaspersky Labs, (7 February 2007), http://www.viruslist.com/en/analysis?pubid=204791921.

[40] For example, see Kelly Jackson Higgins, "Slow And Silent Targeted Attacks On The Rise," Dark Reading, (8 January 2009), http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=212701434.

[41] U.S. Centers for Disease Control and Prevention, "HIV/AIDS Basic Information," http://www.cdc.gov/hiv/topics/basic/index.htm; See also Oren Zaidel and Henry C. Lin, "Uninvited Guests: The Impact of Small Intestinal Bacterial Overgrowth on Nutritional Status," *Nutrition Issues in Gastroenterology*, Series #7.

[42] Geer, "Measuring Security," 129.

[43] *Ibid*., 132.

[44] *Ibid*., 134.

[45] *Ibid*., 143.

[46] Verizon Business RISK Team, "2008 Data Breach Investigations Report," (2008): 22, http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

[47] "Hospital Epidemiology and Infection Control," C. Glen Mayhall, Lippincott Williams & Wilkins, (2004).

[48] Louis Cheng, "Automated 'Bots' Overtake PCs Without Firewalls Within 4 Minutes," (30 November 2004), http://www.avantgarde.com/ttln113004.html.

[49] "Computer Virus Incident Reports," Information Technology Promotion Agency, Japan, http://www.ipa.go.jp/security/english/virus/press/200608/virus200608-e.html.

[50] "The New E-spionage Threat," *Businessweek*, (10 April 2008).

[51] Jeremy Kirk, "Global ATMs affected by malware claims researcher," *TechWorld*, June 8, 2009, http://www.techworld.com/security/news/index.cfm?newsID=117060.

[52] Steve R. White, Jeffrey O. Kephart and David M. Chess, "Computer Viruses, A Global Perspective," section 4.1, "Michelangelo Madness," (1995), http://www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib-node7.html#SECTION00041000000000000000.

[53] Rob Rosenberger, "Michelangelo Fiasco: a Historical Timeline," *VMyths*, (1 June 1992), http://vmyths.com/column/1/1992/6/1/.

[54] For example, see Peter M. Sandman and Jody Lanard, "Swine Flu Risk Miscommunication," *Risk = Hazard + Outrage*, (29 June 2009), http://psandman.com/col/swineflu2.htm.

[55] Evelynn Hammonds, "Infectious Diseases in the 19th-Century City," Annenberg Media, http://www.learner.org/workshops/primarysources/disease/transcript04.html.

[56] Phillip Porras, Hassen Saidi and Vinod Yegneswaran, "An Analysis of Conficker's Logic and Rendezvous Points," SRI International, (19 March 2009), http://mtc.sri.com/Conficker/index.html.

[57] Dan Geer and Scott Charney, "Debate on the Monoculture Threat," (30 June 2004), http://www.usenix.org/event/usenix04/tech/sigs/geer.txt.

[58] "The Red Queen Principle," *Principia Cybernetica Web*, (August 1993), http://pespmc1.vub.ac.be/REDQUEEN.html.

[59] "A History of Computer Viruses," *Viruscan Software*, http://www.virus-scan-software.com/virus-scan-help/answers/the-history-of-computer-viruses.shtml.

[60] "Malware Outbreak Trend Report: Storm-Worm," *Commtouch Software Ltd*, (31 January 2007), http://www.commtouch.com/downloads/Storm-Worm_MOTR.pdf.

[61] Byron Acohido, "The Evolution of an extraordinary globe-spanning worm: Conficker Timeline," *The Last Watchdog on Internet Security*, (25 March 2009), at http://lastwatchdog.com/evolution-conficker-globe-spanning-worm/.

[62] "WHO raises pandemic alert to second-highest level," CNN, (30 April 2009), http://www.cnn.com/2009/HEALTH/04/29/swine.flu/index.html.

[63] Phillip Porras, et al., "An Analysis of Conficker's Logic and Rendezvous Points," *SRI International*, (19 March 2009), http://mtc.sri.com/Conficker/.

[64] "Conficker as seen from the UCSD Network Telescope," *CAIDA*, http://www.caida.org/research/security/ms08-067/conficker.xml.

[65] "Simple steps to protect yourself from the Conficker Worm," *Symantec*, http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2009033012483648; See also "Conficker Timeline, Conficker Working Group," http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline.

[66] "Swine Flu Events Around The World," *MSNBC*, http://www.msnbc.msn.com/id/30624302/ns/health-cold_and_flu.

[67] Phillip Porras, et al., *An Analysis of Conficker's Logic and Rendezvous Points, SRI International*, (19 March 2009), http://mtc.sri.com/Conficker.

[68] *Ibid*.

[69] "Conficker C Analysis," *SRI International*, http://mtc.sri.com/Conficker/addendumC/.

[70] Smith GJ, Vijaykrishna D, Bahl J, Lycett SJ, Worobey M, Pybus OG, Ma SK, Cheung CL, Raghwani J, Bhatt S, Peiris JS, Guan Y, Rambaut A (June 11, 2009). "Origins and evolutionary genomics of the 2009 swine-origin H1N1 influenza A epidemic." *Nature*, 459 (7250): 1122–5. doi:10.1038/nature08182.

[71] Taubenberger, Jeffrey K., and Morens, David M. “1918 Influenza: The Mother of all Pandemics,” *Emerging Infectious Diseases* Vol. 12 No.1 (January 2006), http://www.cdc.gov/NCIDOD/EID/vol12no01/05-0979.htm.

[72] “Thermal camera placed at Istanbul airport to prevent swine flu,” *Xinhua*, (29 April 2009), http://news.xinhuanet.com/english/2009-04/29/content_11280748.htm.

[73] Kim Willsher, “French fighter planes grounded by computer worm,” *The Daily Telegraph*, http://telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html, (Accessed 1 April 2009).

[74] For example, the European Union recommended travelers to postpone trips to the U.S. and Mexico, “Europeans urged to avoid Mexico and U.S. as swine flu death toll exceeds 100,” *Guardian*, (27 April 2009).

[75] Hong Kong kept nearly 300 people for seven days in a Wanchai hotel, the Metropark, which gathered international reporters outside. Taxis would routinely avoid streets nearby to avoid the spot, which also had a role in the earlier SARS outbreak. See Sophie Leung, “Hong Kong Lifts Swine Flue Quanrantine on 351 People,” *Bloomberg*, (8 May 2009), http://www.bloomberg.com/apps/news?pid=20601087&sid=aO8D7j8zVdWA.

[76] United States Computer Emergency Readiness Team, “Technical Cyber Security Alert TA08-297A,” (29 October 2008), http://www.us-cert.gov/cas/techalerts/TA08-297A.html.

[77] Jim Giles, “The inside story of the Conficker worm,” *The New Scientist*, (12 June 2009), http://www.newscientist.com/article/mg20227121.500-the-inside-story-of-the-conficker-worm.html?full=true.

[78] Microsoft, “Microsoft Collaborates With Industry to Disrupt Conficker Worm,” (12 February 2009), http://www.microsoft.com/Presspass/press/2009/feb09/02-12ConfickerPR.mspx.

[79] Conficker Working Group, “FAQ – Announcement of Working Group,” http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/FAQ.

[80] World Health Organization, “Current WHO phase of pandemic alert,” http://www.who.int/csr/disease/avian_influenza/phase/en/index.html.

[81] World Health Organization, “History of WHO,” http://www.who.int/about/history/en/index.html.

[82] Center for Infectious Disease Preparedness, “Conducting an Outbreak Investigation in 7 Steps (or less),” UC Berkeley School of Public Health, (June 2006), http://www.idready.org/slides/03outbreak-notes.pdf.

[83] *Ibid*.

[84] Verizon 2008 Data Breach Investigations Report, 3 and 23.

[85] The National Institute of Allergy and Infectious Diseases, “Immunity: Natural and Acquired,” http://www3.niaid.nih.gov/topics/immuneSystem/immunity.htm.

[86] For an extended analogy of the similarities between the human immune system and cyber defense, see Martin Libicki, “Postcards from the Immune System,” *Defending Cyberspace and Other Metaphors* (Institute for National Strategic Studies), (1997).

[87] Geer, “Measuring Security,” 164.

[88] *Ibid*., 165.

[89] Barabasi, *Linked*, 34.

[90] Dan Geer and Scott Charney, “Debate on the Monoculture Threat.”

[91] Geer, “Measuring Security,” 162.

[92] *Ibid*., 162.

[93] “Egypt orders slaughter of all pigs over swine flu,” *MSNBC*, (29 April 2009), http://www.msnbc.msn.com/id/30480507/.

[94] Michael Bailey, et. al, “The Blaster Worm: Then and Now,” *IEEE Security & Privacy*, Vol.3 No. 4 (July 2005): 26-31.

[95] Geer, “Measuring Security,” 160.

[96] For a discussion of the Chinese response to SARS, see Ellen Bork, “China’s SARS Problem, and Ours,” *The Weekly Standard*, (4 April 2003), http://www.weeklystandard.com/Content/Public/Articles/000/000/002/504jlpnl.asp; for information about the Chinese response to avian and swine flu, see “China to help ASEAN countries in fighting bird flu,” *Xinhua*, (12 December 2005), http://www.chinadaily.com.cn/english/doc/2005-12/12/content_502767.htm.

[97] The Internet Storm Center, The SANS Institute, for more information, see http://isc.sans.org/ *See also*, The ShadowServer Foundation, for more information, see http://www.shadowserver.org/ *See also*, Baker, Wade H., Hylender, C. David, Valentine, J. Andrew, “2008 Data Breach Investigations Report,” Verizon Business Risk Team *See also*, Virus Radar Online, ESET, LLC, for more information, see http://www.virusradar.com/.

[98] Raffles Medical Group, “What is DORSCON,” http://www.rafflesmedicalgroup.com/web/Contents/Contents.aspx?ContId=1196.

[99] World Health Organization, “Current WHO phase of pandemic alert,” http://www.who.int/csr/disease/avian_influenza/phase/en/index.html.

[100] “Multi-State ISAC Procedures and Protocols for Cyber Alert Indicator,” *Multi-State Information Sharing and Analysis Center*, http://www.msisac.org/alertlevel/.

[101] “Security Response,” *Symantec*, http://www.symantec.com/business/security_response/index.jsp#.

[102] Information Storm Center, “Infocon,” http://isc.sans.org/infocon.html.

[103] “Conducting an Outbreak Investigation in 7 Steps (or less),” Center for Infectious Disease Preparedness UC Berkeley School of Public Health.

[104] “Working for Health — An Introduction to the World Health Organization,” http://www.who.int/about/brochure_en.pdf.

[105] World Health Organization, “Global Alert and Response,” http://www.who.int/csr/alertresponse/en/.

[106] World Health Organization, "Global Outbreak Alert and Response Network," http://www.who.int/csr/outbreaknetwork/en/.

[107] For example, see "Emergency Preparedness and Response: What CDC Is Doing," Centers for Disease Control and Prevention, http://www.bt.cdc.gov/cdc/.

[108] Agency for Healthcare Research and Quality, "Community-Based Mass Prophylaxis: A Planning Guide for Public Health Preparedness," http://www.ahrq.gov/research/cbmprophyl/. *See also*, Centers for Disease Control and Prevention, "Smallpox: Preparation and Planning," http://www.bt.cdc.gov/agent/smallpox/prep/.

[109] California Department of Public Health, "Strategic Plan, 2008 – 2010," http://www.cdph.ca.gov/Documents/CDPH-Strategic-Plan.pdf.

[110] Coordinating Office for Terrorism Preparedness and Emergency Response (COTPER), Funding Guidance and Technical Assistance to States, U.S. Centers for Disease Control and Prevention, http://www.bt.cdc.gov/cotper/coopagreement.

[111] "Introducing the National Response Framework," United States Department of Homeland Security, http://www.fema.gov/pdf/emergency/nrf/about_nrf.pdf.

[112] "National Incident Management System," United States Department of Homeland Security, http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.

[113] Robert McMillan "Group Takes Conficker Fight To New Level," *IDG News Service* (1 April 2009).

[114] "About Us," US-CERT, December 2009, http://www.us-cert.gov/aboutus.html.

[115] Albert-Laszlo Barabasi and Eric Bonabeau, "Scale-Free Networks," *Scientific American*, (May 2003).

[116] CSIS, http://csis.org/program/commission-cybersecurity-44th-presidency, 45.

[117] John Markoff, "Internet Traffic Begins to Bypass the U.S.," *The New York Times*, (29 August 2008), http://www.nytimes.com/2008/08/30/business/30pipes.html.

[118] For example, during the Red Flag exercises organized by the 414th Combat Training Squadron, http://www.acc.af.mil/library/factsheets/factsheet.asp?id=7359.

[119] The need for development of cyber deterrence strategy was addressed in both the CSIS Commission report on *Securing Cyberspace* for the 44th Presidency and the 2009 White House Cyber Review.

[120] From a good collection of contemporaneous press reports, http://www.informationwar.org/2001/china/new.htm.

[121] *Ibid*.

[122] Ethnic Russians protested in Estonia and with cyber attacks over the removal of a statue of a WWII Russian solider. See NATO Cooperative Cyber Defense Center of Excellence, "International Cyber Incidents: Legal Considerations," 23.

[123] *Ibid*, 15.

[124] In Estonia, there were strong pro-Russian protests with one person killed and hundreds injured and arrested: "Tallinn tense after deadly riots," *BBC News*, (28 April 2007), http://news.bbc.co.uk/2/hi/europe/6602171.stm.

[125] For example, the Russian Parliament threatened to impose sanctions against Estonia: Laura Sheeter, "Russia slams Estonia statue move," *BBC News*, (17 January 2007), http://news.bbc.co.uk/2/hi/europe/6273117.stm.

[126] NATO Cooperative Cyber Defense Center of Excellence, "International Cyber Incidents: Legal Considerations," Draft version, (2009): 29.

[127] From the Center for Strategic and International Studies report, *Securing Cyberspace for the 44th Presidency*, (December 2008): 27.

[128] AFP, 23 January 2008, from http://afp.google.com/article/ALeqM5i0glFFpGvkJZDF-b21ieCDc2HbYQ, (Accessed 8 November 2009).

[129] As the U.S. Cyber Consequences Unit has done brilliantly for the attacks against Georgia in their "Overview by the USCCU of the Cyber Campaign Against Georgia in August of 2008." John Bumgarner and Scott Borg, (August 2009).

[130] Though the U.S. has announced we have or will conduct attacks, they are rare and controlled.

[131] See for example, the U.S. Cyber Consequence Unit, "Overview by the USCCU of the Cyber Campaign Against Georgia in August of 2008," (2009).

CHAPTER VI:
POWER PLAYS IN THE INDIAN OCEAN: THE MARITIME COMMONS IN THE 21ST CENTURY

By Robert D. Kaplan

As the pirate activity off the coast of Somalia and the terrorist carnage in Mumbai last fall suggest, the Indian Ocean — the world's third-largest body of water — already takes center stage for the challenges of the 21st century.

POWER PLAYS IN THE INDIAN OCEAN: THE MARITIME COMMONS IN THE 21ST CENTURY

By Robert D. Kaplan

Maps often form—and reinforce—our conceptual views of geopolitics. The right map can stimulate foresight by providing a spatial view of critical trends. Fifty years before the end of World War II, naval strategist Alfred Thayer Mahan predicted the Cold War significance of naval forces and their strategic importance in the Atlantic and Pacific oceans:

> …We must be an effective naval force in the Pacific. We must similarly be an effective force on the Atlantic; not for the defense of our coasts primarily, or immediately, as is commonly thought—for in warfare, however much in the defense of right, the navy is not immediately an instrument of defense but of offense.[1]

Almost 65 years after World War II, Americans continue to concentrate on the Atlantic and Pacific oceans because of their country's geographic circumstances. World War II and the Cold War shaped this outlook: Nazi Germany, imperial Japan, the Soviet Union, and Communist China were each oriented toward one of these two oceans, much as Mahan predicted in 1905.

The bias towards the Atlantic and Pacific oceans is even embedded in mapping conventions: Mercator projections tend to place the Western Hemisphere in the middle of the map, splitting the Indian Ocean at its far edges. Throughout the 20th century, the focus on maritime security remained on protecting the movement of commerce across these two oceans. And yet, as the pirate activity off the coast of Somalia and the terrorist carnage in Mumbai last fall suggest, the Indian Ocean—the world's third-largest body of water—already takes center stage for the challenges of the 21st century.

Understanding the map of Europe was essential to understanding the 20th century. Although recent technological advances and economic integration have fostered global thinking, some places continue to hold more importance than others. And

This chapter draws from Robert Kaplan, "Center Stage for the 21st Century," *Foreign Affairs,* (March/April 2009).

in some of those, such as Iraq and Pakistan, two countries with inherently artificial contours, politics is still at the mercy of geography.

So, in what quarter of the Earth today can one best glimpse the future? The greater Indian Ocean region encompasses the entire arc of Islam, from the Sahara desert to the Indonesian archipelago. Although the Arabs and the Persians are known to Westerners primarily as desert people, they have also been great seafarers. In the Middle Ages, they sailed from Arabia to China; proselytizing along the way, they spread their faith through sea-based commerce. Today, the western reaches of the Indian Ocean include the tinderboxes of Somalia, Yemen, Iran, and Pakistan—constituting a network of dynamic trade as well as a network of global terrorism, piracy, and drug smuggling. Hundreds of millions of Muslims, the legacy of those medieval conversions, live along the Indian Ocean's eastern edges, in India and Bangladesh, Malaysia and Indonesia.

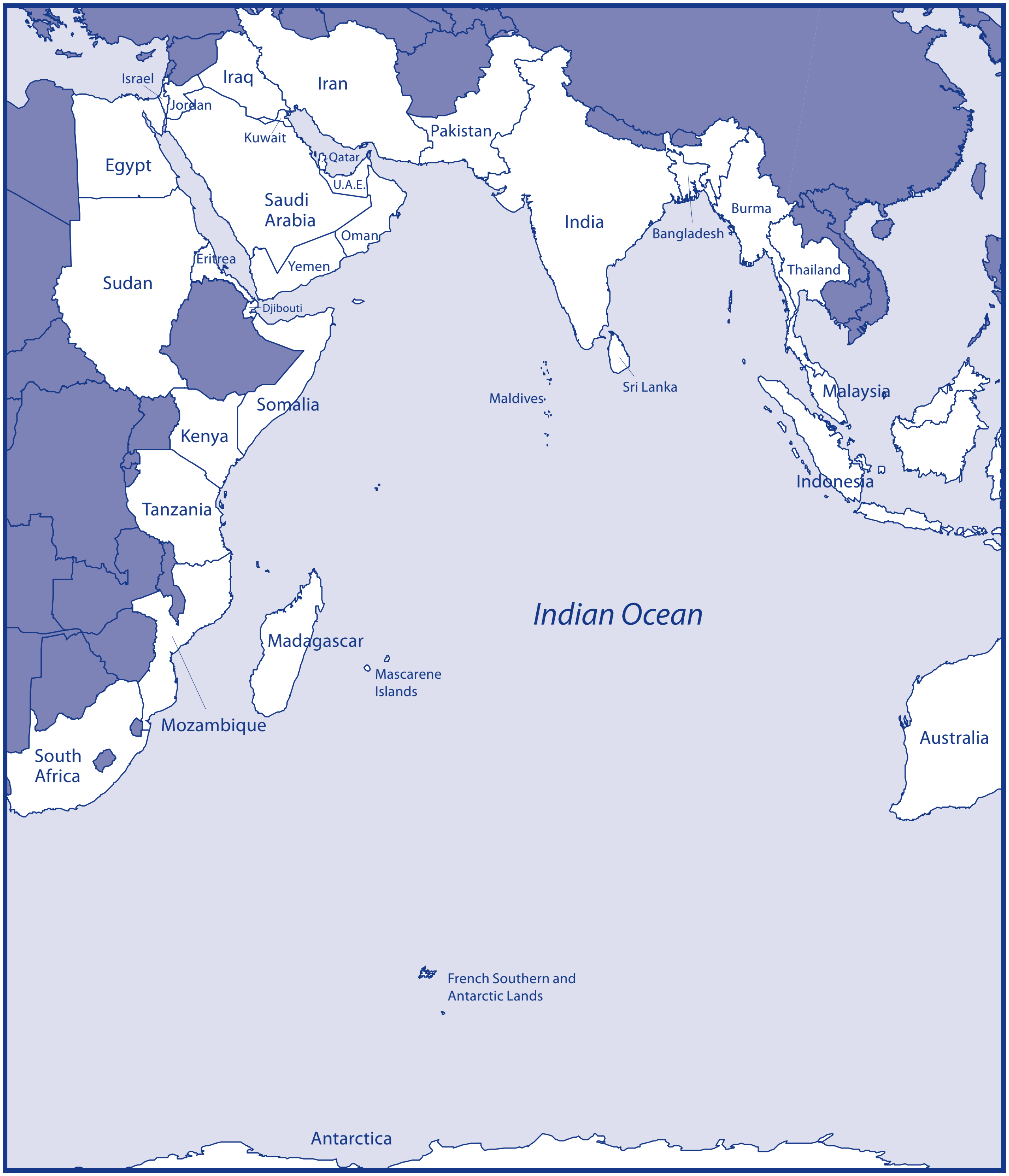
The Indian Ocean is dominated by two immense bays, the Arabian Sea and the Bay of Bengal, near the north of which are two of the least stable countries in the world: Pakistan and Myanmar (also known as Burma). State collapse or regime change in Pakistan would affect its neighbors by empowering Baluchi and Sindhi separatists seeking closer links to India and Iran. Likewise, the collapse of the junta in Myanmar, where competition over energy and natural resources between China and India looms, would threaten economies nearby and require a massive seaborne humanitarian intervention. On the other hand, the advent of a more liberal regime in Myanmar would undermine China's dominant position there, boost Indian influence, and quicken regional economic integration.

Yet this is still an environment in which the United States will have to keep the peace and help guard the global commons—interdicting terrorists, pirates, and smugglers; providing humanitarian assistance; and managing the competition between India and China. It will have to do so not—as in Afghanistan and Iraq—as a land-based, in-your-face meddler, leaning on far-flung army divisions at risk of getting caught up in sectarian conflict, but as a sea-based balancer lurking just over the horizon. Sea power has always been less threatening than land power. As the cliché goes, navies make port visits, and armies invade. Ships take a long time to get to a war zone, allowing diplomacy to work its magic. And as the U.S. response to the 2004 tsunami in the Indian Ocean showed, with most sailors and marines returning to their ships each night, navies can exert great influence on shore while leaving a small footprint. The more the United States becomes a maritime hegemon, as opposed to a land-based one, the less threatening it will seem to others.

Moreover, as India and China emphasize their sea power, the job of managing their peaceful rise will fall on the U.S. Navy, to a significant extent. There will surely be tensions between the three navies, especially as the gaps in their relative strength begin to close. But even if the comparative size of the U.S. Navy decreases in the decades ahead, the United States will remain the one great power from outside the Indian Ocean region with a major presence there. It is a unique position that will give it the leverage to act as a broker between India and China in their own backyard. To understand this dynamic, one must look at the region from a maritime perspective.

Sea Changes

Throughout history, sea routes have mattered more than land routes, writes the historian Felipe Fernández-Armesto, because they carry more goods more economically. "Whoever is lord of Malacca has his hand on the throat of Venice," went one saying in the late 15th century, alluding to the city's extensive commerce with Asia. "If the world were an egg, Hormuz would be its yolk," *Indian Ocean Area*



went another. Even today, in the jet and information age, 90 percent of global commerce and about 65 percent of all oil travel by sea. Globalization has been made possible by the cheap and easy shipping of containers on tankers, and the Indian Ocean accounts for half the world's container traffic. Moreover, 70 percent of the total traffic of petroleum products passes through the Indian Ocean, on its way from the Middle East to the Pacific. As these goods travel that route, they pass through the world's principal oil shipping lanes, including the gulfs of Aden and Oman—as well as some of world commerce's main chokepoints: Bab el Mandeb and the straits of Hormuz and Malacca. Forty percent of world trade passes through the Strait of Malacca; 40 percent of all traded crude oil passes through the Strait of Hormuz.

70 percent of the total traffic of petroleum products passes through the Indian Ocean, on its way from the Middle East to the Pacific.

Already the world's preeminent energy and trade interstate seaway, the Indian Ocean will matter even more in the future. Global energy needs are expected to rise by 45 percent between 2006 and 2030, and almost half of the growth in demand will come from India and China.[2] China's demand for crude oil doubled between 1995 and 2005[3] and will double again in the coming 15 years or so.[4] By 2030, China is expected to import 8.1 million barrels of crude per day—half of Saudi Arabia's planned output. More than 85 percent of the oil and oil products bound for China cross the Indian Ocean and pass through the Strait of Malacca.[5]

India—soon to become the world's fourth-largest energy consumer, after the United States, China, and Japan—depends on oil for about 31 percent of its energy needs, 68 percent of which it imports. Ninety percent of its oil imports could soon come from the Persian Gulf. India must satisfy a population that will, by 2030, be the largest of any country in the world.[6] Its coal imports from far-off Mozambique are set to increase substantially, adding to the coal that India already imports from other Indian Ocean countries, such as South Africa, Indonesia, and Australia. In the future, India-bound ships will also be carrying increasingly large quantities of liquefied natural gas (LNG) across the seas from southern Africa, even as it continues importing LNG from Qatar, Malaysia, and Indonesia.

As the whole Indian Ocean seaboard, including Africa's eastern shores, becomes a vast web of energy trade, India is seeking to increase its influence from the Plateau of Iran to the Gulf of Thailand—an expansion west and east meant to span the zone of influence of the Raj's viceroys. India's trade with the Arab countries of the Persian Gulf, as well as Iran, with which India has long enjoyed close economic and cultural ties, is booming. Approximately 4.3 million Indians work in the six Arab states of the Gulf Cooperation Council and send home more than 9.5 billion dollars in remittances annually.[7] As India's economy continues to grow, so will its trade with Iran and, once the country recovers, Iraq. Iran, like Afghanistan, has become a strategic rear base for India against Pakistan, and it is poised to become an important energy partner. In 2005, India and Iran signed a multibillion-dollar deal under which Iran will supply India with 7.5 million tons of LNG annually for 25 years, beginning in 2009. There has been talk of building a gas pipeline from Iran to India through Pakistan, a project that would join the Middle East and South Asia at the hip (and in the process could go a long way toward stabilizing Indian-Pakistani relations). In another sign that Indian-Iranian relations are growing more intimate, India has been helping Iran develop the port of Chah Bahar, on the Gulf of Oman, which will also serve as a forward base for the Iranian Navy.

India has also been expanding its military and economic ties with Myanmar, to the east. Democratic India does not have the luxury of spurning Myanmar's junta because Myanmar is rich in natural resources — oil, natural gas, coal, zinc, copper, uranium, timber, and hydropower — resources in which the Chinese are also heavily invested. India hopes that a network of east-west roads and energy pipelines will eventually allow it to be connected to Iran, Pakistan, and Myanmar.

India is enlarging its navy in the same spirit. With its 169 warships, the Indian Navy is already one of the world's largest, and it expects to add three nuclear-powered submarines and three aircraft carriers to its arsenal by 2017. One major impetus for the buildup was the humiliating inability of its navy to evacuate Indian citizens from Iraq and Kuwait during the 1990–91 Persian Gulf War. Another is what Mohan Malik, a scholar at the Asia-Pacific Center for Security Studies, in Hawaii, has called India's "Hormuz dilemma," referring to its dependence on imports passing through the strait, close to the shores of Pakistan's Makran coast, where the Chinese are helping the Pakistanis develop deep-water ports.

Indeed, as India extends its influence east and west, on land and at sea, it is bumping into China, which, also concerned about protecting its interests throughout the region, is expanding its reach southward. Chinese President Hu Jintao has bemoaned China's "Malacca dilemma." The Chinese government hopes eventually to be able to partly bypass that strait by transporting oil and other energy products via roads and pipelines from ports on the Indian Ocean into the heart of China. One reason that Beijing wants desperately to integrate Taiwan into its dominion is so that it can redirect its naval energies away from the Taiwan Strait and toward the Indian Ocean.[8]

According to some reports, the Chinese government has adopted a so-called "string of pearls" strategy for the Indian Ocean, which reportedly consists of setting up a series of ports in friendly countries along the ocean's northern seaboard. China has built a large deep-water port and possible listening post in Gwadar, Pakistan, from which it may already be monitoring ship traffic through the Strait of Hormuz. In addition, China may be building a port in Pasni, Pakistan, 75 miles east of Gwadar, which is to be joined to the Gwadar facility by a new highway; a fueling station on the southern coast of Sri Lanka; and a container facility with extensive naval and commercial access in Chittagong, Bangladesh. Beijing reportedly operates surveillance facilities on islands deep in the Bay of Bengal. In Myanmar, where the junta gets billions of dollars in military assistance from Beijing, the Chinese are constructing or upgrading commercial and naval bases and building roads, waterways and pipelines to link the Bay of Bengal to the southern Chinese province of Yunnan. Some of these facilities are closer to cities in central and western China than those cities are to Beijing and Shanghai, so building road and rail links from these facilities into China could serve to spur the economies of China's landlocked provinces. The Chinese government also envisions a canal across the Isthmus of Kra, in Thailand, to link the Indian Ocean to China's Pacific coast — a project on the scale of the Panama Canal that could further tip Asia's balance of power in China's favor by giving China's burgeoning navy and commercial maritime fleet easy access to a vast oceanic continuum stretching from East Africa to Japan and the Korean Peninsula.

What the Chinese actually plan for the Indian Ocean remains unclear and open to debate. Indeed, some in Washington are skeptical of the whole notion of a string of pearls strategy. China's reliance on access to foreign resources and markets to support domestic economic development leads China to examine ways to operate in the Indian Ocean to protect its vital sea links. Beijing may not necessarily follow the British and American examples of establishing overseas coaling stations or bases. Rather, China may be planning a series of ports in friendly countries along the ocean's northern seaboard with the capability to supply Chinese forces with fuel, food, and spare parts. The Chinese are not seeking outright control, preferring, in the example of Gwadar, to stand by as Singapore-based PSA International operates the facility. Nevertheless, geography and China's deep historical ties to the Indian Ocean region in medieval and early modern history suggest more. Visiting the port construction site in southern Sri Lanka and observing Chinese workers there, I was detained for hours in a jail by Sri Lankan authorities that appeared to be quite sensitive of the site's activities.

It is not the port projects that are critical, per se, for all of them are primarily motivated by domestic politics and local developmental realities that have nothing to do with China. Rather, what is interesting—and therefore bears watching—is the combination of these ongoing construction projects and plans and Beijing's efforts to cultivate strong diplomatic and economic ties with all these littoral countries. Modern port facilities only become meaningful for Beijing if they are in countries where it has good ties. It is a subtle world we are entering: not one of overt military bases like during the Cold War, but one of dual-use civil-military facilities and implicit rather than explicit bilateral agreements. Nor is anything China is doing a threat to the United States.

Yet, all of these activities are unnerving for the Indian government. With China building deep-water ports to its west and east and a preponderance of Chinese arms sales going to Indian Ocean states, India fears being encircled by China unless it expands its own sphere of influence. The two countries' overlapping commercial and political interests are fostering competition, even more in the naval realm than on land. Zhao Nanqi, former director of the General Logistics Department of the People's Liberation Army, reportedly proclaimed in 1993, "We can no longer accept the Indian Ocean as an ocean only of the Indians."[9] India has responded to China's naval base project in Gwadar by further developing one of its own in Karwar, India, south of Goa. Meanwhile, Zhang Ming, a Chinese naval analyst, has warned that the 244 islands that form India's Andaman and Nicobar archipelago could be used like a "metal chain" to block the western entrance to the Strait of Malacca, on which China so desperately depends. "India is perhaps China's most realistic strategic adversary," Zhang has written. "Once India commands the Indian Ocean, it will not be satisfied with its position and will continuously seek to extend its influence, and its eastward strategy will have a particular impact on China."[10] These may sound like the words of a professional worrier from China's own theory class, but these worries are revealing: Beijing already considers New Delhi to be a major sea power.

As the competition between India and China suggests, the Indian Ocean is where global struggles will play out in the 21st century. The old borders of the Cold War map are crumbling fast, and Asia is becoming a more integrated unit, from the Middle East to the Pacific. South Asia has been an indivisible part of the greater Islamic Middle East since the Middle Ages. It was the Muslim Ghaznavids of eastern Afghanistan who launched raids on India's northwestern coast in the early 11th century; Indian civilization itself is a fusion of the indigenous Hindu culture and the cultural imprint left by these invasions. It took the seaborne terrorist attacks in Mumbai last November to force most Westerners to locate India on a map; to them, the Indian Ocean's entire coast has always constituted one vast interconnected expanse.

What is different now is the extent of these connections. On a maritime-centric map of southern Eurasia, artificial land divisions disappear. Even landlocked Central Asia is related to the Indian Ocean. Natural gas from Turkmenistan may one day flow through Afghanistan, for example, en route to Pakistani and Indian cities and ports, one of several possible energy links between Central Asia and the Indian subcontinent. Both the Chinese port in Gwadar, Pakistan, and the Indian port in Chah Bahar, Iran, may eventually be connected to oil- and natural-gas-rich Azerbaijan, Kazakhstan, Turkmenistan, and other former Soviet republics. S. Frederick Starr, a Central Asia expert at the Johns Hopkins School of Advanced International Studies, said at a conference in Washington last year that access to the Indian Ocean "will help define Central Asian politics in the future." Others have called ports in India and Pakistan "evacuation points" for Caspian Sea oil. The destinies of countries even 1,200 miles from the Indian Ocean are connected with it.

Elegant Decline

The United States faces three related geopolitical challenges in Asia: the strategic nightmare of the greater Middle East, the struggle for influence over the southern tier of the former Soviet Union, and the growing presence of India and China in the Indian Ocean. The last seems to be the most benign of the three. China is not an enemy of the United States, like Iran, but a legitimate peer competitor, and India is a budding ally. And the rise of the Indian navy, soon to be the third largest in the world after those of the United States and China, will function as an antidote to Chinese military expansion.

The goal of the United States must be to forge a global maritime system that can minimize the risks of interstate conflict while lessening the burden of policing for the U.S. Navy.

The task of the U.S. Navy will therefore be to quietly leverage the sea power of its closest allies—India in the Indian Ocean and Japan in the western Pacific—to set limits on China's expansion. But it will have to do so while seizing every opportunity to incorporate China's navy into international alliances; a U.S.-Chinese understanding at sea is crucial for the stabilization of world politics in the 21st century. After all, the Indian Ocean is a seaway for both energy and hashish and is in drastic need of policing. To manage it effectively, U.S. military planners will have to invoke challenges such as terrorism, piracy, and smuggling to bring together India, China, and others in joint sea patrols. The goal of the United States must be to forge a global maritime system that can minimize the risks of interstate conflict while lessening the burden of policing for the U.S. Navy.

Keeping the peace in the Indian Ocean will be even more crucial once the seas and the coasts from the Gulf of Aden to the Sea of Japan are connected. Shipping options between the Indian Ocean and the Pacific Ocean will increase substantially in the future. The port operator Dubai Ports World was due to release a feasibility study on construction of a land bridge near the canal that the Chinese hope will be dug across the Isthmus of Kra, with ports on either side of the isthmus connected by rails and highways. The Malaysian government is interested in a pipeline network that would link up ports in the Bay of Bengal with those in the South China Sea. To be sure, as sea power grows in importance, the crowded hub around Malaysia, Singapore, and Indonesia will form the maritime heart of Asia: in the coming decades, it will be as strategically significant as the Fulda Gap, a possible invasion route for Soviet tanks into West Germany during the Cold War. The protective oversight of the U.S. Navy there will be especially important. As the only truly substantial blue-water force without territorial ambitions on the Asian mainland, the U.S. Navy in the future may be able to work with individual Asian countries, such as India and China, better than they can work with one another. Rather than ensure its dominance, the U.S. Navy simply needs to make itself continually useful.

It has already begun to make the necessary shifts. Owing to the debilitating U.S.-led wars in Afghanistan and Iraq, headlines in recent years have been dominated by discussions about land forces and counterinsurgency. But with 75 percent of the Earth's population living within 200 miles of the sea, the world's military future may well be dominated by naval (and air) forces operating over vast regions. To a greater extent than the other armed services, navies exist to protect economic interests and the system in which these interests operate. Aware of how much the international economy depends on sea traffic, U.S. admirals are thinking beyond the fighting and winning of wars to responsibilities such as policing a global trading arrangement. They are also attuned to the effects that a U.S. military strike against Iran would have on maritime commerce and the price of oil. With such concerns in mind, the U.S. Navy has for decades been helping to secure vital chokepoints in the Indian Ocean, often operating from a base on the British atoll of Diego Garcia, a thousand miles south of India and close to major sea-lanes. In October 2007, it implied that it was seeking a sustained forward presence in the Indian Ocean and the western Pacific but no longer in the Atlantic—a momentous shift in overall U.S. maritime strategy. *The Marine Corps Vision and Strategy 2025* also concluded that the Indian Ocean and its adjacent waters will be a central theater of global conflict and competition this century.

An F/A-18F Super Hornet assigned to the Strike Fighter Squadron 102, left, and an F/A-18E Super Hornet from Strike Fighter Squadron 27, foreground, fly in formation with two Indian Navy Sea Harriers, bottom, and two Indian Air Force Jaguars, right, over Indian Navy aircraft carrier INS Viraat (R 22) during exercise Malabar 07-2. More than 20,000 personnel from the navies of the United States, Australia, India, Japan and Singapore participated in the exercise.

(MC2 JAROD HODGE/U.S. Navy)

Yet as the challenges for the United States on the high seas multiply, it is unclear how much longer U.S. naval dominance will last. At the end of the Cold War, the U.S. Navy boasted about 600 warships; it is now down to 285. That number might rise to 313 in the coming years with the addition of the new "littoral combat ships," but it could also drop to the low 200s given cost overruns of 27 percent and the slow pace of shipbuilding.[11] The revolution in precision-guided weapons means that existing ships pack better firepower than those of the Cold War fleet did, but a ship cannot be in two places at once. So, the fewer the vessels, the riskier every decision to deploy them. There comes a point at which insufficient quantity hurts quality.

Distance and geography also necessitate greater effort and expense by the U.S. Navy in order to overcome the expeditionary challenge of maintaining presence and influence in the Indian Ocean. While some U.S. Navy warships are forward-deployed, most U.S. warships deploy from homeports within the United States and must for sail several weeks to reach the waters of the Indian Ocean and return home. Once on station, they are sustained by support ships and forward logistics sites around the perimeter of the theater, and they are increasingly reliant on external communications for logistical and administrative needs. To maintain this presence and level of readiness, about 45 percent of U.S. Navy warships are deployed or underway. India, on the other hand, enjoys a front-row seat to the Indian Ocean. It is far less encumbered by the logistical demands required to maintain readiness and project influence from the sea.

Meanwhile, by sometime in the next decade, China's navy will have more warships than the United States'. China is producing and acquiring submarines roughly five times as fast as is the United States.[12] In addition to submarines, the Chinese have wisely focused on buying naval mines, ballistic missiles that can hit moving targets at sea, and technology that blocks signals from GPS satellites, on which the U.S. Navy depends. (The Chinese also have plans to acquire at least one aircraft carrier; not having one hindered their attempts to help with the tsunami relief effort in 2004 and 2005.)

Although the bilateral American-Chinese relationship may in the main be peaceful and productive, a very subtle Cold War of the seas is not out of the question. The South China Sea is full of energy wealth that the Chinese wish to exploit. It is the Pacific gateway to the Indian Ocean. It frustrates the Chinese that the U.S. Navy is present in the South China Sea to such a degree. The goal of the Chinese is "sea denial," or dissuading U.S. carrier strike groups from closing in on the Asian mainland wherever and whenever Washington would like. The Chinese are also more aggressive than U.S. military planners. Whereas the prospect of ethnic warfare has scared away U.S. admirals from considering a base in Sri Lanka, which is strategically located at the confluence of the Arabian Sea and the Bay of Bengal, the Chinese are constructing a refueling station for their warships there.

There is nothing illegitimate about the rise of China's navy. As the country's economic interests expand dramatically, so must China expand its military, and particularly its navy, to guard these interests. The United Kingdom did just that in the 19th century, and so did the United States when it emerged as a great power between the American Civil War and World War I. In 1890, the American military theorist Alfred Thayer Mahan published *The Influence of Sea Power Upon History,* 1660–1783, which argued that the power to protect merchant fleets had been the determining factor in world history. Both Chinese and Indian naval strategists read him avidly nowadays. China's quest for a major presence in the Indian Ocean was also evinced in 2005 by the beginning of an extensive commemoration of Zheng He, the Ming dynasty explorer and admiral who plied the seas between China and Indonesia, Sri Lanka, the Persian Gulf, and the Horn of Africa in the early decades of the 15th century—a celebration that signals China's belief that these seas have always been part of its zone of influence.

At the end of the 19th century the British Royal Navy began to reduce its presence worldwide by leveraging the growing sea power of its naval allies (Japan and the United States). In a similar fashion at the beginning of the 21st century, the United States is beginning an elegant decline by leveraging the growing sea power of allies such as India and

Japan to balance China. What better way to scale back than to give more responsibilities to like-minded states, especially allies that, unlike those in Europe, still cherish military power?

India, for one, is more than willing to help. "India has never waited for American permission to balance [against] China," the Indian strategist C. Raja Mohan remarked in 2006,[13] writing that India has been striving to balance China since the day the Chinese invaded Tibet.[14] Threatened by China's rise, India has expanded its naval presence from as far west as the Mozambique Channel to as far east as the South China Sea. It has been establishing naval staging posts and listening stations on the island nations of Madagascar, Mauritius, and the Seychelles, as well as military relationships with them, precisely in order to counter China's very active military cooperation with these states. With a Chinese-Pakistani alliance taking shape, most visibly in the construction of the Gwadar port, near the Strait of Hormuz, and an Indian naval buildup on the Andaman and Nicobar Islands, near the Strait of Malacca, the Indian-Chinese rivalry is taking on the dimensions of a maritime Great Game.

This is a reason for the United States to quietly encourage India to balance China, even as the United States seeks greater cooperation with China. During the Cold War, the Pacific and Indian oceans were veritable U.S. lakes. But such hegemony will not last, and the United States must seek to replace it with a subtle balance-of-power arrangement. India could emerge as the global pivot state supreme, tilting on some issues toward the United States and on others toward China. If it is accepted that the most important bilateral relationship of the 21st century will be that between the United States and China, then India—because of the size of its population and economy—will emerge as the weathervane of international politics.

Coalition-Builder Supreme

So how exactly does the United States play the role of a constructive, distant, and slowly declining hegemon and keep peace on the high seas in what Fareed Zakaria, the editor of Newsweek International, has called "the post-American world"? Several years ago, Adm. Michael Mullen, then the chief of naval operations (and now chairman of the Joint Chiefs of Staff), said the answer was a "thousand-ship navy… comprised of all freedom-loving nations—standing watch over the seas, standing watch with each other."[15] The term "thousand-ship navy" has since been dropped for sounding too domineering, but the idea behind it remains. Rather than going it alone, the U.S. Navy should be a coalition-builder supreme, working with any navy that agrees to patrol the seas and share information with it. In 2007, the three U.S. maritime services jointly released a new maritime strategy, *A Cooperative Strategy for 21st Century Seapower.* The strategy has been criticized as being less of a complete strategy and more of a strategic vision because it omits a specific long-term shipbuilding plan and a supporting operational concept. While omission may be seen as deficiencies, its deficiencies may have counter-intuitively enabled its strength.

A Cooperative Strategy for 21st Century Seapower was intended to bind U.S. maritime services more closely, but it has had a much stronger impact internationally than at home. Since its debut at the 18th International Seapower Symposium, the world's largest meeting of world naval leaders, the maritime strategy has been highly regarded by international navies for its focus on international cooperation and its assertion that preventing wars is as important as winning wars. *A Cooperative Strategy for 21st Century Seapower* sends an influential strategic message of cooperation.

That cooperation is put into practice in the Indian Ocean. All told, coalition naval forces in the waters in and adjacent to the Indian Ocean now number nearly three dozen ships. Combined Task Force 150 (CTF-151), an international naval task force with logistics facilities at Djibouti, conducts maritime security operations southeast of the Strait of Hormuz, in the Gulf of Aden, Gulf of Oman, in the Arabian Sea, and the Red Sea, and parts of the Indian Ocean. Since 2001, eight nations have commanded CTF-150 and 24 nations have operated as part of the task force.[16] In October 2008, after the capture of a Ukrainian vessel carrying tanks and other military equipment, warships from the United States, Kenya, and Malaysia steamed toward the Gulf of Aden to assist CTF-150, followed by two Chinese warships a few weeks later.

With increased piracy off the coast of Africa, CTF-151 was established as an additional task force in January 2009 specifically to actively deter, disrupt and suppress piracy in order to protect global maritime security and secure freedom of navigation. Recently, Somali pirates ended a seven-month hostage standoff, freeing a Greek cargo ship and its 24 Ukrainian crew for a paid ransom of 2.5 million dollars. In the first nine months of 2009, 114 vessels were boarded by pirates, 34 vessels hijacked, and 88 vessels fired upon.[17] CTF-151 will likely become a permanent fixture because piracy is the maritime ripple effect of land-based anarchy, and for as long as Somalia is in the throes of chaos, pirates operating at the behest of warlords will infest the waters far down Africa's eastern coast.

The task-force model could also be applied to the Strait of Malacca and other waters surrounding the Indonesian archipelago. With help from the U.S. Navy, the navies and coast guards of Malaysia, Singapore, and Indonesia have already combined forces to all but eliminate piracy near the straits in recent years. And with the U.S. Navy functioning as both a mediator and an enforcer of standard procedures, coalitions of this kind could bring together rival countries, such as India and Pakistan or India and China, under a single umbrella. These states' governments would have no difficulty justifying to their publics participating in task forces aimed at transnational threats over which they have no disagreements. Piracy has the potential to unite rival states along the Indian Ocean coastline.

The Indian Ocean shores are lined with weak government and tottering infrastructure, making it necessary for the United States and other countries to transform their militaries. This area represents an unconventional world, a world in which the U.S. military, for one, will have to respond, expeditionary-style, to a range of crises. The problem is not only piracy but also terrorist attacks, ethnic conflicts, cyclones, and floods. For even as the United States' armed forces, and particularly its navy, are in relative decline, they remain the most powerful conventional military on Earth, and they will be expected to lead such emergency responses. With population growth in climatically and seismically fragile zones placing more human beings in danger's way, one deployment will quickly follow another.

It is the variety and recurrence of these challenges that make the map of the Indian Ocean in the 21st century vastly different from the map of the North Atlantic in the 20th century. The latter accentuated a singular threat: the Soviet Union. And it gave the United States a simple focus: to defend Western Europe against the Red Army and keep the Soviet Navy bottled up near the polar icecap. Because the threat was straightforward, and the United States' power was paramount, the U.S.-led North Atlantic Treaty Organization arguably became history's most successful alliance.

One might envision a "NATO of the seas" for the Indian Ocean, composed of South Africa, Oman, Pakistan, India, Singapore, and Australia, with Pakistan and India bickering inside the alliance much as Greece and Turkey have done inside NATO. But that idea fails to capture what the Indian Ocean is all about. Owing to the peripatetic movements of medieval Arab and Persian sailors and the legacies of Portuguese, Dutch, and British imperialists, the Indian Ocean forms a historical and cultural unit. Yet in strategic terms, the Indian Ocean, like the world at large today, has no single focal point. The Gulf of Aden, the Persian Gulf, the Bay of Bengal—all these areas are burdened by different threats involving different players. Today, NATO is a looser alliance, less singularly focused than it was during the Cold War; similarly, any coalition centered on the Indian Ocean should be adapted to the times. Given the ocean's size—it stretches across seven time zones and almost half of the world's latitudes—and the comparative slowness at which ships move, it would be a challenge for any one multinational navy to get to a crisis zone in time. The United States was able to lead the relief effort off the coast of Indonesia after the 2004 tsunami only because the carrier strike group USS Abraham Lincoln happened to be in the vicinity and not in the Korean Peninsula, where it was headed.

A better approach would be to rely on multiple regional and ideological alliances in different parts of the Indian Ocean. Some such efforts have already begun. The navies of Thailand, Singapore and Indonesia have banded together to deter piracy in the Strait of Malacca; those of the United States, India, Singapore, and Australia have exercised together off India's southwestern coast (an implicit rebuke to China's designs in the region). According to Vice Adm. John Morgan, former deputy chief of U.S. naval operations, the Indian Ocean strategic system should be like the New York City taxi system: driven by market forces and with no central dispatcher. Coalitions will naturally form in areas where shipping lanes need to be protected, much as taxis gather in the theater district before and after performances. As one Australian commodore interviewed by the author put it, the model should be a network of artificial sea bases supplied by the U.S. Navy, which would allow for different permutations of alliances. Frigates and destroyers from various states could "plug and play" into these sea bases as necessary and spread out from East Africa to the Indonesian archipelago.

Like a microcosm of the world at large, the greater Indian Ocean region is developing into an area of both ferociously guarded sovereignty (with fast-growing economies and militaries) and astonishing interdependence (with its pipelines and land and sea routes). And for the first time since the Portuguese onslaught in the region in the early 16th century, the West's power there is in decline, however subtly and relatively. The Indians and the Chinese will enter into a dynamic great-power rivalry in these waters, with their shared economic interests as major trading partners locking them in an uncomfortable embrace. The United States, meanwhile, will serve as a stabilizing power in this newly complex area. Indispensability, rather than dominance, must be its goal.

Without a strong U.S. diplomatic, economic, and military presence in Asia and the Indian Ocean, the region would be far less stable and at the mercy of tensions between dynamically growing and

Without a strong U.S. diplomatic, economic, and military presence in Asia and the Indian Ocean, the region would be far less stable and at the mercy of tensions between dynamically growing and highly nationalistic states.

highly nationalistic states. Here is the heartland of the world economy in the 21st century, which affects everyone's standards of living, so all must care what happens here. America's presence is crucial to keeping this region at peace so that it can develop further, into a vital intersection point of energy transfers. The United States will be more important than ever in keeping the peace.

ENDNOTES

[1] Alfred Thayer Mahan. The Problem of Asia and Its Effect upon International Policies (Boston, MA: Little, Brown, and Company, 1905), 64.

[2] International Energy Agency, "World Energy Outlook 2007," Paris (2007).

[3] U.S. Energy Information Administration, "International Energy Statistics," http://tonto.eia.doe.gov/cfapps/ipdbproject/iedindex3.cfm?tid=5&pid=54&aid=2&cid=CH,&syid=1995&eyid=2008&unit=TBPD&products=54. (Accessed 14 December 2009).

[4] U.S. Energy Information Administration, "World Oil Consumption by Region, Reference Case, 1990-2030," http://www.eia.doe.gov/oiaf/ieo/pdf/ieoreftab_4.pdf. (Accessed 15 December 2009).

[5] U.S. Energy Information Administration, "China Energy Data, Statistics and Analysis," http://www.eia.doe.gov/emeu/cabs/China/Full.html. (Accessed 15 December 2009).

[6] U.S. Energy Information Administration, "India Energy Data, Statistics and Analysis," http://www.eia.doe.gov/emeu/cabs/India/Full.html. (Accessed 15 December 2009).

[7] The World Bank, "South-South Migration and Remittances," http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTDECPROSPECTS/0,,contentMDK:21154867~pagePK:64165401~piPK:64165026~theSitePK:476883~isCURL:Y,00.html. (Accessed 15 December 2009).

[8] James R. Holmes and Toshi Yoshihara, "China and the United States in the Indian Ocean: an Emerging Strategic Triangle?" *Naval War College Review*, 61 (Summer 2008).

[9] Ramtanu Maitra, "India-US Security: All at Sea in the Indian Ocean," *Asia Times*, (6 December 2007).

[10] 章明 [Zhang Ming], "马六甲困局与中国海军的战略抉择" [The Malacca Dilemma and the Chinese Navy's Strategic Choices], 现代舰船 [Modern Ships], no. 274 (October 2006).

[11] Government Accountability Office, *Best Practices: High Levels of Knowledge at Key Points Differentiate Commercial Shipbuilding from Navy Shipbuilding*, (13 May 2009): 30.

[12] Congressional Research Service, *China Naval Modernization: Implications for U.S. Navy Capabilities — Background and Issues for Congress*, by Ronald O'Rourke, (21 October 2009): 7.

[13] C. Raja Mohan, remarks at Council on Foreign Relations, (19 June 2006), http://www.cfr.org/publication/11013/will_india_become_a_global_power_transcript_federal_news_service_inc.html.

[14] Mohan, "India and the Balance of Power," *Foreign Affairs*, 85 (July/August 2006): 17.

[15] Adm Michael Mullen, remarks as delivered to the Naval War College, (August 31, 2005), http://www.navy.mil/navydata/cno/speeches/mullen050831.txt. (Accessed 15 December 2009).

[16] See U.S. Navy, "Combined Task Force 150." Available at http://www.cusnc.navy.mil/command/ctf150.html. (Accessed 10 December 2009).

[17] International Chamber of Commerce Commercial Crime Services, See "Unprecedented Increase in Somali Pirate Activity," International Chamber of Commerce Commercial Crime Services, (21 October 2009). http://www.icc-ccs.org/index.php?option=com_content&view=article&id=376:unprecedented-increase-in-somali-pirate-activity&catid=60:news&Itemid=51. (Accessed 10 December 2009).

Appendix

APPENDIX A: CONTESTED COMMONS WORKING GROUPS

STRATEGIC REVIEW WORKING GROUP

Shawn Brimley
OSD Policy

COL Ross Brown (USA)
CNAS

CDR Herb Carmen (USN)
CNAS

David Cattler
National Intelligence Council

Dr. Patrick Cronin
CNAS

Dr. Thomas P. Ehrhard
Office of the Chief of Staff of the U.S. Air Force

Richard Fontaine
CNAS

LtCol Jeffrey Goodess (USMC)
CNAS

Dr. Kristin Lord
CNAS

Dr. Thomas G. Mahnken
Johns Hopkins University, SAIS

Lt Col Kelly Martin (USAF)
CNAS

Dr. John Nagl
CNAS

MARITIME COMMONS WORKING GROUP

Shawn Brimley
OSD Policy

David Cattler
National Intelligence Council

Bryan Clark
OPNAV QDR Integration Group

Michael Cortese

Dr. Thomas P. Ehrhard
Office of the Chief of Staff of the U.S. Air Force

Mark Gorenflo
Department of the Navy

CAPT Ronald Harris, USN (ret.)
The Lockheed Martin Corporation

Dr. Kristin Lord
CNAS

Dr. Thomas Mahnken
Johns Hopkins University, SAIS

CDR Brian McGrath, USN (ret.)

CAPT Mark Montgomery

OPNAV N3/5

LT Emelia Spencer Probasco, USN

Office of the Chief of Naval Operations

Marty Simon

Rear Admiral James Stark, USN (ret.)

CAPT Bruce Stubbs, USCG (ret.)

Professor Milan Vego
U.S. Naval War College

CAPT Stanley Weeks, USN (ret.)
U.S. Naval War College

Dr. Richard Weitz
CNAS

AIR CHAPTER WORKING GROUP

Dr. Tom Ehrhard
Office of the Chief of Staff of the U.S. Air Force

Lt Col Patrick Goodman
Air Force Strategy Development and Integration, USAF HQ

Michael Isherwood
Northrop Grumman Analysis Center

Manny Fernandez
Textron Inc.

Col John Riordan
Space Operation, USAF HQ

SPACE COMMONS WORKING GROUP

Robert Butterworth
Strategic Planning, Policy and Doctrine, USAF Space Command

Josh Hartman
Independent Consultant

Kevin LeClaire
ISDR Consulting

Dr. Scott Pace
George Washington University

Ian Pryke
George Mason University

Col. John Riordan
Space Operations, USAF HQ

CYBER COMMONS WORKING GROUP

John Davis
Joint Task Force, Global Network Operations

Tony Sager
National Cyber Security Center

Herb Lin
National Academy of Sciences

Paul Kurtz
Good Harbor Consulting

Bob Butler
SBC Global

Bob Lentz
OSD Policy

Philip Reitinger
Department of Homeland Security

Chris Painter
National Security Council

(No chapter 6/Indian Ocean working group)

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic, and principled national security and defense policies that promote and protect American interests and values. Building on the expertise and experience of its staff and advisors, CNAS aims to engage policymakers, experts and the public with innovative fact-based research, ideas, and analysis to shape and elevate the national security debate. A key part of our mission is to help inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, DC, and was established in February 2007 by Co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501c3 tax-exempt nonprofit organization. Its research is nonpartisan; CNAS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

Center for a New American Security
1301 Pennsylvania Avenue, NW
Suite 403
Washington, DC 20004

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org
www.cnas.org

Production Notes

Paper recycling is reprocessing waste paper fibers back into a usable paper product.

Soy ink is a helpful component in paper recycling. It helps in this process because the soy ink can be removed more easily than regular ink and can be taken out of paper during the de-inking process of recycling. This allows the recycled paper to have less damage to its paper fibers and have a brighter appearance. The waste that is left from the soy ink during the de-inking process is not hazardous and it can be treated easily through the development of modern processes.

PRINTED WITH SOY INK™

Design by CRABTREE + CO

Center for a
New American
Security

STRONG, PRAGMATIC AND PRINCIPLED
NATIONAL SECURITY AND DEFENSE POLICIES

1301 Pennsylvania Avenue, NW
Suite 403
Washington, DC 20004

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org

www.cnas.org

$39.99
ISBN 978-193508721-2
52999>
9 781935 087212

PRINTED WITH SOY INK™ Printed on Post-Consumer Recycled paper with Soy Inks