Gabriel M. Scheinmann and Raphael S. Cohen

The Myth of "Securing the Commons"

Not since President George W. Bush uttered the words "axis of evil" has a strategic phrase generated as much Beltway buzz as "securing the commons." One of the few points of agreement between President Obama's 2010 National Security Strategy, the 2010 Quadrennial Defense Review, the neoconservative Project for the New America's Century's "Rebuilding American Defense" report, various NATO research papers, and numerous think tank publications is that they all emphasize the importance of "safeguarding the global commons."[1]

And yet, what does that mean? Herein lies the problem: the term has multiple and often contradictory meanings. For the extreme left, it connotes imperialist designs; while to liberal institutionalists it means good world citizenry. To many realists, it is synonymous with overreach; while to conservatives it signals proper hegemonic activity. To the World Bank, it means protecting the world from global environmental challenges,[2] while to others it refers to sustaining American hard power in the post-Cold War era.[3] Even the term "commons" is defined by what it is not—namely, owned by any one individual—than by what it actually is. In other words, despite its prevalence in contemporary strategic literature, what "securing the commons" means as a strategy remains undefined.

The uncertainty of the term has misled and misinformed the crucial strategic debate surrounding the role of the United States in today's global affairs. In an era of runaway budget deficits, defense budget cuts, and the rise of China, an examination of America's ability to remain a global hegemon is in full swing. By misconstruing the definition and viability of a "global commons" strategy, the United States risks making a false choice between a global hegemonic strategy that is costly but stabilizing and a "fortress America" strategy that is cheaper, and

The authors are Ph.D. students in international relations at Georgetown University. They can be reached, respectively, at gms46@georgetown.edu and rsc39@georgetown.edu.

The Washington Quarterly • 35:1 pp. 115–128
http://dx.doi.org/10.1080/0163660X.2012.642789

yet shortsighted. Consequently, Washington need not follow the rapid collapse of the British Empire after World War II when, overburdened by both the financial and human cost of the war, London quickly abandoned its century-old security commitments "East of Suez" and launched itself down the steep path of decline.

The U.S. risks making a false choice between a global hegemonic and a "fortress America" strategy.

What the debate fails to understand is that securing the global commons does not mean patrolling every square inch of open water, eying every iota of airspace, or monitoring every megabyte of the internet. Joseph Nye justifies its need as a form of soft power, as a way to "legitimize our power in the eyes of others."[4] Properly defined as something beyond the scope of traditional national defense, or protecting American territory and assets from a rival state's aggression, securing the commons should entail protecting maritime trade from non-state actors in and around six strategic chokepoints, while also monitoring and mitigating the effects of natural disasters—in particular volcanoes—on trans-Atlantic and trans-Pacific air traffic. It does not involve a space or cyberspace component, as the former lacks a specific threat and the latter involves an area that should fall either under traditional national defense or law enforcement strategies. Redefined in concrete terms, Washington can pursue a global commons strategy that is manageable, beneficial, and necessary.

Toward a Meaningful Global Commons Strategy

For a strategic objective to have any meaning, it needs at least two distinct elements—a location and a specified threat: protecting who or what from whom or what. A location without a specific threat has little utility as a guiding strategic principle. Through much of the 18th and early 19th centuries, for example, the Lake Champlain Valley region was of vital strategic importance to the United States. Not only did the region provide the primary route into Canada, but control of the valley could also cut the United States in two. Today, while the terrain of the valley has not changed much, the threat of foreign invasion from Canada has long since passed and so the valley's strategic importance has faded into the history books. Similarly, for the first half of its existence, the United States was deeply concerned with securing its eastern approaches—from Narragansett Bay to Hampton Roads to Guantanamo Bay—from foreign navies, but with the threat gone few worry about their security.

Likewise, a threat without a location is equally meaningless. In some ways, this lies at the heart of the isolationist argument: why does it matter if the world is filled with nasty people doing bad things if they are not directly threatening the U.S. homeland or vital interests? Ever since George Washington delivered his famed farewell address, U.S. strategic thinking has had an isolationist streak. Whether prior to World War I, World War II, or today, this school of thought argues less about whether something is a menace to national security in absolute terms, but rather can the given actor in fact hurt the United States—especially across the vast oceans. And even if the actor can legitimately harm the United States, a threat absent a target is meaningless; one need only look at the plethora of post-9-11 terrorist threat reporting. While raising threat warnings may reflect some sort of reality in the abstract, few Americans take them to heart. Indeed, the "someone is going to do something bad somewhere" warning provides little utility to anyone.

"Safeguarding the global commons" also should not be conflated with traditional defense—protecting U.S. assets and territory from direct attack. A foreign navy steaming toward the shores of the United States poses a direct threat to U.S. national defense, as do terrorist groups who seek the destruction of U.S. assets. Similarly, Chinese hackers attempting to disrupt U.S. command, control, communication, and computer networks, al-Qaeda trying to disrupt transportation infrastructure, or the Chinese ballistic missile program directed at U.S. naval assets or even American cities pose direct threats to the United States. While these objectives are important, they fall under the guise of general air, sea, cyber, and space defense of the *United States*, not the *global commons*. With this definition in mind, a global commons strategy now seems more feasible: the United States is no longer tasked with a vague, all-encompassing mission, but rather with protecting the most critical maritime, aerial, space, and cyber nodes outside of the United States from their greatest threats. The natural question then is: what are the "critical nodes" and the "greatest threat" in each domain of the global commons?

Securing the commons should not involve a space or cyberspace component.

The Maritime Commons: Pirates, Political Violence, and Passageways

Given its Britannic origins and geographical position, the United States has a long maritime tradition, beginning with the construction of six frigates in the early years of the Republic. As a result, U.S. grand strategy has historically

sought to prevent foreign navies from gathering off its coasts, and to ensure the safety and viability of its global trade, 90 percent of which remains seaborne today.[5] These U.S. maritime trade interests are not related solely to a single coast or area of the world, but instead flourish across all three major bodies of water that surround the lower 48 states. America's largest trading ports by value—Los Angeles, Houston, and New York City[6]—are located on each of the country's three coasts, and America's largest trading partners are found across the Pacific (China, Japan, South Korea, and Taiwan), the Gulf of Mexico (Mexico, Venezuela, and Brazil), and the Atlantic (Germany and the United Kingdom).[7] The U.S. Navy is not only the largest but also the sole force capable of projecting power far from its own shores, having done so as early as 1801 when it dispatched warships to the Mediterranean in the First Barbary War.

Today, seafaring commerce operates rather freely across most of the world, threatened only by falling consumer demand and Mother Nature. However, chokepoints of global maritime trade do exist, where trade can be disrupted more easily by a variety of threats. Long and narrow bodies of water, such as straits or man-made channels, offer particularly tempting targets for preying pirates, terrorists, and hostile states alike. These geographic features funnel large numbers of ships into constricted passages, where they are vulnerable to coastal batteries, suicide-boaters, and marauders. A recent study, which used GPS locators to track the actual routes of global shipping, revealed that all but one of the 20 busiest ports in the world are either in the United States, Western Europe, or the Far East, and the two most-trafficked passageways are the Panama and Suez canals, respectively.[8] These passages must remain clear and unhindered so that U.S. warships may traverse them in pursuit of their missions. Guaranteeing the security of these nodes ought to be the primary task of any global commons strategy.

Six maritime passages are key to the safety of the global maritime commons: the Panama Canal, the Suez Canal, the Strait of Hormuz, the Strait of Malacca, the Strait of Gibraltar, and the Bab el-Mandeb. All are narrow channels of water not directly controlled by the United States through which a disproportionate amount of global trade passes, much of it U.S.-bound. For example, roughly 20 percent of total oil trade and 40 percent of worldwide seaborne oil trade passes through the Strait of Hormuz, making it the largest maritime transit zone in the world.[9] The Panama Canal, currently undergoing a major widening, is of particular importance to U.S. commerce, and the United States is, by far, the origin and destination of the largest share of canal traffic, totaling more than 135 million long tons in FY 2010—more than the next five countries combined.[10] The greatest trade route through the canal moves goods between the East Coast of the United States and the Far East, followed second by goods traveling between Europe and the U.S. West Coast.[11]

Meanwhile, the Suez Canal is the third busiest maritime oil route in the world, linking the Mediterranean economies to Asia. Without it, ships would

have to reroute around the Cape of Good Hope, the southern tip of Africa, adding 6,000 miles of transit to their route. Forty percent of world trade traverses the Strait of Malacca, including 15 million barrels of oil per day.[12] The Strait of Gibraltar connects the Mediterranean basin to the Atlantic Ocean and is the most direct route of trade to the United States as well as Western Europe by sea from ports as far away as the Black Sea. Finally, the Bab el-Mandeb (Gate of Scars), linking the Red Sea to the Indian Ocean through the Horn of Africa, is the gatekeeper to the Suez Canal, as any goods from Asia to the Mediterranean, and vice versa, must pass through both. More than 3.3 million barrels of oil pass through it daily.

Six maritime passages are key to the safety of the global maritime commons.

Over the years, threats to the chokepoints have come from a variety of sources. Interstate war has been the primary disrupter of safe passage through the chokepoints. The Suez Canal has been closed five times in its history, but has remained opened uninterrupted since 1975 following the last Egyptian–Israeli war.[13] During the Iran–Iraq War in the 1980s, Iranian forces mined the Strait of Hormuz and attacked Kuwaiti oil tankers, while the U.S. Navy reflagged Kuwaiti oil tankers, extending protection against Iranian mines and small missile boat attacks, from July 1987–September 1988. In recent years, Iran has consistently threatened to close the Strait of Hormuz if attacked by Israeli or U.S. forces in an attempt to deter an attack on its nuclear facilities. In 1989, the Panama Canal closed entirely for a little more than 24 hours following the U.S. invasion to remove Manuel Noriega and the supposed threat his regime posed to the canal.

Natural threats also closed some of the channels in the past. Natural disasters have twice closed the Panama Canal, once in 1915–1916 with mudslides and in December 2010 for 17 hours due to heavy rains.[14] In Southeast Asia, monsoon season typically brings high winds and heavy rains, but its ability to adversely affect the Strait of Malacca seldom lasts longer than a couple of hours.[15] Nevertheless, while the 2004 Asian tsunami did not devastate commercial vessels traversing the strait, studies have shown that subsequent tsunamis could ravage trans-strait shipping.[16]

Today's greatest threat to the security of the maritime commons comes from piracy and terrorism. Al-Qaeda cells have targeted the passages in the past, including the January 2000 failed bombing of the USS The Sullivans, the October 2000 attack on the USS Cole which killed 17 crew members, and the October 2002 attack on the French oil tanker Limburg, all near the entrance to the Bab el-Mandeb. One could similarly imagine the impact of a USS Cole-style attack against a U.S. warship or oil tanker in the Persian Gulf on the price of oil,

U.S. policy, and worldwide financial markets. In fact, an al-Qaeda affiliate group was responsible for an explosion on a Japanese tanker in the Strait of Hormuz on July 28, 2010, injuring one crew member in an attack by an apparent suicide boater.[17] The fact that, more than a year later, we still cannot confirm the departure point of the boat demonstrates the difficulty of detection. Washington has noted such challenges and has begun conducting military exercises specifically designed to defend the maritime passages. Although the Panama Canal has not experienced threats related to piracy or terrorism, in August 2010, the United States led 17 other countries, consisting of 2,000 personnel, in conducting 12 days of naval exercises aimed at exploring how best to ensure the security of the canal and its roughly five percent of global trade.[18]

Piracy has also taken a toll on the safety of the chokepoints of the maritime commons. In the past five years, annual rates of piracy have almost doubled—from 239 incidents in 2006 to 445 in 2010. Somali pirates were responsible for about half of the incidents in 2010 (219).[19] While piracy may not yet pose a vital threat to international commerce, it has resulted in the deaths of Americans in 2011, is becoming increasingly violent, and seems poised to become a greater threat in the years ahead.[20] The United States has taken action to increase its presence in the Horn of Africa. In spring 2003, the United States moved into a revamped Camp Lemonnier in Djibouti, and has recently expanded the base to a 500-acre facility which is now a naval base under USAFRICOM with 2,500 U.S. soldiers. In the early 21st century, securing the maritime commons largely means protecting maritime trade in these six critical passages from pirate and terrorist attacks.

The Aerial Commons: Natural Catastrophes and Navigation Corridors

Since the advent of the first commercial air flight nearly a century ago, aviation has become a critical means of transport for freight and passengers around the world. Air traffic has increased exponentially since the 1960s, slowed only by bouts of economic downturn.[21] 2010 saw over five billion air passengers and 91 million tons of air cargo, a robust 6.6 percent and 15.3 percent increase, respectively.[22] Moreover, the majority of air transport activity is centered on the largest industrial regions of the world: North America, Europe, and the Asia–Pacific accounted for roughly 85 percent of both passenger and cargo traffic in 2010.[23] These trends are also accurately reflected by the world's 30 busiest airports: all but one (Dubai) by passenger traffic and all but three (Dubai, Doha, and Mumbai) of the busiest by cargo tonnage are in the United States, Western Europe, or the Asia-Pacific rim.[24] By and large, the security of the aerial commons is dictated by the protection of the airspace in

the United States, Europe, the Asia-Pacific Rim, and the trans-Atlantic and trans-Pacific aerial highways.

Threats to the aerial commons are manifold and unconventional. With the memories of September 11, 2001 still fresh, terrorism is usually considered the overarching strategic threat to safe air travel. The attacks forced the total closure of U.S. airspace for three full days, cancelling most trans-Pacific and trans-Atlantic flights as a consequence. From the 1988 Lockerbie Bombing to the recent failed attacks such as the 2009 Christmas Underwear Bomber and the October 2010 Cargo Plane Bombs, terrorism continues to pose a large threat to commercial freight and passenger aviation. Billions of dollars have been spent on airport and airline security, and the entire national security strategy of the United States has been reoriented to combat the groups that launched these attacks.

Air traffic faces other threats as well. Human and technical error continue to be the greatest cause of accidents, even though the number of fatalities as a percentage of total air travel has been dropping precipitously every year.[25] Conflict zones have also increased the chances of miscommunication, as Moscow shot down Korean Air Line Flight 007 in 1983, killing 269 people, and Washington shot down Iran Air Flight 655 in 1988, killing all 290 on board. Pandemics are also a source of concern for air travel. The 2002–2003 SARS epidemic traveled globally within days through air travel and caused major Asian airlines to reduce destinations or incorporate the effect of the virus in their planning.[26] The 2005–2006 Avian Influenza (H5N1) and the 2009 Mexican Swine Flu had similar effects.

Somewhat surprisingly, the greatest threat to the aerial commons over the years has not come from terrorism, conflict, or even from airborne disease, but from natural disasters, particularly volcanic eruptions. In the past 30 years, 90 commercial planes have entered volcanic ash clouds and have all been damaged as a result, some saved only by extraordinary pilot skill.[27] As the 2010 eruption of Eyjafjallajökull in Iceland demonstrated, dense swathes of international airspace could be closed for weeks on end. European airspace remained nearly entirely closed for eight days in mid-April, the largest shutdown of airspace in commercial flight history, and the ash cloud caused further disruptions at various European airports into mid-May.

The greatest threat to the aerial commons has come from natural disasters, particularly volcanoes.

Volcanic eruptions are actually frequent occurrences and a constant worry for air traffic controllers. In 1989, Alaska's Mount Redoubt spewed volcanic ash that

nearly ended the lives of 245 people aboard KLM Flight 867, which managed to safely land in Anchorage after free-falling for 14,000 feet as the engines went off-line. Similar near-catastrophes happened following the explosions of the Galunggung volcano in Indonesia in 1982 and Mount Pinatubo in the Philippines in 1991, which closed Philippines airspace to all flights for more than five days and forced the permanent closure of the 9,000-acre U.S. Clark Air Base.[28] In June 2011, the Puyehue–Cordon Caulle eruption in Chile caused severe disruptions in air travel over the southern half of South America and much of Australia.[29]

The United States Geological Survey (USGS) constantly monitors and models potential volcanic eruptions as their effect on air travel could be devastating. U.S. volcano ranges are located in the Aleutian Island chain, Hawaii, and the Pacific Coast. In particular, U.S. geologists coordinate frequently with their Russian counterparts, as the ash from the active volcano chain located in the Kuril Islands could quickly spread into U.S. airspace. More than 200 aircraft and 25,000 people fly over the Kurils every day and could be at risk if there were an eruption.[30] Prevailing winds could easily send the cloud hundreds of miles across the airspace within a day, shutting down air traffic across the Pacific.

Geologists continue to fret about the possibility of major volcanic eruption daily. Particularly, each of Eyjafjallajökull's eruptions in the past millennia has triggered the eruption of the nearby, and much larger, volcano Katla, which would cause even larger damage to European airspace.[31] Similarly, Mount Tambora in Indonesia is monitored particularly closely, since it could cause substantial damage to Indonesian infrastructure, quarantine Indonesian airspace, and have catastrophic effects on Indonesia's 220 million people.

Oft-overlooked, securing the aerial commons is largely a matter of monitoring potential volcanic ash in Indonesia, Hawaii, the Kuril and Aleutian volcano chains, and Iceland, and mitigating its effect on trans-Atlantic and trans-Pacific commercial air travel. And yet, for all the uncertainty surrounding when and where the next eruption may be, one thing is clear: the primary threat to the aerial commons falls outside of the jurisdiction of the national security establishment.

The Space Commons: A Location without a Threat

The space commons possesses similar characteristics to its air and sea brethren: a large—infinitely so in fact—open space owned by no entity. Its governance structure is analogous to the body of international law which oversees state conduct at sea, though not as legally developed. Only five international treaties governing space relations exist, most of them ratified by states that do not even

possess space-faring capabilities. Drafted in 1967, the "Outer Space Treaty," as it is colloquially known, set the basic parameters for the military use of space, banning weapons of mass destruction, weapons testing, and the establishment of military installations in outer space.[32] The treaty, ratified by all nine space-capable nations except Iran, also forbids states from claiming sovereignty over any celestial body, such as planets, moons, or stars, which could be discovered in the future, calling them "the province of all mankind." Today, space serves as a critical zone for scientific discovery, commercial enterprise, and military activity, all related to the satellite-based positioning technology so critical to both warfare and everyday use such as cell phones, GPS, and the internet.

Despite the fact that space clearly qualifies as a "commons," it faces no grave threat beyond those traditionally associated with national defense. Armageddon-inducing asteroids are a bigger obsession of moviemakers than policymakers. "Space junk"—that is, man-made debris without further utility such as defunct satellites, spent rocket stages, or object fragments—is a growing cause for concern, but the number of collisions has been minimal, with little operational consequence, and no loss of life. Threats to the space commons emanate primarily from the ability of states to jam or destroy assets critical to both national defense and national prosperity, such as anti-satellite weapons (ASAT), a capability only possessed by the United States, Russia, and China. ASATs can only target national assets and therefore a hypothetical Chinese decision to launch an ASAT—as it did, unannounced, against its own satellite in January 2007—against a U.S. or European satellite would be designated an act of war.

In short, threats to the space commons are the 21st-century equivalent of the 18th-century naval armada, 19th-century cavalry, and 20th-century fighter jet: threats that are inherently part of evolving national defense planning. While the increase in space junk and growth of a private sector space industry may yet create a threat to the space commons, there is currently little the United States could or should do to secure the space commons from a commons-based threat. Space contains all the natural characteristics of a commons, but, apart from those associated with traditional national defense, faces no major threats.

The Cyber Commons: Threats without a Location

The ubiquity and utility of cyberspace in today's world is undeniable, evident in its critical function for commerce, entertainment, media, and the military. Web-based communication is essential to private use, financial institutions, and even modern military operations. Unlike the other commons previously described, the cyber commons is an ill-defined term or space; it is a network

of networks, possessing both physical and incorporeal elements. While the information contained in cyberspace is located in "clouds" and the pathways of information transfer do not traverse national territory, accessible to all and located outside the bounds of traditional sovereignty, the physical aspects of the cyber commons, such as computers, servers, phones, and fiber optic cables, are nationally-owned and located within the bounds of a governed territory.

Moreover, cyber-attacks are not always immediately attributable. In sharp contrast to the space commons, where the threshold for participation is extraordinarily high and the origin of threats is easily identifiable, internet users number two billion and are growing exponentially[33] and an attacker may go to great, and successful, lengths to conceal his or her identity. Cribbing terms associated with other axes of the global commons, internet piracy is common, cheap, and difficult to defend against. As many observers have noted, securing something intangible is a Sisyphean task.[34]

There is no shortage of threats menacing cyberspace, but there is a lack of true commons. To be sure, industrial sabotage, privacy violations, and commercial espionage are major concerns. Stealing proprietary technology can have both an economic impact, resulting in a loss of competitive advantage, and national security ramifications, such as if the loss of a technological advantage becomes a disadvantage on the battlefield. The distinction, however, is that these attacks do not occur in ungoverned spaces: the attackers live in one state and attack a target in another. In other words, most cyber-threats should be countered through traditional international law enforcement, where criminals may move across boundaries but the crimes occur within a sovereign state, rather than as an issue of safeguarding the commons.

Another type of cyber threat falls more in line with traditional national defense matters, rather than issues of safeguarding the commons.[35] The April 2007 attack on Estonian government and key private sector websites has largely been attributed to Russia over Tallinn's planned relocation of a Soviet-era grave site.[36] Similarly, Moscow was widely deemed responsible for the cyber-attacks on Georgian government websites prior to its August 2008 war with that former Soviet republic, including replacing the image of the Georgian president with that of Adolf Hitler.[37] Other attacks, such as when Chinese hackers were able to access sensitive U.S. Department of Defense sites in 2008 and the infiltration of the private networks of Google and other major U.S. corporations operating in China, elicited a statement from Secretary of State Hillary Clinton demanding an explanation from Beijing.[38] Similarly, the 2010 Stuxnet worm that targeted uranium enrichment infrastructure in Iran is suspected of being part of U.S. and/or Israeli efforts to delay Tehran's nuclear program. Most recently, a computer virus of unknown origin infected the cockpits of U.S. Predator and

Reaper drones, a clear-cut case of an attack on U.S. military assets, not on the "commons."[39]

These cyber threats, therefore, should fall under the rubric of traditional national defense; attacks tend to be state-sponsored and politically-motivated attempts to damage essential infrastructure of other states. While there are plenty of threats in cyberspace, the location of the attack often occurs within sovereign states and outside of the cyberspace commons.

Conclusion: The Myths of a "Securing the Commons" Strategy

For all the talk about the need to secure the commons, the term still remains shrouded in three essential myths. First, the location of the "commons" is a myth. The term connotes a strategy directed against vast expanses of unowned spaces around and beyond the globe. In reality though, much of what is meant by a commons strategy are not vast expanses, but rather a select few critical nodes that are vital to U.S. national security beyond American borders. And so far example in the maritime domain, while the oceans may cover the majority of the earth, we care primarily about a select few waterways.

> "Securing the commons" remains shrouded in three essential myths.

Second, securing the commons is a myth. The term congers up images of fences and guard towers. In reality though, few of the commons can be secured in this manner. In fact, as with the aerial commons, true security may lie very far afield from the purview of the Department of Defense or even the national security establishment broadly defined.

Finally, but most importantly, the notion of a commons strategy is a myth. For a concept to have a strategic meaning, it must consist of both a precise threat and a precise location: one without the other has only limited utility. Moreover, the concept must also be distinct from other strategic imperatives—separate from traditional national defense and international law enforcement—or else it is simply redundant.

Redefined, a global commons strategy loses some of its luster, but it also gains practicality. On one hand, it is no longer the broad overarching concept that some have made it out to be. On the other, the United States need not be tormented by the false choices of neo-isolationism and global imperialism often prompted by talk of protecting the global commons. Properly defined, a "securing the commons" strategy also allows for concrete planning to meet specific objectives, rather than simply waving one's hand at the globe and proclaiming the need to protect everything. The current debate can be reduced

to protecting maritime trade in and around six strategic chokepoints from non-state actors, while also monitoring and mitigating the effects of natural disasters on air traffic.

The good news is that, behind the novelty of using the term, a true "global commons" strategy is even feasible within the resource constraints of the post-financial crisis era. Indeed, only a small sliver of the defense budget is actually dedicated to securing the commons above and beyond the needs of traditional national defense. It is time to abandon the term and allow a more accurate discussion of America's global role to emerge.

Notes

1. "The National Security Strategy of the United States, May 2010," p. 49, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf; U.S. Department of Defense, "Quadrennial Defense Review Report," February 2010, http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf; Donald Kagan, Gary Schmitt, and Thomas Donnelly, "Rebuilding America's Defenses: Strategy, Forces and Resources For A New Century," The Project for a New American Century, September 2000, pp. 7, 51, and 64, http://www.newamericancentury.org/RebuildingAmericasDefenses.pdf; C. Raja Mohan, "U.S.–India Initiative Series: India, the United States and the Global Commons," Center for a New American Security, October 2010, http://www.cnas.org/files/documents/publications/CNAS_IndiatheUnitedStatesandtheGlobalCommons_Mohan.pdf; Michael Auslin, "Security in the Indo-Pacific Commons: Toward a Regional Strategy," American Enterprise Institute, December 2010, http://www.aei.org/docLib/AuslinReportWedDec152010.pdf; Brooke Smith-Windsor, "Securing the Commons: Towards NATO's New Maritime Strategy," NATO Defense College, Rome, September 2009, http://www.ndc.nato.int/research/series.php?icode=1.
2. World Bank Group, Global Environment Facility Program, "Protecting and Improving the Global Commons: 15 Years of the World Bank Group Global Environment Facility Program," 2006, http://siteresources.worldbank.org/GLOBALENVIRONMENTFACILITYGEFOPERATIONS/Resources/Publications-Presentations/GEFoverviewweb.pdf.
3. Barry R. Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* 28, no. 1 (Summer 2003): pp. 5–46, http://belfercenter.ksg.harvard.edu/files/posen_summer_2003.pdf.
4. Joseph S. Nye Jr., "The American National Interest and Global Public Goods," *International Affairs* 78, no.2 (April 2002): p. 241.
5. International Maritime Organization Maritime Knowledge Centre, "International Shipping Facts and Figures—Information Resources on Trade, Safety, Security, and the Environment," 2011, p. 6, http://www.imo.org/KnowledgeCentre/ShipsAndShippingFactsAndFigures/TheRoleandImportanceofInternationalShipping/Documents/International%20Shipping%20Facts%20and%20Figures%20final.pdf.
6. See U.S. Department of Transportation Maritime Administration, "U.S. Waterborne Foreign Trade by U.S. Custom Districts," http://www.marad.dot.gov/library_landing_page/data_and_statistics/Data_and_Statistics.htm. These numbers are all a decline since the peak in 2008, but have remained the top three ports by total trade value since at least 2003. Moreover, Houston passed New York City in 2006.

7. See U.S. Department of Transportation Maritime Administration, "U.S. Waterborne Foreign Trade by Trading Partners," http://www.marad.dot.gov/library_landing_page/data_and_statistics/Data_and_Statistics.htm.
8. Pablo Kaluza, Andrea Kolzsch, Michael T. Gastner, and Bernd Blasius, "The Complex Network of Global Cargo Ship Movements," *Journal of the Royal Society Interface*, January 19, 2010, http://rsif.royalsocietypublishing.org/content/7/48/1093.abstract.
9. U.S. Energy Information Administration, "World Oil Transit Chokepoints," February 2011, http://www.eia.doe.gov/cabs/world_oil_transit_chokepoints/Full.html.
10. Panama Canal Authority, "Top 15 by Origin and Destination of Cargo Fiscal Year 2010 (Long Tons)," http://www.pancanal.com/eng/op/transit-stats/table13.pdf.
11. Panama Canal Authority, "Trade Routes," http://www.pancanal.com/eng/op/routes.html.
12. Neil Chatterjee, "Singapore Raises Security Alert after Malacca Threat," Reuters, March 5, 2010, http://www.reuters.com/article/idUSTRE62335120100305.
13. James Feyrer, "The 1967–75 Suez Canal Closure: Lessons for Trade and the Trade-Income Link," VoxEU.org, December 23, 2009, http://www.voxeu.org/index.php?q=node/4428.
14. "Panama Canal Reopens after Temporary Closure," BBC News, December 9, 2010, http://www.bbc.co.uk/news/world-latin-america-11953800.
15. J. Ashley Roach, "Enhancing Maritime Security in the Straits of Malacca and Singapore," *Journal of International Affairs* 59, no. 1 (Fall/Winter 2005), http://www.southchinasea.org/docs/Enhancing%20Maritime%20Security%20in%20the%20STraits%20of%20Malacca%20and%20Singapore.pdf.
16. Koh Hock Lye, Teh Su Yean, Kew Lee Ming, and Nor Azazi Zakaria, "Simulation of Future Andaman Tsunami Into Straits of Malacca By TUNA," *Journal of Earthquake and Tsunami* 3, no. 2 (2009), http://redac.eng.usm.my/html/publish/2009_16.pdf.
17. Tim Lister and Paul Cruickshank, "Al Qaeda Affiliate Looks to New Targets in Persian Gulf," CNN.com, November 22, 2010, http://edition.cnn.com/2010/WORLD/meast/11/22/gulf.abdullah.azzam.brigades/.
18. "18-nation Military Maneuvers Focus on Panama Canal Security," UPI.com, August 18, 2010, http://www.upi.com/Business_News/Security-Industry/2010/08/18/18-nation-military-maneuvers-focus-on-Panama-Canal-security/UPI-45921282166076/.
19. International Chamber of Commerce's International Maritime Bureau, *Piracy and Armed Robbery Against Ships: 1 January-31 December 2010* (London: International Maritime Bureau, January 2011).
20. See Greg Jaffe, "Deaths of Four Americans Reflect Increasing Violence of Somali Piracy," *Washington Post*, February 22, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/02/22/AR2011022202451.html.
21. "World Air Travel and World Air Freight Carried, 1950–2010," Hofstra University, http://people.hofstra.edu/geotrans/eng/ch3en/conc3en/evolairtransport.html.
22. Airports Council International, "ACI Releases World Airport Traffic Report 2010," January 8, 2011, http://www.aci.aero/cda/aci_common/display/main/aci_content07_banners.jsp?zn=aci&cp=1-7-46^43915_725_2__.
23. Ibid.
24. Airports Council International, "Passenger Traffic 2010 Final," http://www.aci.aero/cda/aci_common/display/main/aci_content07_c.jsp?zn=aci&cp=1-5-54-55_666_2__; Airports Council International, "Cargo Traffic 2010 Final," http://www.aci.aero/cda/aci_common/display/main/aci_content07_c.jsp?zn=aci&cp=1-5-54-4819_666_2__.
25. "Number of Yearly Fatalities Due to Air Transport Crashes, 1918–2009," Hofstra University, http://people.hofstra.edu/geotrans/eng/ch3en/conc3en/airfatalities.html.

26. "SARS Affects the Health of Air Travel," About.com, http://airtravel.about.com/cs/safetysecurity/a/SARS_4.htm.
27. The Boeing Company, "Advances in Volcanic Ash Avoidance and Recovery," http://www.boeing.com/commercial/aeromagazine/aero_09/volcanic.pdf.
28. Thomas J. Casadevall, Perla J. Delos Reyes, and David J. Schneider, "The 1991 Pinatubo Eruptions and Their Effects on Aircraft Operations," http://www.preventionweb.net/files/3000_USGS2.pdf.
29. Rhys Haynes, "Volcanic Ash Cloud Forces Qantas to Cancel Wednesday flights, international flights delayed," *The Daily Telegraph*, June 21, 2011, http://www.dailytelegraph.com.au/news/second-volcanic-ash-cloud-coming/story-e6freuy9-1226079369713.
30. "Kurile Island Volcanoes and the Threat to Aviation," Sakhalin Volcanic Eruption Response Team (SVERT), http://www.avo.alaska.edu/activity/svert.php.
31. The majority of news reports say scientists have trouble predicting the time between the eruptions. See Joel Achenbach, "Scientists Find it Difficult to Predict Volcano Behavior," *Washington Post*, April 21, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/04/21/AR2010042102100.html.
32. UN Office for Outer Space Affairs, "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies," http://www.oosa.unvienna.org/oosa/SpaceLaw/outerspt.html.
33. "World Internet Usage and Population Statistics," March 31, 2011, http://www.internetworldstats.com/stats.htm.
34. Greg Rattray, Chris Evans, and Jason Healey, "American Security in the Cyber Commons," in *Contested Commons: The Future of American Power in a Multipolar World*, eds. Abraham Denmark and James Mulvenon (Center for a New American Security, January 2010), p. 141, http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf.
35. "War in the fifth domain," *The Economist*, July 1, 2010, http://www.economist.com/node/16478792.
36. Charles Clover, "Kremlin-Backed Group Behind Estonia Cyber Blitz," *Financial Times*, March 11, 2009, http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz1G2YS54Ux.
37. Travis Wentworth, "You've Got Malice," *Newsweek*, August 22, 2008, http://www.newsweek.com/2008/08/22/you-ve-got-malice.html.
38. Secretary of State Hillary Clinton, "Statement on Google Operations in China," January 12, 2010, http://www.state.gov/secretary/rm/2010/01/135105.htm.
39. Noah Shachtman, "Computer Virus Hits U.S. Drone Fleet," CNN.com, October 10, 2011, http://edition.cnn.com/2011/10/10/tech/innovation/virus-hits-drone-fleet-wired/index.html?hpt=hp_t2.