

Topical Essays

What Is National Security?

Kim R. Holmes, PhD

The challenge in devising a reliable measure of U.S. military power is that the effort must be rooted in a concrete understanding of what national security is and what it is not. This essay examines the elements of national security, providing both definitions of terms and a clarification of related concepts. It concludes with a number of take-aways from this analysis to help guide the making of a National Security Strategy.

A Short History of National Security

Modern concepts of national security arose in the 17th century during the Thirty Years War in Europe and the Civil War in England. In 1648, the Peace of Westphalia established the idea that the nation-state had sovereign control not only of domestic affairs such as religion, but also of external security.

The idea of the nation-state is commonplace today, yet it would be wrong to assume that it is the only way to look at international security. The pre-Westphalia international system was based on the assumption that there existed a universal principle governing the affairs of states led by emperors, popes, kings, and princes. That was indeed the principle of the Holy Roman Empire. The new idea of the nation-state took a different approach. Peace and stability could be better served if people were not slaughtering each other over some universal principle—in that case, religion. It would be far better to have an international system based on the equilibrium of nation-states dedicated to the limited purposes of national sovereignty and self-defense.

This idea was challenged by the philosopher Immanuel Kant (1724–1804), who resurrected the universal principle idea not in the old religious context, but in a secular one inspired by the Enlightenment. In his 1795 essay “Perpetual Peace: A Philosophical Sketch,” he outlined his idea that the system of nation-states should be replaced by a new enlightened world order. Nation-states should subordinate their national interests to the common good and be ruled by international law.

Thus was born the secular view of supranational institutions governing international affairs, which today is reflected in the global worldview of liberal internationalism and most clearly manifested in the United Nations.

It is important to keep these two schools of thought in mind when considering the various definitions of national security. They are present in current debates over national sovereignty, international law, and the role of international institutions in world affairs. American liberal internationalists for example, with their dedication to the United Nations and international governance, are neo-Kantians, whereas realists tend more to the views of Thomas Hobbes (1588–1679), Hugo Grotius (1583–1645), and other philosophers who espoused the supremacy of the nation-state.

Some Basic Definitions

Before analyzing different definitions of national security, it is important to understand some of the concepts the term incorporates.

The first is the concept of *power*. It can best be defined as a nation's possession of control of its sovereignty and destiny. It implies some degree of control of the extent to which outside forces can harm the country. *Hard*, or largely military, power is about control, while *soft* power is mainly about influence—trying to persuade others, using methods short of war, to do something.

Instruments of power exist along a spectrum, from using force on one end to diplomatic means of persuasion on the other. Such instruments include the armed forces; law enforcement and intelligence agencies; and various governmental agencies dedicated to bilateral and public diplomacy, foreign aid, and international financial controls. Variables of power include military strength, economic capacity, the will of the government and people to use power, and the degree to which legitimacy—either in the eyes of the people or in the eyes of other nations or international organizations—affects how power is wielded. The measure of power depends not only on hard facts, but also on perceptions of will and reputation.

Another term to understand properly is *military strength*. This term refers to military capacity and the capabilities of the armed forces, and it is a capacity that may not actually be used. It often is understood as a static measure of the power of a country, but in reality, military strength is a variable that is subject to all sorts of factors, including the relative strength of opponents, the degree to which it is used effectively, or whether it is even used at all.

Force is the use of a military or law enforcement capacity to achieve some objective. It is the actual use of strength and should not be equated with either strength or power *per se*. Using force unwisely or unsuccessfully can diminish one's power and strength. By the same token, using it effectively can enhance power. Force is an instrument of power just as a tool or some other device would be, but unlike institutional instruments like the armed forces, its use in action is what distinguishes it from static instruments of strength like military capacity. Thus, force should be understood narrowly as an applied instrument of coercion.

Finally, there is *national defense*. Strictly speaking, this refers to the ability of the armed forces to defend the sovereignty of the nation and the lives of its people; however, since the attacks of September 11, 2001, the mission of *homeland security*—using domestic as well as military instruments to defend the nation

from terrorist and other attacks either inside or outside the country—has come to be understood as an element of national defense.

International Systems of Security

Understanding the major schools of thought on international security that have arisen since the end of World War II will also help to explain the international context in which American national security is expected to operate. These schools of thought include:

- **Collective Defense.** Collective defense is an official arrangement among nation-states to offer some defense support to other member states if they are attacked. It is the basis of the classic defense alliances like the Triple Entente among the United Kingdom, the French Third Republic, and the Russian Empire before World War I and the North Atlantic Treaty Organization today. It is distinguished not only by geographical limitation, but also by its focus on military commitments.
- **Collective Security.** Collective security refers to various types of arrangements. Strictly speaking, collective defense involving mutual commitments of member states could be considered a form of collective security, albeit one limited geographically to military defense. More often, however, collective security is thought of as a regional and global concept represented by such international institutions as the League of Nations and the United Nations. Often, such arrangements are buttressed by concepts of international law and international aid and governance. Their distinguishing characteristic is their hybrid character between collective action at the international level and the acceptance of nation-states being ultimately responsible for their own security.
- **Global Security.** Global security is a set of ideas, developed largely by the United Nations since the end of the Cold War, that the world's security is everybody's business. It rests on the premise that no single nation is secure unless all are secure. While lip service is given to the idea of national defense, the far greater focus is on attempting to eliminate conflict through international law, aid, confidence-building measures, and global gover-

nance. The use of force should thus be reserved largely for international peacekeeping, peace enforcement, and the protection of innocent citizens from violence and should be decided upon and organized by the U.N.

- **International Law.** To the American ear, the use of the term “law” in the phrase “international law” conjures up the idea of binding rules enforced by judicial authorities and law enforcement officials. However, what Americans understand as “law” in a domestic context is often out of place in considering U.S. compliance with “international law.” The U.S. government must comply with the supreme law of the land, which the U.S. Constitution makes clear consists of the Constitution itself, laws made in pursuance thereof, and “all Treaties made, or which shall be made, under the Authority of the United States” (quoting Article VI of the Constitution). The United States also makes a practice of following what is known as “customary international law,” which “is comprised of those practices and customs that States view as obligatory and that are engaged in or otherwise acceded to by a preponderance of States in a uniform and consistent fashion” (quoting *United States v. Yousef*, 327 F.3d 56, 91 n. 24 (2d Cir. 2003), *cert. denied*, 540 U.S. 993 (2003)).

Non-Military Ideas of National Security

For most of the 20th century, national security was focused on military security, but as a concept, it expanded over time beyond what armed forces could do (or not do as the case may be). In 1947, the United States created the National Security Council to “advise the President with respect to the integration of domestic, foreign, and military policies relating to the national security....”¹ In the wake of total war, and at the dawn of the nuclear age, it was well understood that the days of defining national security solely in terms of armies fighting it out in set-piece battles were things of the past.

Since then, national security has come to mean different things to different people. Today, there are all kinds of “national securities.” They include economic security; energy security; environmental security; and even health, women’s, and food security. This proliferation of definitions has not always been for the good. In some instances, for example, it is merely a rebranding of domestic agendas to shift

resources away from the Pentagon. In other cases, it is adjusting to the complexities of a changing international environment.

The following list provides definitions of the major contending views of non-military definitions of national security, with no analysis of their merits or deficiencies.

- **Political security** refers to protecting the sovereignty of the government and political system and the safety of society from unlawful internal threats and external threats or pressures. It involves both national and homeland security and law enforcement.
- **Economic security** involves not only protecting the capacity of the economy to provide for the people, but also the degree to which the government and the people are free to control their economic and financial decisions. It also entails the ability to protect a nation’s wealth and economic freedom from outside threats and coercion. Thus, it comprises economic policy and some law enforcement agencies but also international agreements on commerce, finance, and trade. Recently, it has been defined by some in a human security context to mean eradicating poverty and eliminating income inequality.
- **Energy and natural resources security** is most often defined as the degree to which a nation or people have access to such energy resources as oil, gas, water, and minerals. It would be more accurate to describe it as access freely determined by the market without interference from other nations or political or military entities for non-market, political purposes.
- **Homeland security** is a set of domestic security functions that since 9/11 have been organized in a single agency, the Department of Homeland Security. It includes airport and port security, border security, transportation security, immigration enforcement, and other related matters.
- **Cybersecurity** refers to protection of the government’s and the peoples’ computer and data processing infrastructure and operating systems from harmful interference, whether from outside or inside the country. It thus involves not only

national defense and homeland security, but also law enforcement.

- **Human security** refers to a concept largely developed at the United Nations after the end of the Cold War. It defines security broadly as encompassing peoples' safety from hunger, disease, and repression, including harmful disruptions of daily life. Over time, the concept has expanded to include economic security, environmental security, food security, health security, personal security, community security, political security, and the protection of women and minorities. Its distinguishing characteristic is to avoid or downplay national security as a military problem between nation-states, focusing instead on social and economic causes and an assumed international "responsibility to protect" peoples from violence. It is to be determined and administered by the United Nations.
- **Environmental security** is an idea with multiple meanings. One is the more traditional concept of responding to conflicts caused by environmental problems such as water shortages, energy disruptions, or severe climate changes; it is assumed that these problems are "transnational" and thus can cause conflict between nations. The other, more recent concept is that the environment and the "climate" should be protected as ends in and of themselves; the assumption is that the environmental degradation caused by man is a threat that must be addressed by treaties and international governance as if it were the moral equivalent of a national security threat. In the past, natural disasters were not considered threats to national security, but that presumption is changing as the ideology of "climate change" and global warming takes hold in the national security community.

What National Security Is Not

It is true in life, as in strategic planning, that if you try to do everything, you will likely end up doing few things right. America's definitions of national security should be guided not only by a sensible understanding of what is truly vital to the nation's security, but also by what the nation can practically expect the government to do and not to do.

It is particularly important that the Department of Defense and armed forces understand this point.

An "all of the above" definition of national security, which primarily suits political constituencies, will only lead to confusion, waste, distractions, and possibly even military failures as the U.S. government is asked to do things that are either beyond its capacity or, worse, tangential to the real mission of protecting the country from harm.

It is thus critical to identify what national security is *not*. The best way to do this is to establish clear criteria for what exactly constitutes a threat to national security.

Is it, for example, truly a threat to the American people and the American nation as a whole? Can it be tolerated, or must it be eliminated? If the latter, does the nation have the proper means to defeat, contain, or influence the threat? If not, can it obtain those means within a reasonable time frame to make a difference and at an affordable cost?

Is the threat external or internal? If internal, is it from foreign, unlawful, and unconstitutional sources and thus reasonably understood as hostile and a risk to peoples' freedoms, or is it merely an act of lawful dissent or protest by Americans? The last thing the nation's leaders should do is to mistake political dissent as a threat to homeland security; although surveillance and intelligence-gathering capabilities are necessary to combat terrorism, it is imperative that America's leaders keep a bright line between watching terrorists and monitoring the political views of Americans.

Are the threats man-made or natural in origin? Natural disasters like hurricanes can be very dangerous, but even if one assumes they are caused by climate change (which is disputable), are they threats to the nation? Are "threats" from the weather, disease, or lack of food due to manipulations by states or terrorist groups or natural in origin, to be dealt with accordingly?

Finally, a crucial question: To what extent is the insecurity of other peoples related to our own? Does U.S. national security come into play only when the safety and security of allies who share America's values and interests are endangered? Or is America committed generally not only to the safety and security of all peoples around the globe, but also to their health, human rights, and general well-being?

The answers to these questions are not difficult.

First, national security is not something that merely affects the well-being of Americans. Rather, it involves their safety, their security, and their freedoms. It is becoming more commonplace to view

perceived social “injustices” as national security problems, but this distorts the very concept. Perceptions of social injustice or inequality are domestic concerns, not national security matters. Making less money than a neighbor is hardly as important to one’s life as being safe from incineration in a skyscraper in a terrorist attack.

A similar distinction holds true for so-called health security. While a pandemic disease could endanger the safety and security of thousands of Americans, unless it is committed as an act of biological terrorism, it should be considered a matter of health and domestic safety, not national security. As for the social implications, whether individuals have health insurance is vital to their lives, but that is a matter for them and their insurance agents or program administrators at the Department of Health and Human Services. It is a matter of “social” security, not national security.

Admittedly, global security concepts like health and human security come into play mainly overseas—in definitions of international security—and not in defining American security. But even there, some distinctions need to be made. “Food security” often means little more than preventing malnutrition or responding to famine caused either by natural causes or by political instability or war. The causes of these problems can be addressed through humanitarian aid, mediation, or (in extreme cases) peacekeeping or even military intervention, but little is gained by creating neologisms that may intend to heighten political concern but do little to help shape an adequate response for solving them.

A similar problem exists with the concept of environmental security. Clearly, wars can cause environmental damage and disruptions. Water shortages can create transnational and social tensions that may lead to conflict, and melting polar caps could open up waterways that exacerbate international tensions. As far as national and international security is concerned, however, the root causes of those conflicts are not environmental; they are political and military. Environmental issues are tangential and, at best, merely contributing factors. For example, Saddam Hussein did not burn the oilfields to damage the environment; he burned them to disrupt America’s military advance. Water shortages exist, but the problem begins when rival nations or groups start manipulating that scarcity for political purposes. Tensions with Russia over Arctic routes

are rooted in Russia’s geopolitical ambitions, not in purported concerns about the ozone layer.

A current example of problematic thinking about national security can be found in ideas about environmental security and its link to climate change. Some purport that climate change is a “threat multiplier” insofar as it supposedly could create natural disasters, exacerbate conflicts, and make the operating environment for U.S. armed forces more difficult. Some also see it as a problem for “safeguarding the global commons,” which is a foreign policy problem. From this perspective, government policies focus on using international “engagement to transition to a low-carbon growth trajectory” for the entire planet.² As for the Pentagon’s new role, it is about studying global warming’s supposed impact on military installations, the operating environment, and the Arctic and the assumed increased role in humanitarian assistance and relief that it expects to be caused by “climate change–induced” disasters.

As noted earlier regarding the confused thinking that results when policymakers conflate social conditions or public health matters with “national security,” there are a number of questionable assumptions behind current environmental security policy. There may be a scientific consensus on the fact that the climate warmed for a period, but there is no consensus on how much it is still warming or exactly how factors like vapor and the sun contribute to it. Thus, the more alarmist predictions are unreliable.

This sort of uncertainty means not only that there may not be a grave threat, but also that, at the very least, we have little idea how bad it could be or when it could occur. One sympathetic study of the risks of climate change concluded confidently that there is a one-in-20 chance that catastrophic outcomes could cost \$701 billion worth of coastal damage by the “end of the century.”³ But that is 85 years away. In the computer modeling world it is fairly common to come up with such precise figures (why not \$700 billion or \$702 billion instead of \$701 billion?), but in the real world—especially one that is almost nine decades away—many unpredictable things can and will happen.

Such unpredictability and such poorly disciplined thinking about national security are problematic for Pentagon planning. How do military planners make reliable plans for predictions that span almost a century and for which short-term predictions are highly unreliable? It may be appropriate for military

planners to study possible long-range implications, especially for the Arctic if one assumes the global warming forecasts to be accurate, but it would be imprudent to assume that any specific adjustments to installations or operational planning can be made reliably for periods of time further out than 10 or 20 years.⁴

Further, if things like climate change, global public health, or volcanic eruptions in some distant corner of the world are accepted as threats to national security, they are threats over which the United States does not exercise sovereignty. Yes, the U.S. could choose to do things to help improve the health of its citizens or mitigate the impact on its cities of changing weather patterns, but it stretches reason to assert that the U.S. military should be shaped to account for the policies and conditions of other countries and peoples relative to their own efforts in such cases.

Finally, there is the issue of energy security. All nations need energy to survive, but the market can supply most of their energy needs. Nations like Russia use energy as a geopolitical tool of coercion. Indeed, the Ukrainians can attest to how serious this coercion can be. Other nations like China make satisfying their energy-hungry economies a central part of their foreign policy. By and large, however, whatever attempts these and other countries make to use energy as a geopolitical tool run up against the demands of the international market. Oil and gas markets are highly influenced by nations and cartels, but they are also global in nature. This means that global economic demand also affects the price of energy and typically exerts greater leverage than do the actions of any one country.

Energy security thus becomes more a policy task of keeping the global energy market as free and open as possible than a programmatic objective of national security or even foreign policy. America's main energy problem has been an intentional limit on domestic production and infrastructure like pipelines and liquid gas facilities. Although energy insecurity is a real problem for some nations, the solutions for the United States are largely economic and infrastructural in nature. Energy "security" is mainly about taking advantage of new techniques such as fracking, more drilling for oil, and building more refineries, pipelines, nuclear reactors, and liquid gas facilities at ports for export purposes.

Focusing the Idea of National Security

It is clear that policymakers need a sharper focus as to what is and is not national security. It cannot be all things to all people; if it were, it would be meaningless. The definition of national security must be limited not only to decide what the government should be expected to do, but also, just as important, to decide what it should *not* do. This is especially true because of budget restraints. While it is proper to task the U.S. government with protecting a spectrum of national security interests—from the financial and economic system to access to natural resources—the lion's share of the government's interest and thus budgetary resources should be dedicated to safeguarding the country and its interests from foreign aggression.

Focusing national security policy on what matters most requires a more accurate understanding of power. As mentioned earlier, power is the degree to which a state can influence and control its destiny. All too often in the debate over "trade-offs" between soft and hard power, people assume that the former is interchangeable with the latter. In its crudest interpretation, it is the misguided belief that U.S. diplomats and troops are somehow interchangeable. Diplomats, particularly skilled ones, are no doubt important to American security, but it is inaccurate to suggest that they and U.S. troops play the same or even similar roles.

It is not uncommon for elected and appointed officials to note that the foundation of all American power is hard or military power. Unfortunately, many seem to do this as a mere rhetorical flourish, but in reality, it is a hard fact of international relations. Without military power, soft power is largely symbolic and ineffective. America draws its reputation as a world leader from three sources, and none of them derives from the unique skills of U.S. diplomats. Those sources are America's military power, its economic capacity, and its dedication to the values of freedom and democracy.

Much of the emphasis placed on soft power comes from a political desire to spend less on defense so as to have more to spend on diplomacy and foreign aid. It may very well be that more can be done in some of these areas, but that still begs the question of whether hard power and soft power are interchangeable.

Those who think that they are interchangeable, or that soft power is actually superior to hard power, point to the supposed success of the Euro-

pean Union, but this reveals a misunderstanding. The EU's soft power diplomacy is influential only because Europe's basic security needs, provided largely by America's armed forces, are already being met. Not having to spend money on defense enables Europe to spend disproportionately on foreign aid and social development programs. Furthermore, it is important to keep in mind that the confidence the world has in European stability is based in part on the security guarantee provided by the United States.

This is not a model that the United States has the luxury of following. Unlike Europe, the U.S. has no one to whom it can turn for its security. It is a net security provider, not a security taker as the Europeans are; for this reason alone, America's hard military power responsibilities are unique and should be a top priority. This does not mean that the U.S. should not do a better job in diplomacy, foreign aid, and other means of soft power influence. It means only that any assumptions of zero-sum trade-offs between hard and soft power are fatuous.

Another false assumption is that the U.S. needs only to "rebalance" or "streamline" its way out of a need for military capacity. This presumes that shifting the military's focus from one region to another or being more efficient with fewer resources committed to defense will somehow lessen the requirement for hard power. In fact, the opposite occurs. Less hard power capacity undermines the effectiveness and impact of soft power, encourages opportunism by competitors, and eventually leads to even greater demand for more hard power. For example, the rebalancing strategy in Asia has been largely rhetorical and diplomatic, covering up the fact that U.S. military capacity in East Asia is dwindling.

Moreover, the notion of a "whole of government" approach, which was prominent in the 2010 National Security Strategy, appears to assume that strenuous coordination in training across departments can replace the loss of hard power capacity. "Rebalancing" and "whole of government" sound sophisticated and almost prosaic; in reality, they are covers for America's diminishing capacity to maintain its influential role in the world.

What National Security Is

Now that it is fairly clear what national security is not, the task of crafting a definition of what it is should be easier.

National security is the safekeeping of the nation as a whole. Its highest order of business is the protection of the nation and its people from attack and other external dangers by maintaining armed forces and guarding state secrets. Since the attacks of September 11, 2001, the defense of the homeland from terrorist and other attacks, broadly understood as homeland security, has risen as a major national security concern.

Because national security entails both national defense and the protection of a series of geopolitical, economic, and other interests, it affects not only defense policy, but foreign and other policies as well. Foreign and defense policies should be seen as mutually reinforcing, not as zero-sum trade-offs in budgetary fights. While hard choices will indeed have to be made in national security spending, they should be decided by realities, not by fatuous comparisons or incoherent and tendentious concepts.

The next question to address is how to attain national security. For decades, the United States has tried to answer this question with the official National Security Strategy (NSS). Unfortunately, these official documents have a bad reputation. They are often seen more as public relations exercises than as reliable guides for strategic planning.

Crafting a full NSS is beyond the scope of this essay, but as a bare outline, the U.S. should have goals that are clear, achievable, and mutually reinforcing. The following suggestions for National Security Strategy goals are listed in descending order of importance:

1. **Preserve** the safety of the American homeland and protect the integrity of the nation's domestic institutions and systems vital to that purpose. This goal requires strong Active, Guard, and Reserve forces as well as effective intelligence, law enforcement, counter-terrorism, cybersecurity, and immigration policies to protect the homeland and secure America's borders.
2. **Maintain** a global balance of power in favor of America's security and interests and those of its friends and allies. This requires an armed force capable of successfully completing all of the military missions assigned to it and fulfilling U.S. commitments to defend the security of America's allies and friends.

3. **Guarantee** the freedom of the seas, upon which both the U.S. and world commerce and economic viability depend. This in particular requires a strong U.S. Navy and Marine Corps and overseas bases capable of supporting the projection of American power around the world.
4. **Exert** U.S. influence as much as possible overseas through the entire spectrum of instruments of power, including diplomacy, foreign aid, selective intelligence sharing, public diplomacy, and human rights and humanitarian programs. This requires integrating U.S. diplomacy and foreign aid and humanitarian programs more closely to achieve the purposes of the national strategy.
5. **Dedicate** America to maintaining as much as possible a global economy based on economic freedom (sometimes called democratic capitalism), including free trade and the openness of energy markets and international financial systems based on the rule of law.
6. **Focus** U.S. energy security policy on developing domestic resources and keeping the international energy market as free as possible from harmful political manipulation.
7. **Ensure** that America's dedication to values and their promotion overseas reflects not only its own history of liberty, but also the universal principles of freedom—thus defining human rights as freedom of expression, the right of democratic self-government, economic freedom, equality before the law, and freedom from persecution and oppression. Values should guide and inform the nation's strategy, not direct or control it. Geopolitical compromises will have to be made from time to time, and America should not see itself as the world's policeman enforcing certain values. However, it is important to recognize that this nation's commitments to universal values like freedom and democracy are reasons why foreign nations and peoples support America.

The Way Forward

Any discussion of national security must be rooted in a clear understanding of the concepts it involves. The following are the four most important takeaways from this analysis of national security.

Takeaway #1: Make capacity and flexibility the watchwords of strategic and military planning so as to give the President as Commander in Chief and his military leaders as many options as possible to deal with any contingency that may arise to threaten the nation. Understand that the more capacity and credibility U.S. forces have, the less likely it is that they will be challenged and the more able they will be to respond effectively to surprises when they occur, as they inevitably will. This “peace through strength” strategy is not just a slogan; it is a tried-and-true strategy pursued largely successfully during the Cold War to avoid actual war.

Takeaway #2: Avoid the trap of artificial “trade-offs” between non-military and military programs dedicated to national security. In the real world of budgets, there will always be hard choices, but political leaders and policymakers should avoid pretending that funding for a climate change program is anywhere nearly as important as funding for a new-generation fighter aircraft or for maintaining America's fleet of aircraft carriers.

Takeaway #3: Focus non-military instruments of power and policies on supporting the discrete goals of national strategy listed above. This means consciously aligning U.S. diplomacy, foreign aid, public diplomacy, international trade and financial policies, and human rights policies to advancing discrete national interests. While this involves a global perspective as defined by the national strategy, it does not envision the use of these instruments of soft power either to create a global order of international governance run by international organizations or to bolster the existing international “system” in which the sovereignty of tyrants and human rights abusers is assumed to equal America's own.

Takeaway #4: Be as clear as possible about what can and cannot be achieved by military intervention. Much of the controversy surrounding the issue of military intervention stems from confusion over what can and cannot be achieved by force and, just as important, over what Americans expect their armed forces to do. Are these troops nation builders and humanitarian police forces? Or are they military defenders of narrower security interests? In truth, they have been employed for all of these purposes with varying degrees of success, but the true trade-offs of doing so are scarcely ever understood and articulated by this nation's leaders.

The United States cannot eliminate every bad actor, right every wrong, or correct every perceived injustice in the world. That is impossible. But the United States *can* contribute to building a world order in which the rule of law, the integrity of national borders, democratic capitalism, freedom of the seas, democratic self-government, human rights, and international trade prevail, not as guaranteed outcomes but as opportunities. It is an exhausting and costly enterprise, but no one else can do it. Not only that: It is for America's own good.

Endnotes:

1. National Security Act of 1947 (Public Law 80-253), Section 101(a), now codified at (50 U.S.C. 3021).
2. The White House, *National Security Strategy*, May 2010, p. 34, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed September 15, 2014).
3. Risky Business Project, *Risky Business: The Economic Risks of Climate Change in the United States*, June 2014, p. 4, <http://riskybusiness.org/pdf> (accessed September 15, 2014).
4. Climate change policy supporters have been stymied by the now over 15-year temperature hiatus in the rise of the global temperatures. It is not something their computer models had predicted. Scientists are not sure why this is occurring, but at the very least, it shows the difficulty (if not futility) of using computer models to predict specific outcomes over 10- or 20-year time spans. See "Technical Summary" in *Climate Change 2013: The Physical Science Basis: Working Group I Contribution to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change* (Cambridge: Cambridge University Press, 2013), p. 61, http://www.climatechange2013.org/images/report/WG1AR5_ALL_FINAL.pdf (accessed October 25, 2014). See also Judith Curry, "The Global Warming Statistical Meltdown," *The Wall Street Journal*, October 9, 2014, <http://online.wsj.com/articles/judith-curry-the-global-warming-statistical-meltdown-1412901060> (accessed October 28, 2014).

Building the Right Military for a New Era: The Need for an Enduring Analytic Framework

Daniel Gouré, PhD

The Unique Value of American Military Power

Today, the United States is a global power with worldwide interests, investments, relationships, and concerns. It is also the leader of a like-minded community of nations, a set of alliances, security relationships, and even of what passes for a board of directors for the international economic system. America earned its current role by helping to rebuild the war-shattered nations of Europe and Asia, promoting an open international political and economic order, aiding those suffering from humanitarian crises, and providing a bulwark against regional aggression and internal subversions.

Twice in the past 60-plus years, the United States has chosen to fill the vacuum caused by the collapse of old institutions, relationships, and power centers. After World War II, along with key allies, this country created a new international order anchored by democratic institutions and international agreements that have endured to this day. America, again in concert with many allies, also built a security apparatus and military machine of global reach and power, one unlike any seen in peacetime.

When the Soviet Union collapsed, the United States did not simply declare victory and go home. Rather, even while reducing the size of its military, America chose to remain in the world—forward deployed and committed to maintaining and even expanding long-established alliances and security relationships. As a result, the world was able to

weather difficult and dangerous transitions while maintaining a viable international system.

Ironically, the end of the Cold War increased the United States military's role in maintaining the global order. From 1945 to the collapse of the Soviet Union, there were between 40 and 50 significant instances of the use of U.S. armed forces abroad. From 1991 to the present, that number nearly tripled to between 100 and 135. These figures do not include several hundred humanitarian operations, support for civil authorities after natural disasters, or the myriad of routine deployments for training purposes or to build partnership capacity. Taking these additional actions into consideration, the activity level for the U.S. military increased by a factor of four after 1991.¹

At the same time, in the 1990s, the U.S. military was halved. This dramatic force reduction, coupled with the fourfold increase in activity, resulted in an eightfold increase in the military's "use rate" or "stress level." Were it not for two important factors, the U.S. military might have collapsed.

1. The Reagan–Bush era had yielded an overhang of military procurements, an investment off of which the military has lived for years; and
2. The military engaged in selective hollowing, which allowed the services to reduce spending on maintenance and upgrades rather than relying

on a reduction in force. For the Army alone, this amounted to some \$50 billion in the years prior to September 11, 2001.

U.S. power and presence are the foundation on which the present international order is built. Whether it is the size of the U.S. economy, America's capacity for innovation, the role of the dollar as the world's reserve currency, or the contribution of U.S. military power to the stability and peace of the global commons, the present world order has "made in the USA" stamped all over it. Furthermore:

The United States offered resistance to illiberal and autocratic regional powers that have at time[s] challenged the protocols of the postwar order. And that pushback has allowed weaker nations—such as Poland or the Baltic States—to escape the orbit of post-Soviet Russia, while in the Pacific ensuring that an Australia, New Zealand, or the Philippines is not bullied into subservience by China.

This strange postwar world ushered in the greatest advancement in prosperity amid the general absence of a cataclysmic world conflagration or continental war since the dawn of civilization. For the first time since the rise of the Greek city-state, most nations have been able both to prosper and to assume that their boundaries were inviolate and their populations mostly free from attack. A system of international communications, travel, commerce, and trade is predicated on the assumption that pirates cannot seize cargo ships, terrorists cannot hijack planes, and rogue nations cannot let off atomic bombs without a U.S. led coalition to stop them from threatening the international order.²

For more than four decades, the modern American military has served this nation with distinction. However, the U.S. military today faces a growing number of challenges. Some of these are of our own making, most notably an unwillingness to put forward the relatively modest amount of resources required to maintain a military capable of meeting enduring security requirements. Others come from without, including the proliferation of advanced conventional and even nuclear weapons and delivery systems; significant increases in the defense

budgets of potential adversaries; and the rise of new types of warfare based on new technologies, many of them commercial in nature.

The most important challenge facing America is the apparent inclination of its political elite to turn away from this nation's role as the linchpin in the international security order—an inclination that places this nation's vital interests, as well as the freedom and security of friends and allies, at risk.

From Global Containment to the Two Major Theater War Standard

For more than 60 years, the adequacy of U.S. military power was measured with reference to a dominant strategic concept (deterrence); a single adversary (the former Soviet Union and its allies); and largely in terms of one type of conflict (a large-scale, high-end conventional conflict centered in Europe). A full-spectrum conventional military force, reinforced by robust theater and strategic nuclear capabilities, was viewed as sufficient to deter any Soviet leadership from employing force directly against the United States, its allies, or their vital interests. In addition, it was generally accepted that the broad range of capabilities necessary to conduct and sustain such a major war would provide sufficient richness with which to address multiple lesser conflicts and contingencies.

Historically, the U.S. government has used as a sizing standard the number and character of wars in which the U.S. might be engaged. The standards were defined in terms of the prospective opponents, the scale of the conflict, and the ultimate objectives.

At the height of the Cold War, the United States maintained a two-and-a-half-war strategy: major, simultaneous wars against the Soviet Union and China plus another nation. Following the Sino-Soviet split and the U.S. opening to China, the Nixon Administration changed the sizing criteria to a one-and-a-half-war strategy that planned for a major war with the Soviet Union plus a second, possibly related conflict in the Persian Gulf or on the Korean peninsula.

The Cold War period was not free of debate and disagreement over the size and composition of U.S. military forces. The answer to the question of "how much is enough?" was pursued from a variety of perspectives: strategic, political, and budgetary. What is notable about the Cold War effort to define the required size and character of U.S. military forces is

the application of rigorous and consistent analytic methods. By focusing on a consistent and commonly accepted set of scenarios, performance requirements, and measures of effectiveness, analysts were able to track the strength and weaknesses in force structure decisions, particularly in light of a changing threat, and provide clear information, traceable over time, that contributed to the public debate on the adequacy of American military power.³

Eventually, the Department of Defense's use of analytics yielded the "net assessment process." Developed by the Office of Net Assessment (ONA) under the leadership of Mr. Andrew Marshall to examine the balance of military power between the West and the Soviet bloc, the process answered questions concerning both the present and the future by anticipating changes in technologies, defense budgets, and even alliances.

A strategic net assessment began with a thorough understanding of America's military capabilities and those of other nations, most notably the Soviet Union and its Warsaw Pact allies. To this quantitative assessment was added an appreciation for how military forces might be employed in various kinds of conflicts—the qualitative dimension. Changes in alliance relationships, advances in technology, and fluctuating defense budgets were also considered as factors influencing the final or net assessment of the military potential of the opposing sides.⁴

Over time, ONA also developed an approach to the long-term competition between the two sides called Competitive Strategies. The central idea of Competitive Strategies was to focus areas of U.S. advantage against areas where America's competitors were weak while simultaneously limiting their ability to do the same. The long-term goal was to move the balance of military power increasingly in America's favor, thereby enhancing deterrence. ONA helped to train several generations of analysts and policymakers in the methodologies and ways of thinking about net assessment and competitive strategies.⁵

Analytics and the End of the Cold War. With the fall of the Soviet Union and the end of the Cold War, the strategic and analytic pillars that supported a coherent and consistent debate on force sizing and composition vanished almost overnight. Since the end of the Cold War, the basic metric for judging the adequacy of the U.S. military has been its ability to fight in two geographically separated regions of the world at approximately the same time. Referred

to at different times as "Major Regional Contingencies (MRCs)," "Major Theater Wars," or "multiple, large scale operations," the two-war standard has stood the test of time because it reflects a basic strategic reality that was well expressed by the 2012 Strategic Guidance for the Department of Defense: "As a nation with important interests in multiple regions, our forces must be capable of deterring and defeating aggression by an opportunistic adversary in one region even when our forces are committed to a large-scale operation elsewhere."⁶

Moreover, there have been times when the United States, in order to deter possible aggression, has found it prudent or even necessary to build up its forces in two different parts of the world. For example, in 1994, the Clinton Administration faced a crisis on the Korean peninsula. In response to heightened tensions in Northeast Asia, the United States began to move additional forces to the region. At about the same time, Saddam Hussein began to move portions of his army from central Iraq southward in what could have been preparation for another attack on Kuwait. Again, the U.S. deployed an array of forces to that region. Then-Secretary of Defense William Perry later credited the maintenance of a two-MRC military for Washington's ability to deter conflict in both regions simultaneously.⁷

Each Administration has put its own spin on the two-MRC standard, and therein lies the problem: It is impossible to compare the adequacy of the U.S. military to meet national security demands over time because the goalposts keep moving. Initially, the requirement was to fight and win two conflicts similar in size and complexity to Desert Storm, the war that the U.S. and its coalition allies had fought against Iraq. Over time, successive Administrations took liberties with this standard—alterations that reflected a variety of strategic, political, technological, and budgetary priorities.

For instance, the 2001 and 2006 Quadrennial Defense Reviews (QDRs) paid minimal obeisance to the two-MRC standard, instead reflecting the impact of September 11, the Bush Administration's determination to prosecute the global war on terrorism, the requirements of two long-term stability operations in Iraq and Afghanistan, and rising defense budgets.

The 2009 and 2014 QDRs were driven by the Obama Administration's markedly different strategic and policy perspectives. They continued, for

example, the two-MRC standard but significantly modified the definition of the type of conflicts for which the U.S. military should be prepared. Gone was the requirement for a protracted, large-scale stability operation—another Iraq or Afghanistan. The military still had to fight two conflicts, but only one would be a full-out conventional war. In the other conflict, the U.S. military's objective would be limited to “denying the objectives of—or imposing unacceptable costs on—a second aggressor.”⁸ In theory, because this second conflict would be based on more limited objectives than those pursued in the first, it would require fewer forces and would last for a shorter period of time. As a consequence of these changes, the Obama Administration was able to extract a significant “peace dividend” from ensuing defense budgets.

While post-Cold War defense policy has always advocated being able to fight two wars at the same time, successive Administrations have never provided sufficient resources to ensure a force structure capable of achieving such a goal—except at extremely high risk. It was possible to get away with this charade in the past because the U.S. military was relatively modern as a result of the Reagan buildup and America's potential adversaries were rather weak. Neither of these conditions holds true today.

In fact, even before the Budget Control Act became law, the U.S. military would have had a very hard time fighting two regional conflicts. This difficulty is the reason that the Obama Administration changed the standard for American military adequacy from winning two wars to winning one and attempting to deny an aggressor his objectives or punish him severely in the second. No one really knows what this second objective means or how to assess the adequacy of U.S. military forces to do either denial or punishment. If, as some experts have speculated, the second requirement means using air and sea power to attrite an aggressor's military forces without employing significant land forces, it is by no means clear that our ammunition stocks are sufficient for such an effort.

The 2014 QDR did the Obama Administration, the Pentagon, and the American people a disservice by pretending that the proposed budgets were adequate to maintain a force structure with sufficient readiness. The reality is that if America wants a two-war military, its citizens have to be willing to pay for it. The next Administration will face a diffi-

cult choice: increase defense spending or turn one important region of the world over to the tender mercies of authoritarian or even fundamentalist-theocratic states.

Inadequacy of the Current Analytic Paradigm

It is increasingly evident that the current approach to defining a sizing standard is inadequate. In fact, it is not really a sizing standard at all; rather, it is a way to justify reductions in the size of the military in the face of a declining defense budget.

Some have characterized the new formulation as a one-and-a-half-war standard, but the threat of major theater wars in Southwest and Northeast Asia is no less serious today than it was when the two major theater war standard was articulated some 20 years ago. If anything, the possibility of two major conflicts that overlap in time is increasing, and the formulation of the mission for the second conflict as the capability to deny an aggressor's objectives or impose unacceptable costs is so vague as to be meaningless. The lack of a clear, more precise and usable standard for sizing the U.S. military leaves defense planners in a quandary: Is the one major theater war to take place in the desert, jungles, or mountains? Is it against a nuclear-armed adversary or one with only limited long-range strike capabilities? Will America have capable allies in theater? The two regions of the world of most interest to military planners are quite dissimilar and require different force structures.

Similarly, regarding the second part of the standard, how many fighter wings or strategic bombers are needed to deny an aggressor's objectives or impose unacceptable costs? One nuclear weapon should do it, but America is not about to go back to the good old days of the 1950s. Without a sense of against whom or when a buildup might be required, it is impossible for the military to judge as it downsizes today how much equipment or which people and capabilities should be retained in order to have the ability to expand in the face of a larger future threat.

The public debate on the adequacy of America's national defenses waxes and wanes with every crisis. There is a high point every four years with the publication of the Quadrennial Defense Review. Unfortunately, each QDR is *sui generis* and, despite claims by each Administration that it has taken a long-term perspective, deals only with near-term challenges. There is no common standard, no yardstick

by which to measure the adequacy of U.S. military power over time.

Moreover, even though QDRs are required by law to take a long-term perspective on the adequacy of U.S. forces, they have never done so. Rather, they provide a static vision of the adequacy of U.S. military forces and, even then, not against the most formidable threats and adversaries. Hence, the QDR is a backward-looking, out-of-focus Polaroid picture that tells us nothing about how much military power the nation needs relative to both missions and threats.

The static, disconnected nature of this analytic approach does not permit an adequate characterization of the arc of strategic trends involving defense spending, force evolution, or technology proliferation. As a consequence, it is easy for negative conditions such as the long-term decline in the U.S. military to be obscured in policy discussions. But this is only half of the problem. The decline in American power has been exceeded by that of its major allies: Not even a handful of NATO countries spend the agreed minimum of 2 percent of gross domestic product (GDP) on defense.

This is now a military beset by challenges on all sides. It is worn out from overuse and inadequate modernization. There is a clear and growing negative tilt in the strategic military balance between the United States and its allies on one side of the scales and rogue states and prospective adversaries on the other side. A combination of factors—war weariness, financial crises, unfavorable demographics, entitlement spending's growing weight on national finances, the rising costs associated with modern all-volunteer militaries and the global commons, and a failure to make the case publicly for adequate defense spending—has contributed to the pronounced decline in Western military strength.

And now the United States is about to tilt the scales further against its own interests. Sequestration would impose serious and poorly distributed cuts in defense spending across the entire Department of Defense. The military already is reducing end strength, retiring hundreds of airplanes and dozens of ships and slashing training activities. Sequestration will only make the situation worse.

Military Investment by America's Adversaries. While it is important to appreciate the long-term downward trends in U.S. military forces and capabilities, this is only half of the problem. It is

equally important to appreciate the trends in military investments by prospective adversaries.

Over the past five years, the overall share of defense spending by the West has shrunk from around three-quarters to one-half of the global total. For more than a decade, however, China has increased its defense spending by double digits, more even than the annual growth in its GDP. It has developed, deployed, and—according to recent reports—demonstrated an operational anti-ship ballistic missile. And China's area denial/anti-access capabilities continue to grow: Beijing is deploying anti-space forces that could deny the United States the use of space in a future conflict.

Furthermore, Russia has announced yet another major defense spending program designed to close the technology gap between Moscow and the U.S. and its NATO allies. Within another decade, the combined defense spending of Russia and China could exceed that of the United States.

The International Institute for Strategic Studies' *2014 Military Balance* makes a particular point of the contrast between the decline in Western military investments and the sharp rise in defense spending and concomitant arms expansion of programs in the Asia-Pacific region:

Whereas defence spending in North America and Europe has stagnated or declined since the 2008 financial crisis, over the same period real defence outlays in China and Russia rose by more than 40% and 30% respectively.

In real terms, total Asian defence spending in 2013 was 11.6% higher than in 2010. The largest absolute spending increases over the past year occurred in East Asia, with China, Japan and South Korea accounting for more than half. China now spends about three times as much as India on defence, and more than neighbours Japan, South Korea, Taiwan and Vietnam combined.

These outlays are fuelling heightened military procurement in a region replete with conflicting territorial claims as well as long-standing potential flashpoints. Not least because of the Asia-Pacific's central place in the global economy, the rapid pace of capability development and the potential for accidental conflict and escalation will continue to be of concern.

Overall, the scope for competition—and potential confrontation—is broad. It might develop in different domains, such as space and cyber, through the development of new military technologies, such as directed energy weapons, or even in newly accessible regions, such as the Arctic.

For the West, what is clear is that the end of the Iraq War and the impending drawdown from Afghanistan mark neither an end to crises inviting Western military responses, nor a definitive end to Western intervention. Events on Europe's periphery will continue to demand attention, and there remains substantial capacity to deploy force.⁹

Yet because of the limits of the current analytic paradigm, the intersecting implication of these two trends—Western military decline and the growing military capacity of states hostile to Western interests—is never addressed. The current analytic paradigm neither acknowledges these adverse trends nor makes any serious effort to identify the investments in U.S. military forces, platforms, and capabilities that must be made to reverse them.

More with Less. Moreover, as American military power declines, the demands made on the U.S. military are increasing. The then-Commandant of the Marine Corps, General James Amos, recently opined that in view of projected U.S. defense budget cuts on the one hand and the explosion of international crises and threats to U.S. interests on the other, he expected his service and the Joint Force, at a minimum, to be asked “to do the same with less.” His real concern, he acknowledged, was that the U.S. military would be asked “to do more with less.”¹⁰

Yet this potentiality—having to do more with less—is another area in which the current analytic paradigm is inadequate. Specifically, it fails to account for unchanging or increasing demands on the military at a time when both the size of the force and its capabilities relative to evolving threats are declining.

How does the military do the same or more with less? One way is by working the force harder. Units, particularly those with high demand/low density capabilities, are deploying overseas for longer periods and, as a consequence, spending less time at home. Platforms and equipment are operated at a higher rate than predicted, thereby increasing maintenance and sustainment costs and bringing for-

ward the date at which aircraft, ships, and vehicles will need to be overhauled or even replaced. Eventually—really, in a few short years—this approach will break the force.

The other way to do more with less is by accepting greater risk. The term “risk,” while often used by military officers, Defense Department civilians, and think tank experts, is never clearly or accurately defined in ways that are understandable to Members of Congress or the public. What “risk” really means is that while the mission, the region, or the commitment will not be formally abandoned, there is no way it can be supported or defended with the forces available. Insufficient, inadequately trained, or poorly supported forces will be sent to accomplish the impossible. Remember Task Force Smith in Korea in 1950? Ultimately, this approach means that Marines (and other service personnel) may sacrifice their lives needlessly.

Further defense budget cuts—a consequence of sequestration—will require reductions in force structure and modernization programs that will virtually guarantee the inability of the United States to deploy credible military forces to two regions at the same time. For two years, senior Administration officials and uniformed personnel have been attempting to make clear to Congress and the American people the consequences of sequestration. The lack of a comprehensive, credible, and consistent analytic national methodology for assessing the adequacy of U.S. military capabilities and identifying shortfalls has severely impeded this effort.

Indeed, the closest anyone has come to clarifying what the Pentagon means by “accepting increased risk” was in testimony by the Joint Chiefs of Staff last year before the House Armed Services Committee. If sequestration comes into effect in 2016, the Pentagon will not have sufficient forces, air and sea-lift, or munitions to conduct two major regional conflicts. As the Vice Chief of Staff of the Air Force, General Larry Spencer, warned, “We won’t have the capacity to respond to what we say we can respond to today.”¹¹

Then-Army Vice Chief of Staff General John Campbell, whose service is facing the possibility of simultaneous land wars in Europe, the Middle East, and Northeast Asia, stated the danger in even starker terms: “We’re mortgaging the future. We’re really pushing hard for additional money to try to bring up short-term readiness, but then in 2016, if we go to sequestration, we all just fall off the map again.”¹²

The Elements of a New Methodology

If the American people are to be engaged in a reasonable debate over future defense spending and the adequacy of the U.S. military, a new yardstick for defining sufficiency is required. Such an index of U.S. military power needs to be designed for the long haul: a methodology capable of tracking changes in military capabilities and critical technologies that can take decades to make an impact.

This yardstick must reflect both the high-impact/low-probability scenarios and those that are more likely to occur but have lesser consequences. It must also reflect changes not only in U.S. forces and capabilities, but also those of friends, allies, and—most important—adversaries. Thus, this methodology must go beyond quantitative measures of military power (the bean counts) and include a clear articulation of enduring and vital U.S. security interests, an accurate assessment of both the current and likely future threats to those interests, and a net assessment of the ability of the U.S. military to achieve desired results in the face of changing threats over time.

A new methodology must start with a vision of U.S. national security, as well as the defense strategy to support it, that recognizes vital American interests. For America, uniquely among the great powers of history, securing its vital interests did not mean diminishing those of other nations. Rather, America's defense of its vital interests has supported the economic, social, and political development of the majority of the world's peoples. There is a strong correlation between American interests and those of a liberal and peaceful world order:

After more than two centuries of independence, the United States' vital interests, in our evaluation, have largely remained consistent over long periods of time, with transformative technologies serving as the single greatest reason for change in American interests. In many respects, two centuries of growth and change only served to filter and clarify what is and is not in the national interest. By reinforcing the enduring nature of the nation's interest, events such as World War I & II, the Cold War, and the attacks of September 11, 2001 have not fundamentally reshaped what matters most.¹³

In the past, it has been America's tendency to focus both strategic analyses and force planning on

the demands of the war-fighting mission. Certainly, at present, the minimum standard for the U.S. military is to be able to fight two MRCs.

It is necessary but insufficient to evaluate the adequacy of the U.S. military against the standard of its ability to fight its nation's wars. Instead, a new methodology must recognize that today and for the foreseeable future, the U.S. military is the linchpin in the global security system.

Indeed, most U.S. vital interests have to do with issues related to maintenance of a stable international order: freedom of the seas and airways, access to trading partners, maintenance of a community of like-minded liberal democracies, and deterrence of would-be regional aggressors. The international system is not a game of Jenga in which the removal of a critical support structure merely results in one's tower collapsing. Helping to maintain a peaceful international order is a vital U.S. national security interest.

Toward a New Strategic Concept

For more than 20 years, it has been an accepted fact of U.S. security policy that the ability to deter regional aggression in two separate regions of the world at the same time—to fight and win two MRCs—also is critical to the maintenance of a peaceful international system. In view of the growing militancy of the regimes in North Korea and Iran, as well as efforts by both Russia and China to assert control over adjacent land, sea, and air spaces, it is difficult to conceive of a time when the two-MRC standard will no longer be applicable.

The Chairman of the Joint Chiefs of Staff, General Martin Dempsey, recently proposed a variation on the regionally focused MRC standard to include Russia and China. He proposed a strategic concept that he calls “two, two, two, one.”

Here's my elevator speech about strategy. Two, two, two, one: Two heavyweights will influence our future strategy, Russia and China. Two middleweights, North Korea and Iran. Two networks, al-Qaida and transnational organized crime from our southern hemisphere. And one domain—cyber. And those things have influenced, are influencing me today and will influence you in the future. One of them or more.¹⁴

What is most noteworthy about General Dempsey's formulation is that it includes both Rus-

sia and China as prospective challengers. While previous defense strategies and each QDR have made reference to the challenges posed by Russia and China, this is the first time that these two countries have been clearly identified as countries with whom the United States must consider the prospect of conflict.

Mapping the two-MRC requirement against the “two, two, two, one” strategic concept raises some interesting questions about the adequacy of the U.S. military. Is the Pentagon capable of fighting two nearly simultaneous regional conflicts against both Russia and China? General Dempsey makes it clear that he does not think war with either nation is likely, particularly if the United States and its regional allies maintain the means to deter them. But to deter, U.S. forces must be able to pose a credible threat at least to Russia’s and China’s presumed or prospective war aims or valuations.

Furthermore, is the U.S. military postured to fight two middleweight powers? Since, as General Dempsey says, these two states are less predictable and more roguish, does America not have to plan to defeat both of them in detail, including changing their regimes? Is a force structure able to defeat in detail one or both middleweight powers essentially adequate to achieve denial/cost imposition against Russia or China?

One approach to force sizing for multiple MRCs that would also match General Dempsey’s strategy would be to consider a conflict with a middleweight power as the full-out conventional conflict and a face-off with Russia or China as requiring the abilities to deny their objectives and/or impose unacceptable costs. In other words, a war with Russia or China would be limited in scope, which seems reasonable considering the large nuclear arsenals that both nations possess.

Strategic Surprises. A new methodology must not only address known challenges; it must also make allowances for the possibility of strategic surprises. The recent blitzkrieg that took the extremist group that goes by the name of the Islamic State of Iraq and al-Sham (ISIS) almost to the gates of Baghdad should be enough to convince any reasonable observer that this is a bad time to be reducing the size of the U.S. military.

As of a few months ago, no one in Washington had even heard of ISIS, and it was just a couple of years ago that President Obama assured the American

people that al-Qaeda and its affiliate groups (one of which, it turns out, was ISIS) were decimated and on the run. Now U.S. “advisers” are back in Iraq, unmanned aerial systems are conducting surveillance missions over the newly declared caliphate, a carrier battle group and amphibious assault ship loaded with Marines are positioned in the northern Arabian Gulf, and air strikes are underway.

This sudden turn of events is ironic in part because one of the central operating assumptions of the Administration’s defense policy was that this country would not again engage in a large-scale and sustained stability operation. This assumption was the basis for slashing the size of the active U.S. Army from a high of 570,000 troops to some 450,000. While President Obama has promised that there will be no American boots on the ground, can we accept this as an ironclad certainty if ISIS threatens to take Baghdad? What about when ISIS turns its attention to Jordan, a long-standing U.S. ally?

The reality is that America’s leaders have generally done a poor job of predicting when, where, and how this nation will fight. Since 1950, three factors have repeatedly saved the U.S. from military disaster: the size of the armed forces, America’s technological superiority, and the robustness of the defense industrial base. For example, the Cold War military was of sufficient size and power to make up for a plethora of strategic and operational mistakes. America discovered, for example, that the B-52s originally acquired to deliver nuclear weapons on Soviet targets were more effective as conventional bombers. Moreover, there were so many B-52s that the Air Force could afford to lose nearly two dozen during Operation Linebacker II over North Vietnam.

Today, all three of these historic sources of salvation are at risk. The military is being reduced to a size at which it will be able to fight one war at best. America’s technological edge is being challenged by prospective adversaries abroad and by a broken acquisition system at home. The U.S. defense industrial base, while still capable of producing world-class weapons systems, lacks the robustness to support a rapid and sustained defense buildup. On its own, the requirements for a robust and responsive defense industrial base should be considered in any new assessment of U.S. military capabilities.

The rise of ISIS is but one of a host of strategic, operational, and technological surprises that have confronted the United States in recent years. If this

nation is going to protect its vital interests, deter conflicts with would-be regional hegemons, reassure allies, and respond to crises of all sorts, it needs a robust military of sufficient size, sophistication, resources, and readiness to deal not only with the known threats, but also with the inevitable surprises. A key measure of the adequacy of U.S. military might is its ability to withstand surprises of all kinds.

A New Approach. Recognizing the limitations of the existing methodology for assessing the adequacy of the U.S. military, the House Armed Services Committee has proposed a new approach that would replace the QDR with two documents: a Quadrennial National Security Threats and Trends report (QNSTR) and a Defense Strategy Review (DSR). This new approach also would give greater responsibility to the National Defense Panel.

The QNSTR would provide a definition of U.S. national security interests, an assessment of trends that could affect those interests, and the identification of threats to those interests, all for multiple time periods. The new DSR would address the manifest inadequacies of the existing QDR process while also significantly expanding the roles and responsibilities of the National Defense Panel, requiring it to consider alternative strategies, force structures, capabilities, and budgets—thereby ensuring that the U.S. military is capable of prosecuting the full range of assigned missions.¹⁵

Finally, an informed public debate about the manner in which the adequacy of U.S. military forces is measured, both quantitatively and qualitatively, requires an informed and forward-looking analytic approach. It is therefore time to revitalize the process of net assessment as part of an overall effort to establish an ongoing, publicly accessible index of U.S. military power. In many ways, doing so in the current fluid security environment will be even more challenging than it was during the Cold War.

America's armed forces are at a crossroads. The American people need to understand not only the role this nation and its military play in the world, but the importance of global peace and stability to the security of the homeland and their personal well-being. They also need to be given the facts: how large and capable a military is required in order to meet America's vital national security interests and what it will realistically cost to acquire and maintain such a military.

The American people need to fully appreciate the risks associated with reducing the U.S. military to the point at which it can only "do less with less." Ultimately, however, the American people need to be convinced that their military will be used in ways that support U.S. interests and that decision makers will make wise use of the resources with which they are provided.

Endnotes:

1. Daniel Gouré and Jeffrey Ranney, *Averting the Defense Trainwreck in the New Millennium* (Washington: Center for Strategic and International Studies, 1999).
2. Victor Davis Hanson, "Obama's World Disorder," The Hoover Institution, *Defining Ideas*, June 24 2014, <http://www.hoover.org/research/coming-world-disorder> (accessed September 15, 2014).
3. See Alain C. Enthoven and K. Wayne Smith, *How Much Is Enough? Shaping the Defense Program, 1961-1969* (Santa Monica, CA: The RAND Corporation, 2005), http://www.rand.org/pubs/commercial_books/CB403.html (accessed September 15, 2014), and Lawrence Freedman, *The Evolution of Nuclear Strategy, Second Edition* (New York: St. Martin's Press, 1989).
4. Paul Bracken, "Net Assessment: A Practical Guide," U.S. Army War College, *Parameters*, Spring 2006, pp. 90-100, <http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/O6spring/bracken.pdf> (accessed October 25, 2014).
5. Thomas Mahnken, ed., *Competitive Strategies: Theory, History, Practice* (La Jolla, CA: Stanford University Press, 2012).
6. U.S. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, January 2012, p. 4, http://www.defense.gov/news/Defense_Strategic_Guidance.pdf (accessed November 3, 2014).
7. Daniel Gouré, "The Measure of a Superpower: A Two Major Regional Contingency Military for the 21st Century," Heritage Foundation *Special Report* No 128, January 25, 2013, <http://www.heritage.org/research/reports/2013/01/the-measure-of-superpower-a-two-major-regional-contingency-military-for-21-century>.
8. U.S. Department of Defense, *Quadrennial Defense Review 2014*, March 2014, p. VI, http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf (accessed November 3, 2014).
9. News release, "2014 IISS Military Balance," International Institute for Strategic Studies, February 3, 2014, <http://www.iiss.org/en/about%20us/press%20room/press%20releases/press%20releases/archive/2014-dd03/february-0abc/military-balance-2014-press-statement-52d7> (accessed August 21, 2014).
10. General James F. Amos, Commandant, U.S. Marine Corps, remarks at the American Enterprise Institute for Public Policy Research, Washington, D.C., February 14, 2014, <http://www.hqmc.marines.mil/Portals/142/Docs/130214---CMC%20Remarks%20@%20American%20Enterprise%20Institute%20%28as%20prepared%29.pdf> (accessed August 21, 2014).
11. General Larry Spencer, testimony before the Subcommittee on Readiness, Committee on Armed Services, U.S. House of Representatives, April 10, 2014, quoted in Blake Neff, "Generals: Two-War Strategy in Jeopardy Under Sequester," *The Hill*, April 10, 2014, <http://thehill.com/policy/defense/203195-two-war-strategy-in-jeopardy-under-sequester-generals> (accessed October 31, 2014).
12. General John Campbell, testimony before the Subcommittee on Readiness, Committee on Armed Services, U.S. House of Representatives, April 10, 2014, quoted in Neff, "Generals: Two-War Strategy in Jeopardy Under Sequester."
13. Adam Lowther and Casey Lucius, "Identifying America's Vital Interests," *Space & Defense*, Vol. No. 1 (Winter 2014), pp. 39-54, http://www.academia.edu/7194994/Identifying_Americas_Vital_Interests (accessed August 21, 2014).
14. General Martin E. Dempsey, speech at the U.S. Naval Academy, Annapolis, Maryland, March 26, 2014, <http://www.jcs.mil/Media/Speeches/tabid/3890/Article/8564/gen-dempseys-remarks-at-the-naval-academy-to-class-of-2014.aspx> (accessed August 21, 2014).
15. Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, H.R. 4435, 113th Cong., 2nd Sess., <https://beta.congress.gov/113/bills/hr4435/BILLS-113hr4435pcs.pdf> (accessed August 21, 2014).

Rebalancing to the Pacific: Asia Pivot or Divot?

Bruce D. Klingner

The Obama Administration heralded its Asia Pivot strategy as a major break from the policies of its predecessor, even proclaiming that the U.S. was now back in Asia as a result. Asia was to be given primacy in American foreign policy, reflecting the importance of the region to U.S. national interests and the drawdown of American involvement in Iraq and Afghanistan.

Yet three years after its introduction, uncertainties linger as to just how significant a policy shift the Asia Pivot actually was. More important, Asian nations are now questioning U.S. military capabilities and resolve—the result of underfunded U.S. defense requirements and perceived American foreign policy missteps.

Perceptions that U.S. rhetoric has not been backed by sufficient resources and commitment and that Washington remains focused on a series of unresolved crises elsewhere can have profound implications for Asia. North Korea and China, for example, may be emboldened to test the United States as they pursue policies that are inimical to peace and stability in Asia.

Asia's Strategic Importance to the United States

Asia has been since the 19th century—and will continue to be—a region of vital importance to the United States. At present, Asia contains more than half of the world's population; two of the three largest global economies (China and Japan); and the world's fastest-growing economies, which generate 40 percent of the world's GDP growth—more than any other region.¹

Asia is America's largest trading partner,² accounting for 38 percent of total U.S. trade in goods for 2013,³ compared with 30 percent with North America⁴ and 20 percent for Europe.⁵ Five of the United States' seven major defense treaties are with Asia-Pacific nations, and Washington has strong partnerships with many other nations in the region.

Consequently, control of Asia by a hostile power would threaten American economic and security national interests. Yet stability in Asia is already being threatened by a number of factors: North Korea's growing military capabilities, China's increasingly aggressive behavior, long-standing sovereignty disputes, historical animosities, and rising nationalism.

In the absence of any regional architecture comparable to either the North Atlantic Treaty Organization or the European Union, the United States has proven to be the only nation with both the capabilities and the historical record necessary to assume the role of regional balancer and “honest broker.” But to reassure allies and deter opponents, the United States must maintain a strong economic, diplomatic, and military presence throughout Asia. Such an unambiguous approach is the key to regional peace and stability.

Continuity in U.S. Asia Policy

For decades, the United States has maintained a significant military presence in the Pacific. As President George H. W. Bush declared in his 1990 East Asia Strategy Initiative, “we believe that our forward pres-

ence in the Asia–Pacific region will remain critical to deterring war, supporting our regional and bilateral objectives, and performing our military missions.”⁶ In the words of Admiral Samuel J. Locklear, III, commander of U.S. Pacific Command (PACOM), “For about the last 70 years, we have been the centerpiece of the security architecture [in the Pacific].”⁷

As the U.S. withdrew military forces from Iraq and Afghanistan, the Obama Administration evaluated the United States’ global security interests and saw the need for greater prioritization to Asia. Secretary of State Hillary Clinton’s seminal “America’s Pacific Century” article in *Foreign Policy* defined the Asia Pivot as “among the most important diplomatic efforts of our time.”⁸ President Barack Obama declared in 2011 that “I have, therefore, made a deliberate and strategic decision—as a Pacific nation, the United States will play a larger and long-term role in shaping this region and its future.”⁹

Emphasizing the reinvigoration of American focus on Asia, President Obama declared that “the U.S. is back in Asia.”¹⁰ The policy was able to build on the efforts of multitudes of U.S. diplomats, businesspeople, and servicemembers who had continued to toil in Asia even as greater priority had been placed on the global war on terrorism.

The Obama Administration points out correctly that the Asia Pivot is a multifaceted strategy that consists of more than just a military component. However, nearly three years after the rollout of the Asia Pivot, many of the details remain undefined, and there is uncertainty as to the extent to which the strategy is different from long-standing U.S. policies in Asia.

Since diplomatic and political engagement is ethereal and success is difficult to measure, some experts have adopted metrics such as “number of meetings in Asia attended by senior U.S. officials” in order to measure the success of the Asia Pivot. For example, the National Defense University assessed that Obama Administration officials have “spent significantly more time in [Asian] regional meetings” than those of his predecessors.¹¹ Meetings are important to affirm alliances, establish rapport among leaders, and push policy objectives; but it is easy to get lost in the procedures and forget that meetings, dialogue, and engagement are *tools* to reach an objective rather than objectives themselves.

Other than new trade agreements, economic interaction with Asia is largely outside of the govern-

ment’s control. Moreover, the major economic components cited as proof of the Asia Pivot—the South Korea–U.S. Free Trade Agreement and the multilateral Trans-Pacific Partnership—were both initiated by the Bush Administration.

Changes in the U.S. military force posture in Asia are thus the most measurable component of the Pivot and the one that lends itself to distinguishing this new prioritization from that of previous Administrations. President Obama pledged in 2012 that the United States “will be strengthening our presence in the Asia Pacific and budget reductions will not come at the expense of that critical region.” Then-Secretary of Defense Leon Panetta affirmed that “[w]e will continue not only to maintain, but to strengthen our presence” in Asia¹² and “increase its institutional weight and focus on enhanced presence, power projection, and deterrence in the Asia–Pacific.”¹³

Secretary of Defense Leon Panetta, during his 2012 Shangri-La Security Dialogue speech, declared that by 2020, the Navy would redeploy its forces from today’s 50/50 split between the Pacific and Atlantic to a 60/40 split in favor of the Pacific. He also stated that there would be six aircraft carriers in the Pacific as well as the majority of U.S. cruisers, destroyers, Littoral Combat Ships, and submarines.¹⁴

Asia Pivot Requires Forces and Funding

The Asia Pivot policy is sound only if the requisite military forces are deployed in the Pacific—a number that must be commensurate with a stated increase in the region’s importance. Without such a deployment, the Pivot will fail to reassure allies or deter potential opponents. Claims that U.S. forces in the Pacific will be immune from duties elsewhere or from budget cuts that will affect the U.S. Joint Force over the next several years simply do not hold water. Though the U.S. Army and Marine Corps were increased by 100,000 troops to handle the Iraq and Afghanistan conflicts, U.S. soldiers and Marines were also removed from Asia to serve in those wars.

Even well before sequestration-mandated budget cuts, it was obvious that the United States was underfunding defense requirements essential to maintaining security commitments in Asia. In February 2012, Panetta testified that the United States would rebalance its force posture to emphasize Asia, but he added that the defense budget maintained only the current bomber, aircraft carrier, and

big-deck amphibious fleets and restored Army and Marine Corps force structure in the Pacific to pre-Iraq and pre-Afghanistan deployment levels.¹⁵

On the surface, the Obama Administration's 2015 budget projections appear to maintain current levels of defense spending. As economist Robert Samuelson points out, defense spending in nominal dollars (unadjusted for inflation) remains static between 2013 and 2024: \$626 billion in 2013 and \$630 billion in 2024.

However, a closer review of these numbers reveals that, once adjusted for inflation, U.S. defense spending drops by 25 percent.¹⁶ It is difficult to envision how the President's Pivot can be executed successfully with such a decrease in defense spending, a point underscored by Secretary of Defense Chuck Hagel, who has stated that, with sequestration budget cuts, the military is in danger of becoming "a hollow force, one that is not ready, one that is not capable of fulfilling assigned missions. In the longer term, after trimming the military enough to restore readiness and modernization, the resulting force would be too small—too small to fully execute the president's defense strategy."¹⁷

Asia Pivot Derailed by Defense Budget Cuts

Although there have been no force reductions in the Pacific as there have been in other commands, the cuts in the overall defense procurement and training budgets have already negatively affected U.S. forces in the Asia-Pacific region. Assistant Secretary of Defense for Acquisition Katrina G. McFarland admitted in March 2014 that as a result of defense budget cuts, "Right now, the [Asia] pivot is being looked at again, because candidly it can't happen."¹⁸

The ability of the U.S. to fulfill its security obligations rests on two factors: the actual number of military forces available and the quality of those forces. Having requisite forces in the long term requires sufficient ongoing funding for their procurement. The quality of those forces is determined in part by adequate training. Current U.S. defense budgets for military forces in the Pacific are insufficient to provide for numbers or quality, let alone both.

Navy. Chief of Naval Operations Admiral Jonathan W. Greenert has told Congress that in order to meet the global needs of combatant commanders, the Navy would need a 450-ship fleet. Currently, the Navy has 289 ships and hopes to achieve a 306-ship fleet by the end of the decade, but attaining 306 ships

would require a shipbuilding budget of \$18 billion per year over the next 20-plus years. Since the current FY 2013–FY 2019 plan is for only \$13 billion per year, "the largest fleet of current ship designs that the Navy would be able to afford is 30% smaller than the goal—or about 220 ships."¹⁹

Representative Randy Forbes (R-VA), Chairman of the Seapower and Projection Forces Subcommittee of the House Armed Services Committee, has expressed concern that "in 2007 we met 90-percent [*sic*] of the combatant commander's requirements. This year we will only meet 43 percent."²⁰ In addition, the current defense budget does not include funding to refuel and overhaul the USS *George Washington*, which could lead the Navy to have to decommission the aircraft carrier. Doing so would reduce the carrier fleet from 11 to 10, despite then-Secretary of Defense Panetta's pledge that "the President of the United States and all of us have decided that it is important for us to maintain our carrier presence at full strength. And that means we'll be keeping 11 carriers in our force."²¹

Given that the Navy historically dedicates from one-third to one-quarter of its deployed fleet to operations in the Pacific, such a dramatic decrease in fleet size can only have a negative impact on the United States' naval capabilities in the region.

Marine Corps. Naval and amphibious operations are the backbone of U.S. military deterrence and defense capabilities in the Pacific. Yet Admiral Samuel Locklear, III, PACOM commander, testified that due to a lack of large amphibious ships, landing craft, and other amphibious vehicles, the Navy and Marine Corps do not have enough assets to carry out contested amphibious operations in the Pacific if a crisis were to arise.²² Locklear added that there is a "continuing demand" for PACOM to provide other deployed and ready forces to the other regional combatant commanders, creating "periods in PACOM where we lack adequate intelligence and reconnaissance capabilities as well as key response forces, ultimately degrading our deterrence posture and our ability to respond."

The Marine Corps has stated that it would need 54 amphibious assault ships to fulfill the validated requirements of all the combatant commanders. That would be the number needed to deploy three Marine Expeditionary Brigades (MEBs), since each MEB requires at least 17 ships for a force of 17,500 Marines and all their gear. But the Navy's shipbuild-

ing budget—a critical factor for U.S. forces in the Pacific—has not been sufficient to meet combatant commander requirements for years, so the Marine Corps and Navy have had to settle for the ability to transport and deploy less than two full MEBs—nearly half of required capabilities.

The most recent Quadrennial Defense Review (QDR) again validated the requirement for 38 amphibious warships to move two MEBs, but current fiscal pressures led to a decline from 33 to 28 warships, meaning that the Corps' actual ability to conduct a large-scale amphibious operation will amount to a mere 1.5 MEBs, or roughly a half-dozen battalions of Marines with their supporting aviation—presuming that all amphibs from around the world were brought together for a single operation. The latest Navy plans do not envision a force of 33 amphibious warships until at least the mid-2020s, which would still meet only two-thirds of the total requirement.²³

Then-Marine Commandant General James Amos warned that defense cuts could “translate into increased loss of personnel and materiel, and ultimately [place] mission accomplishment at risk.”²⁴ Twenty retired Marine Corps generals wrote Congress in March 2014 to warn that the shortage of amphibious ships—and the reduced maintenance of the existing fleet—had “degraded our current national security capabilities and will have negative effects long into the 21st century.”²⁵

Beyond this, Marine Corps fighter squadrons used to have 12–14 aircraft available. Now they usually have 12, but in 2015 that may decrease to eight deployable aircraft per squadron.

U.S. Air Force. The U.S. Air Force has grounded 13 combat squadrons (250 planes), nearly one-third of its active-duty fighter and bomber squadrons. Air Force officials said they have implemented a “tiered readiness” approach for active-duty air combat units and warned that there may not be sufficient combat air power to respond immediately to contingencies. Moreover, for every month a squadron does not fly, it takes an equal number of months to retrain the pilots.²⁶

Recently, the Air Force had to cancel a two-week flying exercise in which units from the Asia-Pacific region and allied air forces would have trained together. The 374th Airlift Wing in Japan had to cut its flying program by 25 percent and cancel its participation in a combined drill in Thailand called Cope Tiger.²⁷

U.S. Army. The Army has had to cut training above squad and platoon levels, including all but one of the Combat Training Center rotations scheduled for brigades this fiscal year. Depot maintenance was also halted, and the Army cut flying hours from aviation training, creating a shortfall of pilots. General Raymond T. Odierno, the Army Chief of Staff, told Congress that “should a contingency arise, there may not be enough time to avoid sending forces into harm’s way unprepared.”²⁸

General Curtis M. Scaparrotti, commander of U.N. and U.S. forces in Korea, testified that he has doubts about America’s ability to counter a large-scale North Korean attack effectively due to the low readiness of forces stationed outside of Korea. He warned that “[a]ny delay in the arrival or reduction in readiness of these forces would lengthen the time required to accomplish key missions in crisis or war, likely resulting in higher civilian and military casualties.”²⁹

In other words, cuts in the defense budget affect the ability of the U.S. military to prepare for and engage in operations in general, but especially the Pivot to Asia.

Reducing Requirements Rather than Providing Resources

The ongoing cuts in the U.S. defense budget reflect President Obama’s intent to reduce U.S. commitments overseas. President Obama perceives that “the tide of war is receding” and with it “the end of long-term nation-building with large military footprints.”³⁰ Defining the overseas threat environment as less hostile, the President has directed a decrease in U.S. defense requirements and capabilities.

President Obama’s 2010 QDR stated that “U.S. forces must plan and prepare to prevail in a broad range of operations [including] conducting large-scale stability operations.”³¹ But his 2012 Defense Guidance reversed this position, saying instead that “U.S. forces will no longer be sized to conduct large-scale, prolonged stability operations” like those in Iraq and Afghanistan.³²

Similarly, President Obama’s 2012 defense guidance advocated jettisoning the long-standing “two war” force-sizing construct. The new, more constrained strategy meant abandoning the decades-long U.S. objective of being able to fight two opponents simultaneously—instead substituting a delaying action against the second opponent.³³

By eliminating the standing U.S. objective of being able to fight two major regional conflicts simultaneously, the President provided himself the justification to slash defense forces. For example, the President noted that there is “significant excess capacity in the U.S. airlift fleets.”³⁴ However, this excess exists only because the President’s new policy no longer required the ability to manage two large conflicts. Furthermore, despite a critical need for transport in the Pacific, President Obama directed the Pentagon to cut 27 C-5, 65 C-130, and 38 C-27 transport aircraft³⁵ even though the Pacific theater—presumably the more important region as proposed in the Asia Pivot strategy—has a much higher requirement for long-range lift than any other due to its geography alone.

Unfortunately, as demonstrated by recent events, the international environment remains a dangerous arena. After Russia annexed Crimea, President Obama dismissed the idea of conflict in Europe as “the kind of thinking that should have ended with the Cold War.”³⁶ He described Russian President Vladimir Putin as operating from a “position of weakness” in Ukraine, despite Putin’s obvious success in carving out a portion of Ukraine’s sovereign territory and fomenting dramatic levels of instability in its eastern region. Similarly, Secretary of State John Kerry opined that “[y]ou just don’t in the 21st century behave in 19th century fashion by invading another country.”³⁷ It seems the leaders of other countries are not inclined to behave as the U.S. would prefer.

Kerry was also uncertain of the need to augment forces in the Pacific as part of President Obama’s Asia Pivot. At his confirmation hearings, Kerry announced:

I’m not convinced that increased military ramp-up is critical yet. I’m not convinced of that.... We have a lot more bases [and forces] out there than any other nation in the world, including China today.... You know, the Chinese take a look at that and say, what’s the United States doing? They [*sic*] trying to circle us?³⁸

The Asia Pivot Is Not Working

America’s Allies Are Not Reassured. During his 2014 Asia trip, President Obama claimed that “our alliances in the Asia Pacific have never been stronger. Our relationship with ASEAN countries in Southeast Asia has never been stronger. I don’t think

that’s subject to dispute.”³⁹ But for all the emphasis on the Asia Pivot, there is little to show in actual, tangible results. Allies are nervous, and opponents are emboldened. Indeed, a prevalent theme of President Obama’s foreign policy and his 2014 Asia trip was built around the need to reassure U.S. friends and allies in the region.

Allies of the United States around the world—not just those in Asia—have expressed grave misgivings about Washington’s capability and resolve to help them defend against escalating security threats. First up were the Europeans, who expressed concern that the Asia Pivot meant a reduced American commitment to their defense. The withdrawal of two U.S. Army brigade combat teams (BCTs) from the continent, cutting in half the BCTs that the U.S. maintained in Europe following the dissolution of the Soviet Union, heightened their trepidation.

Asian allies, initially heartened by the renewed U.S. focus on the region, continue to express concern about China’s unrelenting assertiveness in pushing extralegal sovereignty claims on their territories. The weak U.S. response to Beijing’s bullying led the Philippines, one of just a handful of American treaty allies, effectively to cede its claims to the Scarborough Shoals.

Consequently, an increasingly nervous Tokyo has called repeatedly for stronger U.S. support to deter similar Chinese intimidation against the Japanese-controlled Senkaku Islands. South Korea and Japan watched with growing dismay as Washington first cut \$480 billion from the long-term military budget only to warn then of the catastrophic consequences that sequestration would have for U.S. armed forces. Yet when the sequester hit, slicing an additional \$500 billion, Washington claimed that it could still fulfill American security commitments, though admittedly with “additional but acceptable risk.”⁴⁰

Seoul and Tokyo were flummoxed when Syrian President Assad crossed the U.S. redline against using chemical weapons against civilians and President Obama refused to implement the pledged military response. These allies have privately expressed fears that Washington might similarly abandon its defense commitments to them if North Korea or China attacked.

In early 2013, North Korea ratcheted up tensions by threatening nuclear strikes against the U.S. and South Korea, abrogating the armistice ending the Korean War and nullifying all inter-Korean nonag-

gression pacts. Initially, the United States demonstrated resolve, augmenting forces committed to an annual bilateral military exercise with South Korea. However, Secretary of State Kerry soon revealed that as the crisis continued, the Obama Administration had elected to change course in the face of North Korean threats. Kerry stated during a press conference in Seoul that “President Obama [had] ordered a number of exercises not to be undertaken. We have lowered our rhetoric significantly.”⁴¹

Rather than standing up to blatant belligerence, the United States stepped back, citing the potential for conflict escalation on the Korean peninsula as its primary concern. Secretary Kerry explained, “Let’s face it. Everyone here knows this, we’ve got enough problems to deal with around the world.”⁴² One can only imagine the glee in Pyongyang and the trepidation in Seoul at the U.S.’s prioritizing other regions over defending our Korean ally, in addition to the pall cast over the initial optimism accompanying announcement of the United States’ return to Pacific affairs.

Finally, Russia’s military incursion into Crimea and subsequent U.S. affirmation of support to European NATO nations triggered yet more concerns of a “reverse Asia Pivot.” U.S. officials were dispatched to provide reassurance once again to both European and Asian allies. But the ease with which Putin annexed Crimea and the U.S. inability to prevent it from happening heightened anxiety that China could be emboldened to try a similar seizure in the Pacific.

Opponents Have Not Moderated Behavior. Despite an uptick in meetings in Asia—a case of substituting wingtip shoes for soldiers’ boots—the United States has failed to temper Chinese and North Korean belligerence.

In recent years, Beijing has used military and economic threats, bombastic language, and military bullying to extend its extralegal claims of sovereignty in the East and South China Seas. In November 2013, China declared an Air Defense Identification Zone (ADIZ) over the East China Sea, including the Senkaku Islands, and threatened to use its military to enforce it. Washington condemned the declaration as a provocative act that exacerbated tensions in the region and increased the risks of a military clash. However, U.S. protests and those of other countries in the region have had marginal effect as China continues to maintain the ADIZ.

Beijing attempts to divert attention from its own actions by mischaracterizing Japan as a threat to regional security. China’s bellicose actions have fueled regional concern and have triggered a greater Japanese willingness to confront Chinese expansionism and strengthen the Japanese military. Japan’s willingness to defend its territory has been mischaracterized by China as a resurgence of 1930s imperial Japanese militarism when, in fact, it is a logical response to increased Chinese provocations.

North Korean leader Kim Jong-un has maintained his regime’s threatening behavior and has continued its quest to augment its nuclear and missile-delivery capabilities. North Korea credits Jong-un with being the mastermind behind the regime’s two attacks on South Korea in 2010, which resulted in 50 South Korean deaths. Clearly, the Administration’s current approach to North Korea is insufficient as the Communist nation continues to menace U.S. allies.

Conclusion

For the Asia Pivot to deter aggression, America’s opponents must believe that any belligerent act by them will invite a retaliatory response. Such a response must be able to inflict such cost and pain as to outweigh any potential benefit sought by the aggressor—thereby leading the aggressor to refrain from initiating a military attack in the first place. To deter an adversary, the threat of retaliation must be seen as credible, something that requires both viable military means and a demonstrated unquestionable resolve to use them.

Despite strong pledges of support from U.S. politicians and diplomats, America’s Asian allies will not be reassured—and opponents will not be deterred—if they perceive weakness in either American capabilities or American resolve. America’s slashed defense budgets and unenforced redlines embolden its opponents to practice coercive diplomacy and bully its allies.

North Korea and China could also be tempted to act if either perceives an American public weary of war, an intensely divided U.S. Congress, and U.S. allies even more reluctant than usual to employ military force to counter armed belligerence. Increasingly strained relations between Japan and South Korea over historic issues further complicate matters, as such conflict diverts attention away from current security threats while hindering the development of allied military capabilities.

During his 2014 trip to Asia, President Obama declared support for South Korea and affirmed that the Japanese–U.S. security treaty covers the Senkaku Islands. But for the Asia Pivot policy to be effective, a principled message of affirming U.S. support for international law and defending America’s allies must be backed by resolute U.S. actions, including (1) reversing dangerous defense budget cuts; (2) maintaining a robust forward-deployed U.S. military presence; (3) strengthening and modernizing America’s alliances; and (4) standing up to China’s use of intimidation, coercion, or force to assert a territorial claim.

Endnotes:

1. Press release, "Developing East Asia Slows, but Continues to Lead Global Growth at 7.1% in 2013," The World Bank, October 7, 2013, <http://www.worldbank.org/en/news/press-release/2013/10/07/developing-east-asia-slows-but-continues-to-lead-global-growth-7-1-percent-2013> (accessed September 30, 2014).
2. U.S. Census Bureau, "Top Trading Partners—December 2013: Year-to-Date Total Trade," February 6, 2014, <http://www.census.gov/foreign-trade/statistics/highlights/top/top1312yr.html> (accessed September 16, 2014).
3. U.S. Census Bureau, "Trade in Goods with Asia, 2013: U.S. Trade in Goods with Asia," September 4, 2014, <http://www.census.gov/foreign-trade/balance/c0016.html> (accessed September 16, 2014).
4. U.S. Census Bureau, "Trade in Goods with North America, 2013: Trade in Goods with North America," September 4, 2014, <http://www.census.gov/foreign-trade/balance/c0010.html> (accessed September 16, 2014).
5. U.S. Census Bureau, "Trade in Goods with Europe, 2013: U.S. Trade in Goods with Europe," September 4, 2014, <http://www.census.gov/foreign-trade/balance/c0012.html> (accessed September 16, 2014).
6. Ralph Cossa and Brad Glosserman, "Return to Asia: It's Not (All) About China," Pacific Forum CSIS *PacNet* No. 7, January 30, 2012, <http://csis.org/files/publication/Pac1207.pdf> (accessed September 30, 2014).
7. Jim Garamone, "'Friction Points' Stoke Asia Tensions, Locklear Says," American Forces Press Service, May 30, 2014, <http://www.defense.gov/news/newsarticle.aspx?id=122368> (accessed September 30, 2014).
8. Hillary Clinton, "America's Pacific Century," *Foreign Policy*, October 11, 2011, http://www.foreignpolicy.com/articles/2011/10/11/americas_pacific_century (accessed September 30, 2014).
9. News release, "Remarks by President Obama to the Australian Parliament," The White House, November 17, 2011, <http://www.whitehouse.gov/the-press-office/2011/11/17/remarks-president-obama-australian-parliament> (accessed September 30, 2014).
10. Tom Donilon, "America Is Back in the Pacific and Will Uphold the Rules," *Financial Times*, November 27, 2011, <http://www.ft.com/intl/cms/s/0/4f3febac-1761-11e1-b00e-00144feabdc0.html#axzz1ulp3s0Tq> (accessed September 30, 2014).
11. Phillip Saunders and Katrina Fung, "Wheels Up! Has Obama Really Pivoted to Asia?" *The Diplomat*, July 23, 2013, <http://thediplomat.com/2013/07/wheels-up-has-obama-really-pivoted-to-asia/> (accessed September 16, 2014).
12. Karen Parrish, "Panetta Answers Troops' Questions in Japan," American Forces Press Service, October 24, 2011, <http://www.af.mil/news/story.asp?id=123277060> (accessed September 30, 2014).
13. CNN Wire Staff, "China to Raise Defense Budget by 11%," CNN World, March 4, 2012, http://articles.cnn.com/2012-03-04/asia/world_asia_china-defense-budget_1_defense-budget-defense-spending-xinhua?_s=PM:ASIA (accessed September 30, 2014).
14. Leon E. Panetta, "Secretary of Defense Speech: Shangri-La Security Dialogue," U.S. Department of Defense, June 2, 2012, <http://www.defense.gov/speeches/speech.aspx?speechid=1681> (accessed September 30, 2014).
15. Leon E. Panetta, "Defense Budget Request—Written Submitted Statement" prepared for hearing, *Defense Authorization Request for Fiscal Year 2013 and the Future Years Defense Program*, Committee on Armed Services, U.S. Senate, February 7, 2012, <http://www.armed-services.senate.gov/hearings/oversight-defense-authorization-request-for-fiscal-year-2013-and-the-future-years-defense-program> (accessed September 16, 2014) (emphasis added).
16. Robert J. Samuelson, "Defunding Defense," *The Washington Post*, March 9, 2014, http://www.washingtonpost.com/opinions/robert-samuelson-defunding-defense/2014/03/09/80ee0dda-a7bc-11e3-b61e-8051b8b52d06_story.html (accessed September 30, 2014).
17. News transcript, "Remarks by Secretary [Chuck] Hagel and Gen. [Martin E.] Dempsey on the Fiscal Year 2015 Budget Preview in the Pentagon Briefing Room," U.S. Department of Defense, February 24, 2014, <http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5377> (accessed October 28, 2014).
18. "Obama at West Point," *The Wall Street Journal*, May 28, 2014, <http://online.wsj.com/articles/obama-at-west-point-1401318998> (accessed September 30, 2014).
19. Captain Arthur H. Barber III, "Rethinking the Future Fleet," U.S. Naval Institute *Proceedings*, Vol. 140, No. 5 (May 2014), <http://www.usni.org/magazines/proceedings/2014-05/rethinking-future-fleet> (accessed September 16, 2014).
20. Kris Osborn, "CNO Tells Congress the US Needs 450-Ship Navy," *Military.com*, March 12, 2014, <http://www.military.com/daily-news/2014/03/12/cno-tells-congress-the-us-needs-450-ship-navy.html> (accessed September 30, 2014).
21. Phil Stewart, "U.S. Won't Cut Carrier Fleet to Fix Budget, Panetta says," Reuters, January 22, 2012, <http://www.reuters.com/article/2012/01/22/us-usa-defense-idUSTRE80L0OR20120122> (accessed September 16, 2014).
22. Jon Harper, "Commander: US Military Can't Conduct Amphibious Operations in the Pacific," *Stars and Stripes*, March 25, 2014, http://www.stripes.com/news/commander-us-military-can-t-conduct-amphibious-operations-in-the-pacific-1.274419?utm_medium=twitter&utm_source=dlvr.it#.UzG4nvZXenA (accessed September 16, 2014).

23. "Document: Letter From 20 Retired Marine Generals to Congress Calling for More Amphibious Warships," USNI News, March 27, 2014, <http://news.usni.org/2014/03/27/document-letter-20-retired-marine-generals-congress-calling-amphibious-warships> (accessed September 16, 2014).
24. General James F. Amos, Commandant, U.S. Marine Corps, "The Future of the Military Services and the Consequences of Sequestration," statement before the Committee on Armed Services, U.S. House of Representatives, November 2, 2011, p. 8, http://armedservices.house.gov/index.cfm/files/serve?File_id=08eaf78f-203b-4804-ad15-8593b91a86e2 (accessed November 3, 2014).
25. "Document: Letter From 20 Retired Marine Generals to Congress Calling for More Amphibious Warships."
26. Steve Vogel, "Budget Cuts Leave Air Force Pilots Twisting in the Wind," *The Washington Post*, May 27, 2013, http://www.washingtonpost.com/politics/budget-cuts-leave-air-force-pilots-twisting-in-the-wind/2013/05/27/a9e20bce-c329-11e2-8c3b-0b5e9247e8ca_story.html (accessed September 16, 2014).
27. Yuka Hayashi and Patrick Barta, "Pentagon Cuts Feared Tripping Up Pivot to Asia," *The Wall Street Journal*, May 3, 2013, <http://online.wsj.com/news/articles/SB10001424127887324582004578456683694045890> (accessed September 16, 2014).
28. David Ignatius, "Sequestration Is Feeding a Slow-Motion Decay," *The Washington Post*, June 21, 2013, http://www.washingtonpost.com/opinions/david-ignatius-sequestration-is-feeding-a-slow-motion-decay/2013/06/21/874be74c-d9ef-11e2-a016-92547bf094cc_story.html (accessed September 16, 2014).
29. General Curtis M. Scaparrotti, Commander, United Nations Command; Commander, United States–Republic of Korea Combined Forces Command; and Commander, United States Forces Korea, statement before the Committee on Armed Services, U.S. Senate, March 25, 2014, http://www.armed-services.senate.gov/imo/media/doc/Scaparrotti_03-25-14.pdf (accessed September 16, 2014) (emphasis added).
30. U.S. Department of Defense, *Defense Budget Priorities and Choices*, January 2012, p. 7, http://www.defense.gov/news/Defense_Budget_Priorities.pdf (accessed September 16, 2014).
31. U.S. Department of Defense, *Quadrennial Defense Review Report*, February 2010, http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf (accessed November 4, 2012).
32. U.S. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, January 2012, http://www.defense.gov/news/defense_strategic_guidance.pdf (accessed November 4, 2014).
33. U.S. Department of Defense, *Defense Budget Priorities and Choices*.
34. Ibid.
35. Ibid.
36. Katie Zezima, "Obama: Europe Not 'Battleground Between East and West,'" *The Washington Post*, March 24, 2014, <http://www.washingtonpost.com/blogs/post-politics/wp/2014/03/24/obama-europe-not-battleground-between-east-and-west/> (accessed September 16, 2014).
37. Will Dunham, "Kerry Condemns Russia's 'Incredible Act of Aggression' in Ukraine," Reuters, March 2, 2014, <http://www.reuters.com/article/2014/03/02/us-ukraine-crisis-usa-kerry-idUSBREA210DG20140302> (accessed September 16, 2014).
38. Andrew Browne, "China's World: The U.S. 'Pivot' Toward Asia Takes Another Turn," *The Wall Street Journal*, September 10, 2013, <http://online.wsj.com/news/articles/SB10001424127887323595004579064980509607984> (accessed September 16, 2014).
39. "Remarks by President Obama and President Benigno Aquino III of the Philippines in Joint Press Conference," The White House, April 28, 2014, <http://www.whitehouse.gov/the-press-office/2014/04/28/remarks-president-obama-and-president-benigno-aquino-iii-philippines-joi> (accessed November 4, 2014).
40. Stephanie Condon, "Obama Unveils New Defense Strategy," CBS News, January 5, 2012, <http://www.cbsnews.com/news/obama-unveils-new-defense-strategy/> (accessed November 4, 2014).
41. John Kerry, "Remarks With Republic of Korea Foreign Minister Yun Byung-se After Their Meeting," U.S. Department of State, April 12, 2013, <http://www.state.gov/secretary/remarks/2013/04/207427.htm> (accessed September 16, 2014).
42. Ibid.

The Importance of Special Operations Forces Today and Going Forward

Steven P. Bucci, PhD

In the post-9/11 period of war and subsequent military drawdown, Special Operations Forces (SOF) appear likely to grow in numbers, funding, and importance—but not necessarily in general understanding. One of the most flexible and useful instruments in America’s national security toolbox, SOF are regularly referred to incorrectly, incompletely, and with little depth of knowledge by policymakers.

SOF are neither a panacea nor an insignificant oddity. If utilized correctly, they bring great benefit to the nation; used poorly, their capabilities and sometimes their lives are wasted. How, then, should this nation think about these compelling and often mythologized warriors and their role in supporting America’s vital national interests?

During times of austerity, the government often looks for ways to get “more bang for the buck.”¹ When this budgetary philosophy is applied to the military, SOF, with their reputation for doing great things with fewer troops and resources than large conventional forces, seem like a bargain. This vision of a “surgical” capability that is made up of mature, “hard” professionals who make the right choices at the right time and that avoids the need to deploy larger formations of citizen soldiers at great expense can be very compelling.

Given America’s current fiscal difficulties, there is a growing danger of overutilizing or misapplying SOF, but this is not to say that SOF should not be used. In fact, SOF can and should be a major enabler for other elements of power as well as a shaper of

security conditions that can minimize the need for larger deployments of conventional military forces. Getting this balance right is the key challenge for the military and policymakers.

This essay will address numerous issues regarding Special Operations Forces while attempting to answer several questions, including:

- How SOF serve as a tool of U.S. military efforts,
- How SOF provide strategic warning and prepare the environment,
- How SOF enable hard power by providing conventional forces a “warm start” and create options not otherwise possible, and
- How SOF amplify the effectiveness of hard power by doing things like leveraging infrastructure and using their ability to exploit actions/successes.

Finally, this essay will review SOF’s potential as a bridging capability during this time of strained resources. SOF will be a key part of America’s ability to meet the challenges of an increasingly worrisome threat environment while its conventional forces are in decline. Although they are not a substitute for other capabilities in the U.S. military, SOF can mitigate risk by helping to set the operating environment in the most advantageous manner possible.

Special Operations: A Primer

The term “Special Operations Forces (SOF)” is the only correct generic term for the organizations being discussed. It includes certain designated units of all services and all capabilities. First and foremost, SOF are the men and women that make up the units. They are, for the most part, mature and highly trained. A typical special operator (regardless of service or specialty) is married with a family; averages 29–34 years old; has at least eight years on active duty in the general purpose forces (GPF); has some cultural and language training (most are masters of cross-cultural communication); has attended numerous advanced-skills schools; and has at least some college education, if not multiple degrees (this includes the enlisted ranks).²

SOF competently operate a great deal of highly advanced U.S. military equipment and are also proficient with the equipment of other services and countries. They are valued for their out-of-the-box thinking, imagination, and initiative. SOF can and do operate with a small footprint and can survive and thrive with a very light support tail. These SOF are seen as the consummate military professionals and as such are “detached from Main Street” in ways that the 18–22-year-olds in the general-purpose forces are not.

The Department of Defense defines Special Operations (SO) as operations that:

Require unique modes of employment, tactical techniques, equipment, and training often conducted in hostile, denied, or politically sensitive environments and characterized by one or more of the following: time sensitive, clandestine, low visibility, conducted with and/or through indigenous forces, requiring regional expertise, and/or a high degree of risk.³

There are some who claim that conventional forces can and do handle tasks that SOF handle. Yet SOF are often entrusted to perform missions that exceed the authority given to conventional military units, such as operating in “politically sensitive environments” or executing tasks that require special legal authorities.

Organizational Structure

To appreciate how SOF are “special,” one must understand how these forces are organized and how they operate.

U.S. Special Operations Command. The parent command of all SOF is U.S. Special Operations Command (USSOCOM), which is headquartered at MacDill Air Force Base in Tampa, Florida.⁴ Established in 1987, USSOCOM is responsible for manning, training, and equipping all SOF units. It does this in conjunction with the four services, which also provide the troops to the SOF units. Although not a service branch, USSOCOM has certain service-like responsibilities including the procurement of SOF-specific items as needed.

SOCOM has had some disagreements with the services over funding, authorities, and which units get assigned to USSOCOM; it also has sparred with the Geographic Combatant Commanders (GCCs) over the authority to direct SOF missions. Currently, USSOCOM enjoys the widest operational mandate it has ever had and is seen by both the services and the GCCs as a very positive contributor to national security. USSOCOM maintains manning, training, and equipping responsibilities for deployed forces through the Theater Special Operations Commands (TSOCs) that are under the operational control of each GCC. The GCCs operationally manage the TSOCs, but USSOCOM’s worldwide situational awareness allows them to synchronize operations across GCC boundaries.

There are five major subcomponents to USSOCOM: U.S. Army Special Operations Command (USASOC); Navy Special Warfare Command (NSW); Air Force Special Operations Command (AFSOC); Marine Corps Forces Special Operations Command (MARSOC); and Joint Special Operations Command (JSOC)—one for each service with an additional multiservice special mission command. Each of these organizations contributes something unique to the special operations community. They have different roles and tend to specialize in certain types of missions or areas of operation.

Direct vs. Indirect Approaches

SOF operations fall broadly into two categories: direct and indirect. The direct approach consists of SOF raids and other operations that directly target the enemy, such as an operation executed by Navy SEALs to free American and Danish aid workers held by Somali pirates.⁵ According to Admiral William H. McRaven, former Commander of SOCOM:

The direct approach is characterized by technologically-enabled small-unit precision lethality, focused intelligence, and interagency cooperation integrated on a digitally-networked battlefield.... Extreme in risk, precise in execution and able to deliver a high payoff, the impacts of the direct approach are immediate, visible to [the] public and have had tremendous effects on our enemies' networks throughout the decade.⁶

Such missions are typically brief (even if planning for them can be extensive) and usually carry a higher potential for the use of weapons; to use a popular description, they tend to be more "kinetic."

The indirect approach is characterized by long-term commitments of SOF to help enable and aid other nations to improve their own military forces and security. McRaven explains:

The indirect approach includes empowering host nation forces, providing appropriate assistance to humanitarian agencies, and engaging key populations. These long-term efforts increase partner capabilities to generate sufficient security and rule of law, address local needs, and advance ideas that discredit and defeat the appeal of violent extremism.⁷

While the direct approach is focused on addressing immediate situations such as disrupting terrorist operations, the indirect approach is longer-term and seeks to prevent threatening situations from arising or to defuse them with the lowest investment of U.S. assets. One of the main ways it does this is by equipping U.S. partners to address their own security challenges more effectively. This approach can also be a key to ending larger conflicts on favorable terms.

U.S. Army Special Operations Command. The U.S. Army Special Operations Command (USASOC) has its headquarters at Fort Bragg, North Carolina, and is the largest component of USSOCOM (28,500 troops) with troops spread across the country and some overseas. It has six different types of units under its control: Special Forces, Rangers, Special Operations Aviation, Civil Affairs, Military Information Special Operations, and Special Operations Sustainment.⁸

U.S. Army Special Forces Command is the parent headquarters of all Special Forces (SF) soldiers,

more commonly known as Green Berets.⁹ They have five active-duty groups. Each is traditionally oriented on a region, but this has been stretched by the wars of the past decade, which required all the SF units to rotate into the fight: Pacific (1st Group); Africa (3rd Group); the Middle East (5th Group); Latin America (7th Group); and Europe (10th Group, Fort Carson, Colorado).¹⁰ There are also two National Guard Groups (19th and 20th), which augment their active-duty counterparts.

SF units are generally older and more experienced than their fellow SOF. They are specialists in working with foreign militaries. Green Berets, for example, perform both direct missions and indirect tasks (discussed further below). They operate in 12-man teams, often remote in relation to other American forces.

The 75th Ranger Regiment is another element of USASOC. It is headquartered at Fort Benning, Georgia, and commands three battalions of what are considered the finest special light infantry troops in the world.¹¹ While they are organized much as other light infantry units are organized, the Rangers' level of training, readiness, and deployability exceeds that of their non-SOF counterparts. Although they are often used in small elements (squad, platoon, or company), the full weight of the Rangers is demonstrated when they perform battalion-level assaults and raids. They operate primarily as a direct action force.

The 160th Special Operations Aviation Regiment (SOAR) has a variety of highly modified rotary-wing platforms. They are stationed at Fort Campbell, Kentucky, and have three battalions organic to the regiment. Known as the Night Stalkers, they leverage not just their advanced and highly specialized equipment, but also their proficiency at operations conducted in the dark. Their aircraft (AH-6/MH-6 Little Birds, MH-60K/L/M Black Hawks, and MH-47 Chinooks) can be refueled in flight, have additional avionics and protective measures beyond the conventional models of these rotorcraft, and have added weaponry. The 160th delivers, provides fire support and supplies to, and (most important) exfiltrates other SOF elements under the most arduous conditions. Their ethos of leaving no one behind makes them a highly sought-after partner for any military operation.

The 95th Civil Affairs Brigade (CA), another resident of Fort Bragg, includes five battalions. Civil Affairs greatly expanded after it was realized in

Afghanistan and Iraq that there was a greater need for active-duty units of this sort. There is a great deal of additional CA capability in the U.S. Army Reserve. These troops are specialists in operating with the civilian elements of another country's government and economy with expertise ranging from airports to water systems. They can be deployed to assess the needs of a certain region pre-conflict, during combat operations, or post-conflict. They can also assist friendly elements in improving foreign civil structures. They support other SOF units but are regularly assigned to support conventional operations as well.

The 4th Military Information Support Group (MISG) is also stationed at Fort Bragg and has two subordinate MISG groups under its command.¹² Formerly known as Psychological Operations, Military Information Special Operations (MISO) are highly versatile units that often use persuasive methods to convince targeted audiences to act in ways that are desirable to U.S. objectives. From tactical loud-speaker teams that might ask citizens to evacuate a town to strategic leaflet drops to inform an entire region that it would be beneficial to them to surrender, MISO units can be as powerful a weapon as any kinetic or lethal tool.

Also stationed at Fort Bragg, the 528th Sustainment Brigade has medical, logistics, and signal units that support not only Army SOF, but other elements of the U.S. military as well.¹³ These troops provide strategic abilities that deploy as often as their more combat-oriented fellow special operators. Two National Guard companies are aligned with the battalion in the 528th.

Naval Special Warfare Command. Naval Special Warfare Command (NSWC), headquartered at Coronado, California, is comprised of nearly 9,000 sailors.¹⁴ Its operational arms are the six Naval Special Warfare Groups. Each of these elements is organized differently and home-stationed on either the East or West Coast. They are made up of a combination of Sea, Air, Land (SEAL) operators, Special Warfare Combatant-craft Crewmen, and Enablers.

The SEALs are one of the SOF's best-known elements, renowned for their physical toughness and extremely exclusive selection process. Although clearly specialists at maritime-related operations, they perform operations far from water as well. If Army Special Forces are primarily indirect operators that can also perform direct action missions, SEALs are primarily direct operators who can also

perform indirect training missions. Their specialty is small-unit commando actions and support for amphibious operations. As their name implies, they can be deployed through a multitude of means, including the SEAL Delivery Vehicle (a type of open mini-submarine).¹⁵

In the same way the SEALs often support the conventional Navy, the Navy often supports the SEALs, providing infiltration platforms such as attack submarines. The NSWC Combatant-craft Crewmen operate multiple vessels such as the MK V Special Operations Craft, the Special Operations Craft Riverine, and NSW Rigid-hull Inflatable Boat that deliver and recover the SEALs.¹⁶ The NSW Groups also utilize talented Enablers in communications, intelligence, and explosive ordnance disposal (EOD) to augment SEAL operations.

Air Force Special Operations Command. Air Force Special Operations Command (AFSOC), stationed at Hurlburt Field, Florida, is probably the most diverse among the services' SOF components. It has 18,000 members spread across the U.S., Europe, and Asia. Under AFSOC's command is the 23d Air Force, three active-duty Special Operations Wings, two Special Operations Groups, one Air Force Reserve Special Operations Wing, and one Air National Guard Special Operations Wing.¹⁷

One of AFSOC's responsibilities is Pararescue, whose personnel are nicknamed "PJs."¹⁸ These highly skilled operators are medical specialists qualified in multiple infiltration techniques to execute recovery operations. Their mission is "To rescue, recover, and return American or Allied forces in times of danger or extreme duress."¹⁹

The Combat Controllers (CCT), another type of AFSOC personnel, are men who specialize in managing air assets from the ground.²⁰ They can guide aerial bombardments or set up expedient airfields and act as the air traffic control tower. CCT include Special Operations Weathermen who habitually infiltrate into denied areas with other SOF elements to provide weather and intelligence support.

AFSOC also includes Combat Aviation Advisors.²¹ These are pilots and support personnel who work directly with foreign air forces as advisors and trainers. They train to become proficient in whatever systems and aircraft their allies operate. They must also be capable of political, cultural, and linguistic interaction with America's foreign partners.

Finally, there are all of SOF's aircrews. These teams operate numerous fixed-wing (such as AC-130H/U gunships, MC-130E/H infil/exfil, EC-130J MISO platform, MC-130P refueler, and MC-130J and MC-130W multipurpose) and tiltrotor-wing (CV-22B Osprey) aircraft. Powerful and versatile, these aircraft are the long-range lifeline of SOF.

Marine Corps Forces Special Operations Command. Marine Corps Forces Special Operations Command (MARSOC) is the newest of SOF's service components. Established in 2006, MARSOC recognizes the growing need to provide additional numbers of highly skilled operators who can both teach and train allied foreign military forces while maintaining proficiency in direct action missions. Its mission is "to be America's force of choice to provide small lethal expeditionary teams for global special operations."²²

While numbering only 2,600, these Marines filled a critical gap and have become an essential part of the special operations community. Headquartered at Camp Lejeune, North Carolina, the Command oversees the Marine Special Operations Regiment with three battalions of Critical Skills Operators. They also command an SO Support Group, an SO Intelligence Battalion, and the Marine SO School.

Joint Special Operations Command. Joint Special Operations Command (JSOC) is the final component of USSOCOM and is headquartered at Fort Bragg.²³ This organization's primary responsibility is to act as a special test and evaluation element for advanced SOF equipment and techniques.²⁴

JSOC also includes a highly classified unit at the joint headquarters for America's Tier One Countering Terrorism (CT) Special Mission Units (SMU). They have assigned elements from the other components, notably SEAL Team 6 and 1st Special Forces Operational Detachment-Delta. JSOC also has other support (intelligence and communications) units and maintains close relationships with various units from all of the other Commands. The missions given to JSOC are regularly clandestine and are not attributed to its elements.

SOF Operational Methodologies and Ethos: The "SOF Truths"

There is insufficient space here for an in-depth review of the entire history and experience of each element in SOF. It is possible, however, to provide a broad outline of SOF operations.

As noted, all missions assigned to SOF can be categorized as either direct or indirect. Direct missions are executed by the U.S. SOF units themselves, normally unilaterally, and are designed to have a specified result within a well-defined period of time, usually of very short duration. Indirect missions are executed by working with other elements (usually foreign forces aligned with the U.S.) and tend to have longer time horizons.

Each of the various SOF elements focuses closely on some missions while maintaining the ability to perform all others. Specifically:

- **U.S. Army Special Forces:** Primarily indirect actions; habitually operate in small groups; can also perform direct missions.
- **SEALs:** Primarily direct actions; operate in small groups, near the water (but also operate on land and at sea as their name indicates); can also perform indirect training missions.
- **Rangers:** Primarily direct, large-scale operations; can perform smaller operations.
- **Marine Critical Skill Operators:** Primarily indirect; still maintain capability to perform direct missions.
- **Military Information Special Operations:** Indirect; can support direct actions of other units (either SOF or General Purpose).
- **Civil Affairs:** Indirect; can support direct actions of other units (either SOF or General Purpose).
- **Air Force Aviation Advisors:** Indirect.
- **Combat Controllers, Pararescue, Special Operations Weathermen:** Direct or indirect; can support any function as well as all missions.

There is, however, another way to encapsulate the approach to their missions that all SOF share. Referred to as "SOF Truths," the following maxims apply across SOF and help to explain the mindset and ethos of special operators. They are a constant reminder to all members of SOF as to what comprises their professional foundation and what should inform decisions on the use of SOF.²⁵

- **SOF Truth #1: Humans are more important than hardware.** People—not equipment—make the critical difference in the success or failure of a mission. The right people, highly trained and working as a team, will accomplish the mission with the equipment available. On the other hand, the best equipment in the world cannot compensate for a lack of the right people.
- **SOF Truth #2: Quality is better than quantity.** A small number of people, carefully selected, well-trained, and well-led, is preferable to larger numbers of troops, some of whom may not be up to the task.
- **SOF Truth #3: Special Operations Forces cannot be mass produced.** It takes years to train operational units to the level of proficiency needed to accomplish difficult and specialized SOF missions. Intense training, both in SOF schools and in units, is required to integrate competent individuals into fully capable units. This process cannot be hastened without degrading ultimate capability.
- **SOF Truth #4: Competent Special Operations Forces cannot be created after emergencies occur.** Creation of competent, fully mission-capable units takes time. Employment of fully capable special operations capability on short notice requires highly trained and constantly available SOF units in peacetime.
- **SOF Truth #5: Most special operations require non-SOF assistance.** The operational effectiveness of deployed forces cannot be, and never has been, achieved without being enabled by all the joint service partners. The Air Force, Army, Marine and Navy engineers, technicians, intelligence analysts, and numerous other professions that contribute to SOF have substantially increased SOF capabilities and effectiveness throughout the world.

These are not mere slogans; they are the principles by which SOF view themselves, their missions, and their world. Taking a moment to digest these ideals is worth the time and will allow for a higher degree of understanding of the men and women who make up USSOCOM. These five truths offer key insights into America's Special Forces, such as:

- SOF are precious assets that take time, effort, and investment to develop;
- They are not suitable for “big-scale” tasks;
- Suddenly deciding to “make more” of them is a foolish and irresponsible goal; and
- SOF recognize that they are a small part of America's military strength, not a replacement for any other part of the military.

Policymakers who consider employing SOF operationally must understand these facts lest they gamble with one of America's most precious assets.

SOF Core Activities

According to the Department of Defense, “USSOCOM organizes, trains, and equips SOF for special operations core activities ... and other such activities as may be specified by the President and/or SecDef. These core activities reflect the collective capabilities of all joint SOF rather than those of any one Service or unit.”²⁶ The activities enumerated by SOCOM are:²⁷

- **Direct Action (DA).** Short-duration strikes in hostile, denied, or diplomatically sensitive environments to seize, destroy, capture, exploit, recover, or damage designated targets.
- **Special Reconnaissance (SR).** Reconnaissance and surveillance normally conducted in a clandestine or covert manner to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces.
- **Countering WMD Operations (CWMD).** Support provided to GCCs through technical expertise, matériel, and special teams to locate, tag, and track WMD and/or conduct DA to prevent use of WMD or to assist in its neutralization or recovery.
- **Counterterrorism (CT).** Actions taken under conditions not conducive to the use of conventional forces to neutralize terrorists and their networks in order to render them incapable of using unlawful violence.

SOF Core Activities

WHAT	TYPE	WHO	EXAMPLE
DA	Direct	SF, Rangers, SEALs, CSOs	Raids, strikes, terminal guidance
SR	Direct	SF, Rangers, SEALs, CSOs	Long-range recon of strategic target
CWMD	Direct	SF, Rangers, SEALs, CSOs	Capturing a loose nuclear device
CT	Direct	JSOC, SF, SEALs	The raid to kill Osama bin Laden
UW	Indirect	SEALs, SF, CSOs, CA	Operations against the Taliban 2001
FID	Indirect	CSOs, SF, SEALs,	Training Iraqi and Afghan Armies
SFA	Indirect	SF, CSOs, SEALs, CA	Training Iraqi Military
HRR	Direct	SF, Rangers, SEALs, CSOs	Rescue of PFC Jessica Lynch
COIN	Indirect	All SOF	Operations in Iraq 2003-2011
FHA	Indirect	SF, MISO, CA, CSOs	Ebola mission to West Africa
MISO	Both	MISO, CA, SF, CSOs	Convincing insurgents to give up
CAO	Indirect	CA, SF, MISO, CSOs,	Helping local sheik to deliver food

- Unconventional Warfare (UW).** Actions taken to enable an indigenous resistance movement to coerce, disrupt, or overthrow a government or occupying power.
- Foreign Internal Defense (FID).** Activities that support a country's internal defense program designed to protect against subversion, lawlessness, insurgency, terrorism, and other threats to the country's internal security and stability.
- Security Force Assistance (SFA).** Activities that contribute to a broad effort by the U.S. government to support the development of the capacity and capability of foreign security forces and their supporting institutions.
- Hostage Rescue and Recovery (HRR).** Sensitive crisis response missions in response to terrorist threats and incidents where SOF support the rescue of hostages or the recapture of U.S. facilities, installations, and sensitive material overseas.
- Counterinsurgency (COIN).** SOF support to a comprehensive civilian and military effort to contain and ultimately defeat an insurgency and address its root causes. SOF are particularly adept at using an indirect approach to positively influence segments of the indigenous population.
- Foreign Humanitarian Assistance (FHA).** SOF support to a range of DOD humanitarian activities conducted outside the U.S. and its territories to relieve or reduce human suffering, disease, hunger, or privation. SOF can rapidly deploy with excellent long-range communications equipment, and they are able to operate in the austere and often chaotic environments typically associated with disaster-related HA efforts. Perhaps the most important capabilities found within SOF for FHA are their geographic orientation, cultural knowledge, language capabilities, and ability to work with multiethnic indigenous populations and international relief organizations to provide initial and ongoing assessments.
- Military Information Support Operations (MISO).** MISO are planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives.
- Civil Affairs Operations (CAO).** CAO are actions that enhance the operational environment, identify and mitigate underlying causes of instability within civil society, or involve the application of functional specialty skills that are normally the responsibility of civil government.

The varying nature of these activities tends to differentiate between direct and indirect. Furthermore, certain SOF components are more prone to undertake some types of activities over others, although all SOF can be called upon to execute any of these activities if the situation demands. It should be noted that all of the direct missions and some of the indirect missions could and in all likelihood would require support from Army or Air Force aviation assets or NSW craft, as well as PJs, CCTs, and SO Weathermen.

As described, the responsibilities and capabilities of SOF are broad and comprehensive. They play many roles and perform them all with an extremely high level of proficiency. These missions can be simple and tactical, or they can be highly complex and have extremely critical strategic effects. One important thing to note is that SOF never think that they conduct Major Combat Operations alone. This is not humility; it is simple recognition that SOF have their limitations.

How SOF Enables Military Capabilities

SOF are not a panacea for all of this nation's military challenges. However, when used correctly in conjunction with the rest of the American military in support of U.S. national security objectives, SOF can help to make a difference in achieving strategic objectives.

To illustrate this point, it is helpful to overlay SOF's direct and indirect capabilities across the phases of a major military operation:

- **Phase 0:** Shape the situation in the target country (or theater).
 - **Phase I:** Deter the adversary from taking any adverse actions.
 - **Phase II:** Seize the initiative before the adversary can do so.
 - **Phase III:** Dominate the enemy.
 - **Phase IV:** Stabilize the situation.
 - **Phase V:** Enable the friendly civil authorities.
 - **Phase 0:** Return to shaping the situation.
- Within each phase, SOF have a role to play that creates conditions for success and amplifies the effects of other elements of national power. For example:
- **Phase 0 (Shape)**
 1. **Type of Action:** Indirect.
 2. **SOF Activities:** Information and intelligence gathering; building relationships; conducting training; on-the-ground familiarization; keeping the friendly elements functioning.
 3. **Example of Mission:** A rotating training mission conducted on a fairly continuous basis in Kuwait. A small SF training team would provide year-round instruction, tailoring their actions to the specific needs of the Kuwaitis. They also get to know all of the leaders of the units with whom they work.
 - **Phase I (Deter)**
 1. **Type of Action:** Primarily indirect.
 2. **SOF Activities:** Advising local security forces; helping to eliminate threats to the friendly regime through more direct intelligence support.
 3. **Example of Mission:** The forces sent to Mali before the larger intervention by the French as they fought forces backed by al-Qaeda.
 - **Phases II-IV (Seize, Dominate, and Stabilize)**
 1. **Type of Activity:** Direct and indirect.
 2. **SOF Activities:** Long-range reconnaissance; terminal guidance; deep precision strikes; advisory role with local military; advisory role with coalition partners; advisory role with local civil defense forces; CT hunting; raids; cutting supply lines.
 3. **Example of Mission:** In these active combat phases, SOF are often subordinated to conventional forces in the theater and attacks targets at their direction, providing special reconnaissance before conventional

attacks. These forces can also be sent after strategic targets such as the elimination or capture of high-value personnel. They can also provide liaison officers to help overcome allied communications difficulties or to aid in managing supporting assets such as close air support.

- **Phase V (Enable)**

1. **Type of Activity:** Primarily indirect with some isolated direct activities.
2. **SOF Activities:** Continue advisory role; continue gathering intel; bridge the time between the departure of U.S.–Coalition forces and the stepping-up of local capabilities; monitor final resolution of enemy forces or demobilization process.
3. **Example of Mission:** In this phase, SOF can be the key to a smooth turnover of responsibility to the local authorities and departure of American GPF. This was done in Iraq in 2011 as SOF were the last units to leave—an effort to ensure that the Iraqis had the best possible chance of success when the Americans returned home.

- **Phase 0 (Shape)**

1. **Type of Activity:** Indirect.
2. **SOF Activities:** Return to information and intelligence gathering, the building of relationships and networks, training, on-the-ground familiarization, keeping the friendly elements functioning.
3. **Example of Mission:** A small SF training team would provide year-round instruction, tailoring their actions to the specific needs of the Kuwaitis.

As described, SOF are involved across the spectrum of operations from peacetime to conflict to war and back again. The relationships and intelligence that these operators gain in the pre-conflict Phase 0 are critical in maintaining awareness and supporting stabilizing agents in areas of conflict or

interest. If a scenario moves to Phase I, SOF members can act as an early deterrent force, sometimes with their own actions but more than likely by facilitating a local force’s ability to operate more effectively. During Phases II–IV, their direct activities will support conventional general-purpose forces operations, and their indirect ones can keep the host force (be it a resistance force or government forces) in the fight.

The indirect operations of SOF become even more evident in Phase V as U.S. forces try to set the conditions for the general-purpose forces to depart once local authorities no longer need assistance. From there, SOF can stay in smaller pre-conflict numbers to return to their indirect activities and shaping functions.

While SOF may be known publicly more for direct operations such as the bin Laden strike, the indirect shaping activities are arguably more important to long-term U.S. interests and can save a great many lives and assets. As noted, SOF provide strategic warning and, if necessary, prepare the environment for general-purpose forces. SOF enable hard power by providing conventional forces with a “warm start” and can provide options not otherwise possible. Finally, SOF amplify the effectiveness of hard power by doing things like *in situ* targeting, leveraging of infrastructure, and using their ability to exploit actions based on detailed local knowledge and relationships.

SOF’s Abilities to Execute Missions Effectively

On any given day, U.S. Special Operations Forces are operating in about 75 different countries, mostly in non-combat operations.²⁸ Due to the nature of the many dispersed threats facing the U.S. today, SOF’s unique capabilities are also in higher demand than at any other point in their history.²⁹

Assessing the readiness of SOF involves six key questions:

1. Do SOF have the appropriate doctrine: Are the missions the right ones?
2. Does USSOCOM have the correct numbers of forces: Are they adequately sized?
3. Do SOF have the appropriate diversity of personnel: Is the force mix right?

4. Do SOF have the best equipment to do the job: Are the platforms and equipment what are really needed?
5. Are all forces appropriately trained and experienced: Do the personnel have the right skills, abilities, and experience?
6. Does USSOCOM have the correct authorities: Can SOF legally perform actions required of them?

SOF Doctrine. The SOF doctrine is comprehensive and appropriate. It provides for maximum coverage of the various tasks that SOF are called to execute. Units that can perform the Core SO Activities effectively within the Core SO Operations are provided the tools to complete their tasks.

In the early years of SOF, the doctrine was a mix of different approaches, standards, definitions, and perspectives. USSOCOM's efforts to reconcile variations has provided a common direction, has established uniformity as and where necessary, and allows the commanders and planners to know what the troops theoretically are capable of doing while giving unit operators exactly the guidance they need to develop their training regimes. Additionally, the doctrine is tied to the wider Defense Department Joint Doctrine in a way that maximizes the ability to leverage SOF to enable the General Purpose Forces (GPF) and to achieve the best support from the GPF for SOF operations.³⁰

Size of USSOCOM. SOF has grown significantly since 9/11, but is that growth enough?³¹ To make such a determination, one needs to discuss the broader U.S. military reductions that are taking place.³² While reducing the number of conventional ground forces overall—and specifically in the Middle East—is current U.S. policy, such cuts do not make for sound defense policy and, in fact, harm the ability of SOF to do their job in two key ways:

- Since SOF depend so heavily on conventional forces for organic combat support and combat service support,³³ the drawdown of Army and Marine Corps end strength “brings up concerns the services might be hard-pressed to establish and dedicate enabling units needed by USSOCOM while at the same time adequately supporting general purpose forces.”³⁴
- Because SOCOM draws its operators and support staff from the various services, a decrease in the size of the conventional force subsequently decreases the recruiting pool on which SOCOM relies for quality personnel.³⁵

With the coming drawdown in Army and Marine end strength but no apparent reduction in the requirements generated by U.S. global strategy, SOF will likely see an increase in operational tempo. The current force is about 67,000 personnel, a figure slated to increase to 70,000 over the next several years, of which around 12,000 can be deployed at any given time.³⁶ However, the strict requirements for entry into the SOF and the emphasis on retaining a top-tier fighting force limit the growth rate for SOF expansion. The maximum growth rate per year without sacrificing quality is about a 3 percent to 5 percent increase in personnel.³⁷

Combined with the greater use of SOF, this low growth rate will put additional pressure on an already stretched force. As Mackenzie Eaglen, defense expert at the American Enterprise Institute, points out:

While some in Congress have been concerned about the readiness of the U.S. military and troops on their fifth or sixth combat tour, many special forces operators have already served 10 or more overseas combat tours. That pace is unsustainable with even marginal growth of SOF.³⁸

One can conclude that despite the growth of SOF (both current and planned), they are probably only marginally at an appropriate size for the present and coming missions. This is a concern because the pressure on SOF to pick up a greater share of duties will be strong. The questions of force size and quality relative to operational demand must be monitored closely.

SOF Diversity of Force Capabilities. There must be sufficient redundancy to meet surge requirements and unforeseen challenges. Events in multiple parts of the world cannot necessarily be dealt with sequentially and often require simultaneous actions. No individual service component has enough forces to ensure that no gaps will ever develop, but as a whole, USSOCOM appears—at present—to have ample diversity to cover its global responsibilities.

The direct and indirect capabilities construct is a useful guide, as the various forces can move between the two methodologies with enough skill to address various challenges. For instance, SEALs are able to fight deep in mountainous terrain, Army Special Forces can execute SCUBA insertions from submarines, and Marine CSOs can train indigenous forces or perform a raid—all examples of this critically important redundancy. Army SOA can deliver SOF personnel from any service on a counterterrorist strike and then operate alongside Air Force CV-22 Ospreys to deliver supplies to a CA team in an urban area.

The bottom line is that the force mixture gives America a great deal of resilience. If troops are lost or needed elsewhere, USSOCOM has multiple options to replace them with forces from multiple sources. Such diversity of force capabilities is one of SOF's greatest strengths.

SOF Equipment. The units in SOF are more about the people than gear, but operators need specialized tools to perform their specialized tasks; in fact, it is the effective pairing of highly developed skills and the right equipment that enables SOF to do what they do. For the most part, SOF have received the equipment they deem necessary. Their fixed-wing, rotary-wing, and tiltrotor aircraft are typically substantially upgraded versions of GPF models.³⁹ Certain units in SOF have commercially available “add-ons” to weapons and communications gear, but for the most part, SOF carry many of the same items as their conventional counterparts. There is, however, a constant struggle to ensure that they continue to be properly equipped.

USSOCOM has its own acquisition authority (Major Force Program 11) that allows the command to buy items outside of the normal service channels' acquisition processes.⁴⁰ While the services are currently excellent at providing for the needs of their component units, if budget reduction trends continue, this support may become problematic, and MFP 11 can help SOF to sustain their ability to provide for their own specialized equipment needs. SOF are therefore adequate in this measurement.

SOF Training and Experience. SOF personnel are experienced and well-trained. The youngest personnel in SOF enter with extensive GPF experience, while the more mature members in some cases have been deployed in combat nearly constantly for more than a decade. It is possible that SOF are the most combat-experienced command in U.S. history.

Yet there is one area in which SOF, due to the high operational tempo in combat operations, lack experience: indirect actions. Army SF personnel in particular (but also some Navy SEALs and parts of AFSOF) have not undertaken indirect activities for years. This presents a potential training challenge for SOF, although a correction may already be underway. Former USSOCOM Commander Admiral William McRaven began working to shift the command from a nearly single-minded focus on counterterrorist, direct action operations back to the critical Phase 0 indirect activities that were not prioritized while the operators fought al-Qaeda in Iraq and Afghanistan (with the exception of some indirect training missions performed in both of those countries).

The current USSOCOM Commander, Army General Joseph L. Votel, appears ready to continue Admiral McRaven's plans for a global SOF network that would connect America's special operators with like-minded units from around the world both to improve and to leverage their capabilities.⁴¹ Such a network represents classic indirect operational focus; it is safe to assume that in short order, USSOCOM will make up for any training deficiency in its indirect skill set.

In the future, if USSOCOM has its training budget cut in a manner similar to what many GPF are facing, their ability to maintain their absolutely necessary high levels of readiness will be jeopardized. For now, however, this does not seem to be an immediate possibility. That said, any budget cuts must be monitored closely for the simple reason that SOF operators' unparalleled effectiveness derives primarily from the fact that they shoot more, fly more, and conduct realistic exercises more than any other units in history. Lose that edge, and SOF will lose one of the important characteristics that make them so special.

SOF Authorities Under Which USSOCOM Operates. SOF have largely received the legal authority necessary for them to perform their missions. Under Admiral McRaven, USSOCOM was able to secure expanded authority for SOF operations within the GCC Theaters and receive a consensus approval from the senior military commanders and service chiefs to do so.⁴² Admiral McRaven also expanded the command's presence in Washington and across the federal interagency system. USSOCOM now has the ability to synchronize SOF

operations around the world, and it does this without overstepping the authorities of the Geographic Combatant Commanders or U.S. ambassadors who represent the U.S. in their respective countries.⁴³

Conclusion

Given SOF's relatively solid posture and future, as well as their ability to execute subtle yet critical indirect activities, they may be the most advantageous force choice for the difficult period America is entering. Between the lack of appetite in both American government and the public for large-scale force deployments, as well as the fiscal difficulties facing the GPFs, SOF will likely be required to assume increasing amounts of responsibility.

It is hoped that lawmakers will reverse the U.S. military's decline. Until that time, however, policymakers might be tempted to consider SOF as an alternative way to boost military capacity in the immediate future. The indirect activities performed by USSOCOM will likely be called upon increasingly to provide for the protection of American interests or at least to mitigate the threats to those interests.

In that spirit, the following should be understood about Special Operations Forces:

- There are different types of SOF that have different purposes, values, and skills.
- The health and effectiveness of SOF are tightly linked to the professional health of the conventional forces: One cannot be substituted for the other.
- The nature of SOF and the missions they perform enables the U.S. to engage with the world in ways and to an extent not possible with conventional forces alone.
- Understanding how to use SOF properly preserves conventional force capabilities and capacities.

SOF can prepare areas where the U.S. anticipates that military operations might be necessary, is already conducting operations, or is trying to avoid becoming more involved in a given conflict or operation. Properly used, SOF can preclude problems altogether, reduce the size of conflicts if greater force is deemed necessary, amplify the effectiveness of conventional forces, establish relationships with indigenous forces of both state and non-state actors, provide precise targeting, and give high-resolution awareness that maximizes the likelihood of operational success. They can do all of this with a small footprint and while avoiding unintended or undesired damage.

SOF will be a key part of any bridge strategy as America manages a declining military structure in the midst of a growing threat environment. They can help to set the operating environment in the most advantageous manner possible. They are not, however, a replacement for conventional capabilities.

Indeed, there are numerous missions that SOF cannot perform: They cannot fight pitched battles with heavy forces; they cannot execute naval power projection; they cannot deploy strategic nuclear weapons. Furthermore, without an adequate recruitment base, SOF are hard to sustain, and without adequate conventional support, it becomes more difficult either to deploy SOF or to provide them with adequate support. When used correctly, however, SOF are extraordinarily valuable, even irreplaceable, in advancing U.S. security interests.

Such proficiency does come with a cost, as SOF are an expensive asset when compared "man to man" with conventional forces—and wasteful to taxpayers if they are misused. Policymakers must therefore strike an important balance: correctly deciding where, when, and for what purpose SOF should be deployed. There is simply no substitute for a strong and capable conventional ground force, but the same is true for SOF. Yet these units are not interchangeable, and it is unwise to place additional stress on SOF by expecting them to take on tasks for which they are not intended.

Endnotes:

1. Today's austerity is in the form of the Budget Control Act of 2011 and subsequent "sequester" automatic cuts.
2. United States Special Operations Command, *U.S. Special Operations Command Fact Book 2013*, p. 55, http://www.socom.mil/News/Documents/USSOCOM_Fact_Book_2013.pdf (accessed September 10, 2014).
3. U.S. Department of Defense, Joint Chiefs of Staff, *Special Operations*, Joint Publication 03-05, July 16, 2014, p. ix, http://www.dtic.mil/doctrine/new_pubs/jp3_05.pdf (accessed September 10, 2014).
4. United States Special Operations Command, "About USSOC," <http://www.socom.mil/Pages/AboutUSSOCOM.aspx> (accessed September 27, 2014).
5. Jeffrey Gettleman, Eric Schmidt, and Thom Shanker, "U.S. Swoops in to Free 2 from Pirates in Somali Raid," *The New York Times*, January 25, 2012, http://www.nytimes.com/2012/01/26/world/africa/us-raid-frees-2-hostages-from-somali-pirates.html?_r=1&pagewanted=all (accessed September 28, 2014).
6. Admiral William H. McRaven, USN, Commander, U.S. Special Operations Command, posture statement before the Committee on Armed Services, U.S. Senate, 112th Cong., March 6, 2012, http://www.fas.org/irp/congress/2012_hr/030612mcraven.pdf (accessed September 28, 2014).
7. Ibid.
8. United States Army Special Operations Command, "USASOC Headquarters Fact Sheet," <http://www.soc.mil/USASOCHQ/USASOCHQFactSheet.html> (accessed September 29, 2014).
9. Ibid.
10. American Special Ops, "Special Forces," <http://www.americanspecialops.com/special-forces/> (accessed September 16, 2014).
11. United States Army Special Operations Command, "75th Ranger Regiment," <http://www.soc.mil/Rangers/75thRR.html> (accessed September 29, 2014).
12. United States Army Special Operations Command, "4th Military Information Support Group," <http://www.soc.mil/4th%20MISG/4thMISG.html> (accessed September 29, 2014).
13. United States Army Special Operations Command, "528th Sustainment Brigade, Special Operations (Airborne)," <http://www.soc.mil/528th/528th.html> (accessed September 29, 2014).
14. Naval Special Warfare Command, "Mission," <http://www.public.navy.mil/nsw/Pages/default.aspx> (accessed September 29, 2014).
15. Navy SEAL Museum, "SEAL Delivery Vehicles Manned Combatant Submersibles for Maritime Special Operations," <https://www.navysealmuseum.org/home-to-artifacts-from-the-secret-world-of-naval-special-warfare/seal-delivery-vehicles-sdv-manned-submersibles-for-special-operations> (accessed September 29, 2014).
16. Lee Ann Obringer, "How the Navy SEALs Work," How Stuff Works, <http://science.howstuffworks.com/navy-seal14.htm> (accessed September 29, 2014).
17. Air Force Special Operations Command, "Fact Sheet Alphabetical List," <http://www.afsoc.af.mil/AboutUs/FactSheets.aspx> (accessed September 29, 2014).
18. Air Force Special Operations Command, "Pararescue," August 12, 2014, <http://www.afsoc.af.mil/AboutUs/FactSheets/Display/tabid/140/Article/494098/pararescue.aspx> (accessed September 29, 2014).
19. Ibid.
20. Air Force Special Operations Command, "Combat Controllers," August 12, 2014, <http://www.afsoc.af.mil/AboutUs/FactSheets/Display/tabid/140/Article/494096/combat-controllers.aspx> (accessed September 29, 2014).
21. SOFREP (Special Operations Forces Report), "Combat Aviation Advisors: A Day in the Life," <http://sofrep.com/combat-aviation-advisors/a-day-in-the-life/> (accessed September 29, 2014).
22. U.S. Marine Corps Forces Special Operations Command, "About," <http://www.marsoc.com/mission-vision/> (accessed September 16, 2014).
23. GlobalSecurity.org, "Joint Special Operations Command (JSOC)," <http://www.globalsecurity.org/military/agency/dod/jsoc.htm> (accessed September 29, 2014).
24. United States Special Operations Command, "Joint Special Operations Command," <http://www.socom.mil/Pages/JointSpecialOperationsCommand.aspx> (accessed September 29, 2014).
25. United States Army Special Operations Command, "SOF Truths," <http://www.soc.mil/USASOCHQ/SOFTruths.html> (accessed September 29, 2014).
26. U.S. Department of Defense, *Special Operations*, p. II-2.
27. These activities and their summarized or restated descriptions are taken from *ibid.*, pp. II-1 to II-18.
28. Jim Garamone, "Special Ops, Conventional Forces Work Together, Admiral Says," American Forces Press Service, February 7, 2012, <http://www.defense.gov/news/newsarticle.aspx?id=67097> (accessed September 29, 2014).

29. Robert Martinage, "Special Operations Forces: Future Challenges and Opportunities," Center for Strategic and Budgetary Assessments, 2008, <http://www.csbaonline.org/publications/2008/11/special-operation-forces-future-challenges-and-opportunities/> (accessed September 29, 2014).
30. U.S. Department of Defense, *Special Operations*.
31. Hearing, *The Future of U.S. Special Forces: Ten Years After 9/11 and Twenty-Five Years After Goldwater-Nichols*, Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, U.S. House of Representatives, 112th Cong., 2nd. Sess., September 22, 2011, http://fas.org/irp/congress/2011_hr/sof-future.pdf (accessed September 29, 2014).
32. For a comprehensive overview of U.S. military capacity and capability across the services, see the "Capabilities" section of this report.
33. Michael D. Lumpkin, Acting Assistant Secretary of Defense for Special Operations/Low-Intensity Conflict, "The Future of U.S. Special Operations Forces: Ten Years After 9/11 and Twenty-Five Years After Goldwater-Nichols," statement in hearing, *The Future of U.S. Special Operations Forces: Ten Years After 9/11 and Twenty-Five Years After Goldwater-Nichols*.
34. Andrew Feickert, "U.S. Special Operations Forces (SOF): Background and Issues for Congress," Congressional Research Service, June 26, 2012, <http://www.fas.org/sgp/crs/natsec/RS21048.pdf> (accessed July 22, 2012).
35. Ibid.
36. Marcus Weisgerber, "Spec Ops to Grow as Pentagon Budget Shrinks," *Army Times*, February 7, 2012, <http://www.armytimes.com/news/2012/02/defense-spec-ops-to-grow-as-pentagon-budget-shrinks-020812/> (accessed September 29, 2014).
37. McRaven, posture statement before Senate Committee on Armed Services.
38. Mackenzie Eaglen, "What's Likely in New Pentagon Strategy: 2 Theaters, Fewer Bases, A2AD," *Heritage Foundation Commentary*, December 20, 2011, <http://www.heritage.org/research/commentary/2011/12/whats-likely-in-new-pentagon-strategy-2-theaters-fewer-bases-a2ad>.
39. American Special Ops, "Special Operations Aircraft," <http://www.americanspecialops.com/aircraft/> (accessed September 29, 2014).
40. Defense Acquisition University, "Glossary of Defense Acquisition Acronyms and Terms," <https://dap.dau.mil/glossary/pages/2192.aspx> (accessed September 29, 2014).
41. Claudette Roulo, "Votel Takes Charge of Special Operations Command," U.S. Department of Defense, <http://www.defense.gov/news/newsarticle.aspx?id=123032> (accessed September 29, 2014).
42. Donna Miles, "New Authority Supports Global Special Operations Network," U.S. Department of Defense, <http://www.defense.gov/news/newsarticle.aspx?id=120044> (accessed September 29, 2014).
43. Matthew C. Weed and Nina M. Serafino, "U.S. Diplomatic Missions: Background and Issues on Chief of Mission (COM) Authority," Congressional Research Service, March 10, 2014, <https://www.hsdl.org/?view&did=751906> (accessed September 29, 2014).

Strategic Capabilities in the 21st Century

Michaela Dodge and David R. Inserra

Conventional and special operations forces are the most obvious expressions of U.S. military strength. Whether well-understood or not, they are the most visible manifestations of U.S. defense capabilities—especially since the terrorist attacks of September 11, 2001. Less visible and certainly less understood, but equally as vital to any defense of America’s national interests, are three other capabilities: nuclear weapons, satellites, and cyber. Two of these capabilities—nuclear weapons and satellites—have been a part of defense calculations since the 1950s; cyber is a new domain that has emerged coincident with the evolution of the Internet and rapid development of computer-based information and communications technologies.

During the Cold War years, the U.S. made enormous investments to achieve and sustain a dominant position in nuclear and space affairs relative to the Soviet Union. Nuclear and space systems are seldom in the public eye these days but for different reasons.

Nuclear (then atomic) weapons made their appearance with the bombings of Hiroshima and Nagasaki that ended World War II and then became a central element of war planning during the 1950s and early 1960s. After taking a backseat to reporting on the conventional war in Vietnam, they surged back into prominence in the 1970s as tensions with the Soviet Union again became the dominant security issue.

Above-ground testing ended in 1963, and all other “yield producing” testing was halted in 1992, fol-

lowed shortly by the U.S. decision to take its nuclear weapons off “ready alert” status as one of several measures implemented after the end of the Cold War. The “peace dividend” decade of the 1990s served to push nuclear matters even further off the public radar, with visibility (and even interest) clouded further by a decade of focus on counterinsurgency and counterterrorism operations.

Yet America’s strategic security guarantees—for itself and to key allies—rest on its nuclear triad of aircraft-delivered bombs and land-based and submarine-based missiles. Of concern, then, is the almost complete absence of an informed debate about the health of America’s nuclear enterprise.

Similarly, there is almost no public discussion about the health of the United States’ space-based capabilities and the extent to which America depends on them not only in military affairs, but also economically and in broader national security matters. The military and intelligence communities and some portions of the economic sector are very aware of the importance of space. There is little public awareness, however, of the constant effort needed to maintain and upgrade the space-based systems that enable communications both at home and abroad and allow for the safe movement of nearly all forms of transportation that depend on the positioning, navigation, and timing (PNT) signals broadcast by Global Positioning System (GPS) satellites.

As for cyber, the economic, banking, and financial services sectors are at least as aware as the military and intelligence communities of the importance of

this domain, within which information is continuously exchanged and through which attacks are constantly executed. Due to the sensitive nature of almost all factors bearing upon this topic, very little accurate information is available assessing the United States' capabilities and status relative to competitors. Nevertheless, no discussion of America's vital national interests and the relevant capabilities necessary to protect them would be complete without some understanding of this domain and the lengths to which the United States and others go in order to protect their interests.

Each of these areas is qualitatively and quantitatively different from the tools and environments normally associated with conventional "hard power." Yet without them, the exercise of such power would be nearly impossible. In the sections that follow, we will examine each of these unique strategic capabilities and outline the challenges that America faces in guarding its interests in all three areas.

Nuclear Weapons

In the waning days of World War II, the U.S. developed the ability to harness atomic power for military purposes. The U.S. started its program out of a concern that Nazi Germany would develop such a mighty weapon first and, as a result, win the war. As things turned out, the combined conventional forces of the Allied Powers defeated Germany, and it was Japan that experienced the power of the atomic bomb.

On August 6, 1945, the U.S. dropped the "Little Boy" bomb on Hiroshima, Japan. Highly enriched uranium provided the fuel for this bomb. Little Boy had the destructive equivalent of about 12 to 14 kilotons (12,000 to 14,000 tons) of TNT. The destruction caused by the attack has been compared to the bombing of the German city of Dresden in February 1945. In the Dresden attack, as many as 3,300 tons of bombs were dropped on the city by almost 1,300 bombers.

The second atomic bomb—the plutonium-based "Fat Man"—was dropped on Nagasaki three days after Hiroshima. These explosions marked the end of one of the most destructive conflicts in the history of mankind.

Over the next 40 years, a small set of technologically advanced countries developed atomic/nuclear weapons, including the U.S., the Soviet Union, the United Kingdom (U.K.), France, China, and India.¹

Beginning in 1945, the nuclear powers conducted thousands of nuclear weapons tests and yield-producing experiments of various weapon designs under a variety of conditions, with related advances in the ability to deliver nuclear weapons in different ways (missiles, bombers, strike aircraft, ships and submarines, and artillery) with increasing range and accuracy.

For many states, ballistic missiles remain the preferred means for delivering a nuclear weapon. This is because a ballistic missile attack maximizes the element of surprise for the attacker and the missiles can be deployed in a variety of survivable ways and are difficult to intercept. With intercontinental ballistic missiles (ICBMs) and submarine-launched ballistic missiles (SLBMs), it takes only half an hour to deliver a nuclear weapon from any launch location to a target anywhere in the world.

While experts usually distinguish between strategic nuclear weapons (heavy bombers, intercontinental-range ballistic missiles, strategic submarines) and tactical nuclear weapons (short-range and medium-range systems), it is important to keep in mind that any use of a nuclear weapon is strategic in its nature and consequences. Nuclear weapons are qualitatively and quantitatively different from conventional weapons.²

Nuclear command and control is essential both to nuclear deterrence and to maintaining the credibility of the U.S. nuclear weapons arsenal. America must be absolutely sure that the U.S. will be able to communicate with its nuclear platforms and that the President will be able to launch U.S. nuclear-armed delivery systems should a need to do so ever arise. It is also one of the most classified elements of the program. U.S. nuclear command and control is redundant, reliable, secure, and capable even though the U.S. needs to continue to modernize the network as new electronic warfare capabilities emerge.

The decades before the end of the Cold War were marked by an intense competition between the U.S. and the Soviet Union that led to increases in their respective nuclear weapons arsenals by tens of thousands. This multi-decade competition also necessitated a new level of thinking about warfare, deterrence, operational employment concepts, wargaming, and analysis of effects.

Nuclear forces have been a vital component of U.S. force structure. They have been the bedrock of the United States' posture for deterring strategic

attacks against the U.S. itself and its allies under the policy of extended deterrence and assurance. They have also been an essential component of U.S. policy for limiting the proliferation of nuclear weapons.

As former Heritage analyst Baker Spring points out, due to their enormous destructive power packed in a relatively small weapon, nuclear weapons are different from conventional weapons. Nuclear weapons can defeat conventional weapons because of the unique nature and magnitude of their effects: massive blast, direct radiation, fallout, and electromagnetic pulse.³ These qualitatively different effects of nuclear weapons compared to conventional weapons led policymakers to attempt to develop frameworks through which awesome atomic power would be restrained.⁴

Initially, the U.S. explored options for disarmament and international control of nuclear technology. The most prominent proposal was the Baruch Plan, named after Bernard Baruch, U.S. representative to the United Nations Atomic Energy Commission, who presented a U.S. disarmament plan to the commission on June 14, 1946.⁵ The Baruch Plan proposed putting all atomic energy activities under the control of an International Atomic Development Authority. The plan would have required the renunciation of atomic bombs and would have established a system for punishing violators. It envisioned ending the manufacture of atomic bombs, disposing of existing bombs, and limiting possession of the technological knowledge needed to produce bombs to the authority. In other words, the U.S. attempted to eliminate the potential for atomic warfare immediately after its inception.

The Soviet Union, however, rejected the Baruch Plan. Consequently, with the start of the Cold War, the U.S. turned to exploring plans for using its nuclear forces to contain the military expansion of the Soviet Union. U.S. proposals for limiting nuclear arsenals—specifically, arms control and nonproliferation—were among the less ambitious diplomatic options compared to the Baruch Plan. In this context, two subsequent strategies emerged.

First, in the early 1960s, strategist Herman Kahn proposed that the U.S. should adopt a damage-limitation strategy to deter a possible Soviet attack on the United States and its allies. Kahn defined deterrence broadly to encompass both the goal of limiting the damage that would normally be inflicted by an attack that targeted one's offensive forces—a coun-

terforce approach⁶—and the defensive measures necessary to achieve that goal, along with possession of one's own offensive nuclear forces. "I agree with our current national policy that the primary objective of our military forces is to deter war," Kahn said, summarizing his strategy. "However, I feel that there is a second but still very important objective: to protect life and property if a war breaks out."⁷

Second, at roughly the same time, economist and game theorist Thomas Schelling proposed that deterrence be defined much more narrowly. He argued that the goal of damage limitation and the accompanying protective measures were actually at odds with deterrence. While Kahn felt that strong defenses would cause an enemy not to attack, Schelling believed that an attacker would be deterred more effectively by fear that his own valued resources might be attacked. More specifically, Schelling argued that deterrence meant threatening to retaliate by targeting the attacker's population centers:

Thus, schemes to avert surprise attack have as their most immediate objective the safety of weapons rather than the safety of people. Surprise-attack schemes, in contrast to other types of disarmament proposals, are based on deterrence as the fundamental protection against attack. They seek to perfect and to stabilize mutual deterrence—to enhance the integrity of particular weapon systems. And it is precisely the weapons most destructive of people that an anti-surprise-attack scheme seeks to preserve—the weapons whose mission is to punish rather than to fight, to hurt the enemy afterwards, not to disarm him beforehand. A weapon that can hurt only people, and cannot possibly damage the other side's striking force, is profoundly defensive: it provides its possessor no incentive to strike first.⁸

Schelling's retaliation-based deterrence strategy, which the Administration of Lyndon B. Johnson fashioned into a policy of mutually assured destruction (MAD), eschewed defenses, downplayed counterforce capability, and relied instead on survivable offensive strategic nuclear forces to provide for U.S. security. In fact, Schelling's strategy asserted that strategic defenses would be destabilizing by undermining the capacity of the retaliatory force, at least

in the context of the Soviet threat and its accompanying bipolar international political structure. It explicitly argued in favor of mutual vulnerability for the populations and industrial capacities of the U.S. and the Soviet Union so that each side would fear the loss of its people and economy and would thus be deterred from attacking the other.

During the remainder of the Cold War, debate between proponents of these two schools of thought continued. On balance, however, Schelling's strategy of retaliation-based deterrence proved more popular during the Cold War and was a more powerful driver of the U.S. strategic force posture, although every subsequent Administration rejected the pure version of assured destruction.⁹

Both Kahn's damage-limitation strategy and Schelling's retaliation-based deterrence strategy were designed to prevent nuclear war in the bipolar structure of the Cold War. Neither, however, was designed to meet the security needs of the U.S. and its allies in today's multipolar world. And both Kahn's and Schelling's constructs assumed that the possessors of nuclear weapons would be states led by rational actors, an assumption whose merits are debated in today's world. While Schelling's strategy may have proved more popular during the Cold War, a variant of Kahn's strategy is better suited to meeting U.S. and allied security needs in a multipolar world marked by the proliferation of nuclear weapons and delivery systems.

Implications of Limits on Nuclear Testing. Concerns about the environmental and potential public health consequences of nuclear weapons detonations also led to early efforts to limit and restrict nuclear weapons testing. For instance, the U.S. and the Soviet Union entered a moratorium on atmospheric nuclear weapons test explosions between 1958 and 1961.

Washington was surprised when it learned that during the moratorium, the Soviets were preparing to undertake the largest series of nuclear tests ever conducted; Moscow unilaterally resumed atmospheric tests in 1961. The U.S. was also surprised to learn how quickly competency can be lost; when the U.S. resumed its own testing, it found a significant decrease in its competency to test nuclear weapons.¹⁰

Nuclear weapons testing is currently subject to four major international agreements: the 1963 Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space, and under Water (also known

as the Limited Test Ban Treaty); 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 (also known as the Outer Space Treaty), which prohibits nuclear weapons tests on the Moon and other celestial bodies; the 1974 Treaty on the Limitation of Underground Nuclear Weapon Tests (also known as the Threshold Test Ban Treaty), which bans nuclear weapons tests above 150 kilotons; and the 1976 Treaty Between the United States of America and the Union of Soviet Socialist Republics on Underground Nuclear Explosions for Peaceful Purposes.

In addition, there are other international agreements that indirectly affect states' abilities to test nuclear weapons, such as agreements that established the treaties on nuclear-weapons-free zones. These agreements limit tests that would have a destructive impact on the environment.

It is important to understand that weapons in the current U.S. stockpile were designed and developed to meet stringent Department of Defense requirements during the Cold War. The current stockpile is thus based on technology from the 1970s. During the Cold War, key requirements addressed nuclear safety; operational reliability; yield; conservative use of nuclear materials (i.e., using no more material than is absolutely necessary); and operational simplicity.¹¹ They were driven primarily by the demands of Cold War deterrence based on the policy of mutually assured destruction, with the Soviet Union as the prime adversary.

During the Cold War, the United States replaced or modernized its weapons every 10–15 years, vastly increasing their capabilities over time.¹² Testing was considered essential throughout the entire operational cycle of a nuclear weapon. However, this testing did not focus on building databases or tools that would make it possible to ensure the reliability of weapons if testing ever ceased, because the technical feasibility of this approach was rejected.¹³ Thus, the often cited argument that the United States has enough data to continue to confirm the reliability of its stockpile is open to question since both the data and the tools used to collect them are Cold War vintage and were never meant to be used in the absence of new data.

The military requirements of the 1970s also affected how the United States designed its delivery systems: bombers and, in particular, inter-

continental-range ballistic missiles and submarine-launched ballistic missiles. Missiles have to withstand extreme temperatures and stresses during acceleration and re-entry to deliver the warhead to its intended target. Each type of warhead has to be carefully integrated with its delivery vehicle to ensure that the system as a whole will perform exactly as intended.

Given that America is preparing to recapitalize its delivery platforms, such exacting technical specifications could pose a challenge for U.S. engineers. These platforms will have to be made to “fit” the existing warheads, which means that their designs and parameters will have to be more conservative and perhaps different from missions for which the U.S. would design its warheads if it could start over.

The United States today has the oldest nuclear weapons arsenal it has ever had. The average age of U.S. nuclear warheads is approaching 27 years, which is well beyond their originally intended operational life.¹⁴ Since 1992, the nation has been under a self-imposed moratorium on “yield-producing” experiments and has been relying on the Stockpile Stewardship Program (SSP) that, while it does include a suite of experiments, does not include explosive testing or the maintenance of existing warheads. At the heart of the SSP are supercomputers and computer codes based on data from previous nuclear tests and yield-producing experiments that were conducted between the late 1950s and 1992.

As nuclear weapons age, they depart from their tested envelopes, which, as noted, were developed decades ago. As a result, there is inherent risk in not performing explosive tests to confirm safety and reliability. This raises a question about whether the computer codes that American scientists and engineers use to predict and certify nuclear performance are correct. As David Sharp, chief scientist at the Los Alamos National Laboratory, points out:

The only unequivocal way to demonstrate that predictions made with simulation codes meet expected standards of confidence is by establishing a track record of correct and reliable predictions that have been made using that code. For nuclear weapons this means successful prediction of nuclear performance. A track record of this kind is the essential reality check on claims of predictive capabilities; it is the indispensable source of confidence that is needed if codes are

ever to replace nuclear tests. However, the ability to make correct, reliable predictions of nuclear performance using codes has not been demonstrated and cannot be demonstrated without a nuclear test program.¹⁵

The documentation from past explosive tests is not as complete as it might have been had the U.S. anticipated that a future test moratorium was possible. As a result, there are concerns about whether the computer codes that scientists and engineers use today based on previous test data are fully valid.

Dr. Kathleen Bailey, a senior fellow at the National Institute for Public Policy, argues that “Data from past nuclear testing is, in general, too coarse to test the validity of the high resolution, complex models that the SSP [Stockpile Stewardship Program] seeks to develop.”¹⁶ In addition, according to David Sharp, “the right answer could be obtained as a result of compensating errors, a circumstance in which two or more errors balance each other so they have no net effect.”¹⁷ This means that the final calculation might result as expected but that real errors and their potential risks are hidden.

At the time of the Comprehensive Test Ban Treaty in the 1990s, the directors of the U.S. National Nuclear Laboratories requested that the U.S. be allowed to conduct lower than one-kiloton experiments “to determine whether the first stage of multiple stage devices was indeed operating successfully.”¹⁸ The Clinton Administration, however, interpreted the treaty as banning all nuclear yield-producing experiments.¹⁹

Such errors could adversely affect judgments about the condition of the stockpile.²⁰ They are also problematic because other nations have taken a different approach and are testing nuclear weapons. Consequently, these countries are developing a body of data based on modern, real-world testing, potentially developing and trying new weapons designs.

While this proliferation of capabilities, generation of new knowledge, and emergence of new programs has been occurring, the U.S. has remained committed to its policy of banning all yield-producing experiments and refusing to allow nuclear weapons innovation in its National Nuclear Laboratories. It is also worth mentioning that Russia and China are developing new weapons as well as sustaining old ones. This means that their weapons complex is geared toward solving different problems than that

of the U.S. Both Russia and China could potentially develop new and better capabilities.

The Nuclear Threat. Nuclear weapons possess awesome power and have a unique ability to harm U.S. vital interests, especially when coupled with ballistic missiles, which remain the weapon of choice for America's adversaries.

- Ballistic missiles enable an adversary to deliver an attack within minutes (about a half-hour, or less depending on launch and target location, in the case of intercontinental-range ballistic missiles).
- The U.S. and its allies still lack a comprehensive layered ballistic missile defense system that would protect America from missile attack and devalue ballistic missiles as weapons for potential adversaries.
- The knowledge about mechanics of nuclear weapons and the physics behind them is becoming more easily accessible. For example, rudimentary nuclear weapon designs are available on the Internet. The covert network run by Pakistani scientist A.Q. Khan demonstrated that it is possible to buy advanced nuclear technologies—and perhaps material—on the black market, and North Korea has provided covert nuclear weapons assistance to Iran.
- Finally, ballistic missiles provide a more assured means of getting a weapon to its intended target than delivery by aircraft or other means.

Nuclear weapons come in various yields and design types. The weapon's configuration will determine its effects, which can generally be summarized in six categories: blast, direct nuclear radiation, thermal radiation, fires, electromagnetic pulse, and fallout.²¹ Depending on the yield and design type, the weapon's effects could dramatically affect the way the U.S. and its allies operate their forces. It is also worth noting that research and technology have progressed significantly since the U.S. stopped its yield-producing experiments.

New materials and technologies might perform in unexpected ways in a nuclear environment, as opposed to highly controlled testing and experimentation environments, thus introducing an additional layer of uncertainty when thinking through

operational plans and contingencies under which an enemy might use a nuclear weapon or how the U.S. would operate its forces in a post-nuclear weapon attack environment. Extreme conditions and America's limited understanding of the physical processes going on during a nuclear weapons detonation and the consequences of such a detonation make it very difficult and costly to model the effects of nuclear weapons on the different materials that are now used to make them. Even then, assumptions built into nuclear effects modeling may result in misleading understanding and flawed estimates of what the real effects of the use of a nuclear weapon would be.

Current Nuclear Use. Although it may come as a surprise to some, the U.S. "uses" its nuclear weapons every day. As pointed out by General Larry Welch, former Commander of the U.S. Strategic Air Command and former Chief of Staff of the Air Force:

The primary role of U.S. nuclear weapons for well over half a century has been to prevent their use. To that end, we have used them every second of every day since the first deterrent systems were deployed. They have worked perfectly. The nuclear deterrent is the only weapons system I know of that has worked perfectly without fail, exactly as intended, for their entire life span.²²

U.S. nuclear weapons have played a key role in protecting all three vital U.S. interests discussed in the Introduction to this *Index*:

- Safeguarding the homeland from external attack; protecting Americans against threats to their lives and well-being; protecting America's territory, borders, and airspace.
- Preventing a major power threat to Europe, East Asia, or the Persian Gulf, where a regional war would be devastating to U.S. interests and could spin out of control into a global conflict.
- Maintaining the freedom of the commons: free and safe transit of sea-lanes and space upholding the principle of freedom of the seas and space to promote and protect commerce among nations.

Other nations rely on their nuclear weapons capabilities for geopolitical maneuvering as well. For example, North Korea "uses" its nuclear weap-

ons to coerce South Korea and limit South Korea's response to North Korea's aggressive behavior. Russian nuclear weapons are the only reason why other nations think about Russia—a corrupt kleptocracy with enormous economic, demographic, ecological, and public health problems—as a superpower.

Where appropriate, this analysis will focus on states that possess nuclear weapons capabilities and have indicated an intent to attack one or more U.S. vital interests or that the U.S. government views as potential adversaries: e.g., Russia, China, and North Korea. France, the U.K., India, and Pakistan will not be considered threats to the homeland in this analysis because they have not communicated any intent to attack the U.S. (With respect to India and Pakistan, there exists the real possibility that these two nations could start a nuclear war with each other, and the effects of such a war would negatively affect the interests of the U.S. and its allies in the region.)

In addition, many experts believe that Israel possesses a nuclear weapons capability (Israel is not a party to the Non-Proliferation Treaty), although Israel has never publicly acknowledged the existence of its nuclear weapons arsenal. Israel does not have the intent to attack the U.S., so it will not be considered a threat for the purposes of this analysis.

It is also necessary to mention that nuclear weapons, if used, would probably not operate in a conventional conflict vacuum. A nuclear weapons attack would likely be accompanied by conventional operations aimed at achieving the military and political objectives of whichever nation decided to use nuclear weapons. A nuclear weapon could also be used during a conventional conflict as a next step on an escalatory ladder and to signal resolve. A nuclear weapon could also be used as a final resort when the leadership of a warring nation had nothing left to lose. Few countries, however, possess the capability to attack and threaten the U.S. homeland with nuclear weapons, and even fewer have the intent to do so.

The Nuclear Operating Environment. Since the end of the Cold War, the world in which U.S. nuclear forces operate has changed significantly. While the main focus of deterrence, the Soviet Union, receded in importance, the U.S. has had to adjust its posture to be able to deter new actors armed with nuclear weapons as well as emerging nuclear weapons states. India conducted five nuclear explosion tests in May 1998; Pakistan followed suit later that month with six nuclear tests of its own. North Korea

conducted three nuclear device tests, in 2006, 2009, and 2013. Iran does not have a nuclear weapon yet, but the International Atomic Energy Agency has found evidence of weaponization activities, uranium enrichment activities, and even uranium diversion. Iran has not been able to explain these activities in a manner that would allay the agency's suspicion.

Successive Nuclear Posture Reviews (in 1994, 2001/2002, and 2010) have struggled to address these challenges and adjust U.S. strategic posture to the post-Cold War world. With the end of the Cold War, the U.S. nuclear arsenal was dramatically downsized from over 30,000 warheads (its peak in 1967) to its current inventory of less than 5,000 warheads consisting of about 500 tactical nuclear weapons (TNWs); about 1,585 deployed warheads, according to data from the latest New Strategic Arms Reduction Treaty (New START) data exchange; and the remainder in reserve.²³

Since the end of the Cold War, the U.S. has made substantial adjustments in its nuclear posture, while working to preserve deterrence of attack. During the Cold War and Moscow's rapid disintegration, the U.S. focused primarily on the Soviet Union. One of the significant consequences of the dissolution of the Soviet Union was that the nuclear target set got smaller, which allowed for unprecedented reductions in U.S. strategic weapons and U.S. forward-deployed nuclear weapons. Many argued that with the Soviet threat receding, the nation lacked justification for maintaining not only a varied inventory, but also the infrastructure needed to design, develop, test, and maintain nuclear weapons. The U.S. conducted its last nuclear weapons test in 1992.

In the post-Cold War years, working in conjunction with the Soviet Union/Russian Federation, the U.S. has participated in four major programs designed to alter the size and composition of both nations' nuclear weapons arsenals. Counting rules under each of the treaties are different, so the real number of warheads and systems reduced will also be different for each of the treaties.

- On July 31, 1991, the United States and the USSR agreed to the Strategic Arms Reduction Treaty I (START).²⁴ The agreement entered into force in 1994. The accord dictated that each state reduce and limit its strategic armaments to no more than 6,000 "accountable" warheads and 1,600 delivery vehicles. START I relied on extensive verification

measures that included data exchanges and on-site inspections that were either prearranged or conducted on short-notice.²⁵

- The Strategic Offensive Reductions Treaty (Moscow Treaty, or SORT) entered into force in 2003. Rather than attaching warhead quantities strictly to delivery vehicles, SORT concentrated not on “accountable” warheads, but on actual operationally deployed warheads. Each state was allowed a range of 1,700 to 2,200 deployed warheads and the ability to determine the structure of its offensive strategic arms.²⁶ SORT relied on START I verification measures, which expired in 2009. By 2009, the United States had fulfilled its treaty obligations by lowering the number of deployed warheads to below the maximum allowed under SORT.²⁷
- The New Strategic Arms Reduction Treaty (New START) agreement entered into force in 2011. New START limits deployed warheads to 1,550 for each party and the number of deployed strategic nuclear delivery vehicles to 700 for each party.²⁸ Under New START, each bomber counts as only one deployed warhead out of the 1,550 despite the fact that many bombers can carry many more than one warhead (up to 16 for the B-2 and up to 20 for the B-52).²⁹ New START’s verification regime is not as stringent as that defined by START I.³⁰ This change is due in part to the dramatic decrease of inspections allowed to each nation.³¹ After the treaty is implemented, nuclear forces levels established in New START will be 74 percent lower than the limit of the START I Treaty and 10 percent–30 percent lower than the deployed strategic warhead limit under SORT.³²

In addition to these treaties, in 1991, President George H.W. Bush and eventual Soviet President Mikhail Gorbachev (and subsequently Russian President Boris Yeltsin) declared that both countries would reduce their arsenals of tactical nuclear weapons and delivery vehicles reciprocally and unilaterally. These statements are known collectively as the Presidential Nuclear Initiatives (PNIs).³³ Unlike arms control treaties, the PNIs are politically but not legally binding.

As a result, the U.S. eliminated all of its ground-launched short-range theater nuclear weapons, reduced its nuclear artillery shells and short-range

ballistic missile warheads, and withdrew all TNWs from surface ships and attack submarines, as well as TNWs associated with U.S. land-based naval aircraft.³⁴ President Bush’s initiatives led to an 85 percent reduction in U.S. operationally deployed TNWs between 1991 and 1993.³⁵ Russia, however, is said to be in violation of its political commitments under the PNIs.³⁶

President Barack Obama’s 2010 Nuclear Posture Review (NPR), the first U.S. NPR made available to the public, set five objectives of U.S. nuclear weapons policy and posture:

1. Preventing nuclear proliferation and nuclear terrorism;
2. Reducing the role of U.S. nuclear weapons in U.S. national security strategy;
3. Maintaining strategic deterrence and stability at reduced nuclear force levels;
4. Strengthening regional deterrence and reassuring U.S. allies and partners; and
5. Sustaining a safe, secure, and effective nuclear arsenal.³⁷

The underlying goal of the President’s current nuclear weapons policy is to achieve “the peace and security of a world without nuclear weapons.”³⁸ The President operates under the assumption that if the U.S. and Russia reduce their respective nuclear weapons arsenals bilaterally, this will put pressure on others to follow suit and reduce and/or dismantle their own nuclear weapons capabilities.

This assumption seems to go against the historical evidence. The U.S. has reduced its nuclear arsenal dramatically since the end of the Cold War. Washington maintains less than 5,000 nuclear warheads today, down from a peak of about 31,000 in 1967.³⁹ Yet North Korea, Pakistan, and India emerged as nuclear weapons players at the time of massive reductions in the U.S. nuclear arsenal (and also while the U.S. stopped yield-producing experiments on its nuclear arsenal).

Iran seems to be conducting activities that are consistent with the intent to weaponize its nuclear program, although it does not have a nuclear weapon yet.⁴⁰ The massive resources and manpower that

Iran spends on developing ballistic missiles that can reach U.S. allies and could reach the U.S. in the next few years also point to its intent to develop a payload that would be potent enough to coerce the U.S. and other regional powers and alter their calculus regarding possibly taking action against the interests of Tehran.

With the emergence of these new nuclear weapons actors after the end of the Cold War, the U.S. had to reexamine its Cold War notion of deterrence, which was based on the policy of mutually assured destruction. While U.S. policymakers were willing to accept mutual vulnerability in the deterrence equation vis-à-vis the Soviet Union and later Russia, they were not willing to accept retaliation-based deterrence vis-à-vis newly nuclear-armed nations. U.S. decision-makers recognized their limited insight into how the newly nuclear armed nations would operate their nuclear forces; how their command and control structures would operate; under what conditions their leaders would consider actually using a nuclear weapon, and what the U.S. might need to credibly deter these new actors.⁴¹

The U.S. operates in an asymmetrical deterrent environment because it values its population centers and economy, which are far easier to destroy than the hardened leadership bunkers, tools of internal oppression and external attack, and military infrastructure that some of its potential adversaries value.⁴² With the Soviet Union, the U.S. also developed a common understanding of nuclear weapons terminology and concepts through an elaborate arms control process and decades of verification experience, something that is absent from the relationship with the new nuclear powers.

Interactions between the U.S. and these powers on nuclear issues have been limited to trying to convince these actors to give up their weapons and the technologies that pose a proliferation risk. It is not at all clear that these nations have a good understanding of U.S. nuclear weapons policy and potential “red lines.” In the case of North Korea, for example, the U.S. has very limited insight into the inner workings of the hermit kingdom and even less information regarding North Korea’s decision calculus on the use of nuclear weapons. The U.S. will have to understand these new nuclear-armed states and think about how to apply its military capabilities to threaten what they value if the U.S. is to deter them from attacking U.S. interests.

U.S. Nuclear Weapons Outside U.S. Territory. Understanding the perspectives of newly armed nuclear weapons states takes on additional importance because the U.S. has extended nuclear deterrence commitments to over 30 nations around the world with whom the U.S. has alliance commitments.

To that end, the U.S. maintains about 200 B61 gravity bombs in Europe. Deployed to Belgium, Germany, Italy, the Netherlands, and Turkey, these bombs can be employed by U.S. or NATO nuclear-certified aircraft (U.S. F-16 and F-15E aircraft and various European dual-capable aircraft such as the German Tornado). The B61 is the only remaining operationally deployed tactical nuclear weapon in the U.S. arsenal.⁴³

Over the course of decades, the U.S. developed elaborate command and control arrangements through NATO. NATO’s senior body on nuclear matters is the Nuclear Planning Group, where all NATO members (with the exception of France) participate in discussing various policy issues related to nuclear weapons.

NATO’s 2010 Strategic Concept, a document outlining the purpose and nature of NATO’s security tasks, states that:

Deterrence, based on an appropriate mix of nuclear and conventional capabilities, remains a core element of our overall strategy. The circumstances in which any use of nuclear weapons might have to be contemplated are extremely remote. As long as nuclear weapons exist, NATO will remain a nuclear alliance.⁴⁴

The Strategic Concept also explains the relationship between U.S. strategic nuclear forces and the nuclear weapons arsenals of France and the United Kingdom:

The supreme guarantee of the security of the Allies is provided by the strategic nuclear forces of the Alliance, particularly those of the United States; the independent strategic nuclear forces of the United Kingdom and France, which have a deterrent role of their own, contribute to the overall deterrence and security of the Allies.⁴⁵

In 2012, the alliance conducted a comprehensive Deterrence and Defense Posture Review (DDPR), which reaffirmed that “Nuclear weapons are a core component of NATO’s overall capabilities for deter-

rence and defence alongside conventional and missile defence forces.” The DDPF also recognized the contribution of missile defense to NATO’s security and reaffirmed the importance that the alliance assigns to the U.S. nuclear presence in Europe.⁴⁶

With regard to missile defense, the U.S. is pursuing a “phased adaptive approach.” This plan for the protection of the European allies is based on an assessment of the threat from Iran’s short-range and medium-range ballistic missiles. The plan was announced in 2010 and was characterized by the White House Press Office as follows:

- Phase One (in the 2011 timeframe)—Deploy current and proven missile defense systems available in the next two years, including the sea-based Aegis Weapon System, the SM-3 interceptor (Block IA), and sensors such as the forward-based Army Navy/Transportable Radar Surveillance system (AN/TPY-2), to address regional ballistic missile threats to Europe and our deployed personnel and their families;
- Phase Two (in the 2015 timeframe)—After appropriate testing, deploy a more capable version of the SM-3 interceptor (Block IB) in both sea- and land-based configurations, and more advanced sensors, to expand the defended area against short- and medium-range missile threats;
- Phase Three (in the 2018 timeframe)—After development and testing are complete, deploy the more advanced SM-3 Block IIA variant currently under development, to counter short-, medium-, and intermediate-range missile threats; and
- Phase Four (in the 2020 timeframe)—After development and testing are complete, deploy the SM-3 Block IIB to help better cope with medium- and intermediate-range missiles and the potential future ICBM threat to the United States.⁴⁷

The U.S. cancelled Phase Four in 2013 and decided to deploy 14 additional Ground-Based Midcourse Defense Interceptors to address the North Korean and Iranian long-range ballistic missile threat to the U.S. homeland.⁴⁸ Construction of the missile defense sites in Romania is proceeding on schedule.

The deep level of cooperation and integration that exists between the U.S. and European allied forces

on nuclear weapons does not exist in Asia. Japan and South Korea have never been integrated into nuclear planning and operations for cooperative defense in the same way that European NATO allies have been. Some of these countries hosted U.S. nuclear weapons or supported U.S. nuclear weapons deployments in their regions in the past—Japan, for example, supported deployment of the Tomahawk Land Attack Missile/Nuclear (TLAM/N) systems—but the U.S. retired all of its TLAM/N systems in 2013 and currently does not deploy nuclear weapons outside of NATO and the U.S. territories.⁴⁹ The potential to forward deploy dual-capable aircraft with the B61 TNW remains a key option for reassuring Asian allies of America’s commitment to their defense.

U.S. Nuclear Forces and Infrastructure. Following release of the 2010 Nuclear Posture Review, President Obama directed that the U.S. employment strategy guiding U.S. nuclear weapons policy be revised. The Nuclear Posture Review Implementation Study (NPRIS), announced in June 2013,⁵⁰ called for additional nuclear weapons reductions.⁵¹ The Administration concluded that “we can ensure the security of the United States and our allies and partners and maintain a strong and credible strategic deterrent while safely pursuing up to a one-third reduction in deployed strategic nuclear weapons from the level established in the New START.”⁵²

Recently, consensus within Congress regarding funding for National Nuclear Security Administration (NNSA) weapons activities has begun to unravel. The Administration achieved consensus before Senate approval of New START,⁵³ pledging to invest over \$85 billion between fiscal year 2011 and FY 2020. This funding was intended to support costs for maintenance of the nuclear weapons stockpile and associated infrastructure, including the Chemistry and Metallurgy Research Replacement (CMRR) plutonium facility and the Uranium Processing Facility. The NNSA, a semi-autonomous agency within the U.S. Department of Energy, is responsible for nuclear weapons infrastructure recapitalization and nuclear weapons sustainment, and the military services exercise responsibility for the delivery systems.

Due in part to the Budget Control Act (BCA) and the resulting budget sequester, and in part to serious cost escalation in Life Extension Programs and infrastructure recapitalization programs, the Administration’s budget requests since 2010 have not reflected the commitment to fully fund key nuclear programs

on the schedule that it specified to the Senate in November 2010. Congress has decided to support the Administration's request to defer certain programs and slip the schedule for others. The Administration effectively cancelled the CMRR facility in its FY 2013 budget request. Impacts of the BCA and the cost escalation of critical programs will continue to delay and complicate nuclear weapons infrastructure modernization and stockpile sustainment activities.

The U.S. currently operates under a policy constraint that does not allow the National Nuclear Laboratories to develop new nuclear warheads or conduct yield-producing experiments on the current inventory of nuclear warheads. This policy also prohibits supporting development of new military missions for nuclear warheads or providing for new military capabilities.⁵⁴ Rose Gottemoeller, the State Department's Acting Under Secretary for Arms Control and International Security, summarized this policy as follows: "We're not modernizing. We're not modernizing. That is one of the basic, basic, I would say, principles and rules that have really been part of our nuclear posture view and part of the policy."⁵⁵

These policies constrain U.S. activities that could lead to the development of new, safer warheads, because new safety features would require yield-producing experiments to make sure that the new designs perform as expected. These policies will also make it more difficult to preserve the agility within the United States' knowledge and technology base that is necessary to adjust rapidly to surprise developments in other nations' nuclear weapons programs.

The Ongoing Challenge. The U.S. currently deploys nuclear weapons to Europe and is the only nuclear weapons state that deploys nuclear forces outside of its own territory. It is important that the U.S. be able uphold the principle of deploying weapons outside of its territory, because a deployment of nuclear weapons on allied territory is both an important contributor to assuring allies and clearly preferable to having allies develop their own nuclear weapons capabilities.

At the same time, the U.S. will continue to face challenges presented by its aging stockpile, a lack of funding for nuclear weapons modernization and infrastructure recapitalization, and policy constraints on yield-producing experiments. Complex and interdependent missile defense programs are likely to face their own developmental challenges.

National Security Space Systems and Satellites

The ability of the U.S. military to project combat power against an enemy force anywhere in the world depends on an array of command and control, logistics, and other support systems that are made possible by the country's national security space systems and other satellites. In fact, many critical functions can be performed (or performed acceptably) only by satellites, just one example being the American-produced and American-maintained Global Positioning System (GPS) upon which the world's interconnected transportation system relies.

The GPS constellation provides unmatched positioning, navigation, and timing (PNT) capabilities that are used not only by civil aviation, commercial shipping, and directionally challenged drivers everywhere, but also by the military for which it was originally designed. Satellites also enable global communications, which allows for effective command and control of conventional and strategic forces, and play an important role in intelligence gathering: the information on which U.S. forces rely to formulate plans and execute the best battlefield decisions. Military satellite systems also provide early warning and tracking of ballistic missiles, giving the U.S. time to take appropriate defensive measures.

Knowing the status of these systems is important if one is to understand the extent to which they are able to contribute to the viability of U.S. military power. These systems can be assessed across three important characteristics:

- The lifespan of these systems, which is a measure of their health and readiness;
- The number of satellites in orbit, which is a measure of satellite coverage and resiliency; and
- Their ability to provide support-on-demand, which is usually measured in available bandwidth capacity.

These characteristics are interconnected, but the specific purpose for which satellites are deployed determines their numbers, capabilities, and system configuration. For example, fewer highly capable satellites might be better for certain tasks than greater numbers of less capable systems, as is the case with very high orbit or geostationary systems;

in other cases, the number of satellites in orbit might be more important than the number of more capable or longer-lived ones.

Lifespan. The lifespan of satellites is determined largely by the amount of fuel onboard the satellite. In decades past, battery function and component survival against space radiation were key lifespan factors. Satellite technology has now advanced to make these problems less critical than the amount of thruster fuel maintained aboard the satellite.⁵⁶ The gravitational pull of the Earth, Moon, and Sun, together with solar wind and other features of space, can affect a satellite's speed and position, thus changing its position over time.⁵⁷ As a result, satellites must make small adjustments with thrusters to stay in their assigned orbit, a process called "station keeping."⁵⁸

Currently, most GPS satellites orbiting the Earth have a designed lifespan of 7.5 years, though they have often surpassed that figure, and advances in satellite materials are increasing platform life.⁵⁹ The newest GPS model in operation was designed with a 12-year lifespan, and the next generation of satellites is supposed to remain in orbit for 15 years.⁶⁰ The early warning and missile defense satellite known as SBIRS GEO (Space-Based Infrared System-Geosynchronous orbit) has a lifespan of 12 years, and both of the U.S.'s new communications satellite systems (WGS and AEHF) have a designed lifespan of 14 years.⁶¹

The older Milstar communication satellites that provide secure communications were designed for 10 years of service, a target exceeded by the first two systems, which approached or reached 20 years of service.⁶² Similarly, the legacy DSCS III communication satellites have surpassed their 10-year service lives, with the satellites functioning on average at least 50 percent longer than their designed life.⁶³ The Defense Support Program (DSP) satellites being replaced by SBIRS also have had significantly more longevity than planned, with lifespans exceeding design by as much as 250 percent.⁶⁴

Satellite lifespan most closely equates to the readiness of a warship or an aircraft. As the average amount of time remaining on U.S. satellites decreases, the U.S. either has to spend the money necessary to replace these satellites or lose the critical support functions they provide. As noted, the actual lifespan of satellites is often more than expected, but this does not guarantee that all satellites will see extend-

ed use, and the U.S. should not expect to rely on satellites well beyond their intended service lives.

Number of Satellites. GPS satellites are so important that the U.S. maintains excess capacity in the GPS constellation to ensure redundancy, thus reducing risk should any node fail. The constellation requires 24 satellites, but the U.S. routinely operates 27 and maintains four backup satellites flying as well.⁶⁵

The SBIRS satellite system, though significantly behind schedule, currently operates two GEO satellites, with two more nearing completion and two more to be produced. Additionally, two HEO (highly elliptical orbit) systems are in orbit, with a third delivered in mid-2013 but not yet launched and a fourth in production.⁶⁶ While the U.S. waits for the full constellation of SBIRS satellites, no more than five legacy DSP satellites continue to supplement SBIRS satellites in supplying early warning of ballistic missiles.⁶⁷

The WGS satellite constellation of six satellites is working and is supplemented by several of the eight remaining legacy DSCS III satellites, which have exceeded their designed lifespan.⁶⁸ Additionally, it is expected that three extra satellites will be added to the constellation by FY 2018.⁶⁹ The AEHF constellation is currently composed of three satellites, with a fourth in production and two more under contract.⁷⁰ AEHF also uses the five Milstar satellites that were in operation as of February 2014.⁷¹

There is also a variety of other satellite systems, including various high-end reconnaissance satellites and the Mobile User Objective System that, with two of a planned five satellites deployed, provides better connectivity to warfighters in the field and on the move.⁷²

Bandwidth and Processing Capacity. The strength of U.S. satellite constellations is further evidenced by the capacity of satellites to transmit data, as well as by their unique design capability, which allows them to carry out a variety of important tasks. GPS satellites have been updated consistently, adding additional and more powerful signals, anti-jamming capabilities, and accuracy.⁷³ SBIRS similarly advances beyond DSP capabilities by providing more reliable, detailed, and timely information to military forces.⁷⁴

The WGS provides a dramatic increase in capability over the DSCS system, with one WGS satellite providing greater communications capacity than

the entire DSCS III constellation or more than 10 times the capacity of one DSCS III satellite.⁷⁵ Similarly, the AEHF can handle 10 times more data than Milstar and provides each user with more than five times the bandwidth.⁷⁶ AEHF is better able to communicate with other satellites to speed the flow of information and has more antennas able to support specific operations.

Providing direct satellite communications support to battlefield users, however, remains difficult, especially with regard to mobile frontline forces. In 2010, before the launch of two MUOS satellites, Rebecca Cowen-Hirsch, then president of Inmarsat Government Services, Inc., stated that “[T]actical communications in narrowband is one of the areas that is so significantly broken right now.... [F]or every one request for UHF [Ultra-high frequency] capacity [that’s accepted], five are denied.”⁷⁷ With MUOS satellites providing “a 16-fold increases in transmission throughput over the current UAF satellite system,” this support gap is being addressed.⁷⁸

Threat to Lifespan, Number, and Capability. U.S. capabilities in space are unmatched, but with competitors improving their satellite and anti-satellite technologies, continued U.S. dominance is by no means guaranteed. For example, the Chinese BeiDou-2 global navigation system of satellites is operating in East Asia with at least 14 operational satellites in orbit, and Beijing plans to expand this constellation to as many as 35 by 2020.⁷⁹ Additionally, China has at least two communication satellite constellations, a weather satellite constellation, and a number of reconnaissance and intelligence satellites.⁸⁰ The Chinese have also engaged in numerous tests of anti-satellite capabilities without customary warnings to the international community.⁸¹

Moreover, China is not the only one of America’s geopolitical rivals pushing forward with new satellite and space system technology. Russia, for example, has its GLONASS system composed of 24 operational satellites, giving it global coverage.⁸² Russia also maintains a series of communications and reconnaissance satellites.⁸³ The secrecy surrounding space programs makes any full assessment of space capabilities difficult, but enough evidence exists to show that what was once a nearly exclusive advantage for the U.S. is increasingly less so.

As U.S. systems and operations increasingly use and rely on satellite support, satellites and the capabilities they provide will become more critical.

Consequently, one would expect to see a prioritization of funding for satellites, but that has not been the case. Instead, spending on military space systems declined from around \$15 billion in FY 2000 to approximately \$8.5 billion in FY 2010.⁸⁴ In 2012, President Obama requested an additional 22 percent cut in military space spending for his FY 2013 budget. Although Congress rejected this request, the overall pressure on defense spending is likely to stress funding for national security space systems at the same time that the U.S. is increasingly reliant on them.

In fact, it is estimated that some 80 percent or more of the satellite bandwidth currently used by the U.S. military is supplied by the private sector and full motion video.⁸⁵ Data, especially imagery, from various reconnaissance systems including UAVs, ground systems, and other sources that use satellites as relays take up an enormous amount of bandwidth. As a result, the Department of Defense has had no choice but to move this information over commercial satellites.

While considered less secure than military-grade satellites, commercial satellites have the advantage of being more numerous and more frequently updated as private-sector companies compete with one another.⁸⁶ Other nations, like the United Kingdom, have closer cooperation and partnerships between their military and commercial providers, but the U.S. has not yet established this sort of clear relationship, and this limits the effectiveness of the means by which draws on commercial satellites.⁸⁷

With regard to satellite systems, the needs of the U.S. military are currently being met. U.S. military forces are able to do what they need to do with such systems.⁸⁸ However, as data transmission demands continue to increase, the military’s needs will soon exceed America’s existing satellite capacity. Constrained budgets are causing senior leaders to consider ways to manage constellation degradation, to include greater reliance on commercial systems. While this option works well in peacetime, it accepts significant risk in war, especially given the effort by competitors such as China to develop anti-satellite capabilities and the growing challenges to ground station control capability posed by cyber attacks.

In 2011, then-Secretary of the Air Force Michael Donley and then-Vice Chairman of the Joint Chiefs of Staff General James Cartwright suggested looking to partner nations in Europe and perhaps even

geostrategic competitors (like China) to supplement U.S. capabilities.⁸⁹ Doing so would certainly account for shortfalls in U.S. proprietary capacity, but it also would accept significant risk in defense planning—a situation that is in no way conducive to protecting the United States’ vital national interests.

Cyberspace: A New Domain with Unique Challenges and Opportunities

Cyberspace could be said to have begun on October 29, 1969, when engineers 400 miles apart at the University of California in Los Angeles and the Stanford Research Institute (SRI) sent data over the “Arpanet,” a network whose name derived from the agency funding the undertaking, the Defense Department’s Advanced Research Projects Agency (ARPA).⁹⁰ The network began when one scientist attempted to log in remotely to a computer at SRI. He first typed the letter “L,” then “O,” then “G.” Then the system crashed. Three hours later, it was up and running again, and the world has been “logging on” ever since.

In the 1970s, more computers, mostly at research institutions and military organizations, were added to “ARPANET,” and basic applications like e-mail were created. Upgrades to ARPANET’s protocols that enhanced “Internetting,” or the improvement of communication between networks, were developed throughout the decade. As the Internet grew, so did the potential for malware, and the first known virus, dubbed “Brain,” was discovered in 1986.⁹¹

Important transitions of protocols occurred in the early 1980s, enabling a split between research organizations and military operational organizations. Other government agencies and communities saw the power of the early Internet and latched onto it as well. By the end of the 1980s, private companies were able to participate in the development and use of the Internet.⁹² In 1998, the U.S. government relinquished control of the Internet’s naming function to the Internet Corporation for Assigned Names and Numbers (ICANN) under contract to the Department of Commerce, leading to the recent dramatic expansion of Internet-based technologies.

With these advances, however, has come the potential for exploitation. An increase in the capability to break into computer systems for espionage, crime, political statements, cyber destruction, and even physical destruction has paralleled the expansion of cyberspace. Malware, malicious hardware, and other types of cyber attacks are

inherent in cyberspace and have created the need for cybersecurity.

Due to the devastating impact that they could have on critical infrastructure and military systems, cyber weapons—as well as the cyber capabilities of geopolitical rivals—pose a serious threat to U.S. interests.⁹³ Cyber attacks could be used in tandem with efforts to attack or coerce the U.S. or its allies such as Israel, Taiwan, Japan, Poland, or Estonia. Cyber weapons also could be employed at a sufficiently serious level by such belligerent actors as Iran, North Korea, or terrorists who are interested in a show of strength or simply destruction and terror.

While cyber-espionage, cyber-crime, and other cyber threats to U.S. interests and the freedom of the Internet are serious offenses, such actions are, by definition, not a use of hard power: defined as military might or the ability to project physical force.⁹⁴ The *Tallinn Manual*, an effort by 20 respected legal experts to apply various laws of war to cyber conflict, provides perhaps the clearest definition of when to treat a cyber attack as an “armed attack,” or the clear use of hard power that justifies military self-defense.

The manual sees hard-power use of cyber capabilities (i.e., armed attack) as those cyber operations whose “effects ... were analogous to those that would result from an action otherwise qualifying as a kinetic armed attack.”⁹⁵ Therefore, this *Index* will focus on cyber operations that are of sufficient scale and effect that they could be considered hard power and used as part of an “armed attack.” The experts of the manual were divided on whether an operation whose scope and magnitude causes “extensive negative effects,” including economic or physical disruptions, but without large-scale fatalities should be considered an armed attack.⁹⁶ Given that such an attack could be considered an armed attack by different actors, it will also be examined in this *Index*.

Cyberspace as an Operating Environment.

Cyberspace is a unique operating environment that challenges the U.S. in multiple ways. These challenges include the cyber domain’s reach, speed, anonymity, and offense-dominated nature. Being a relatively new field of warfare, the cyber environment is one within which the U.S. is learning to operate. Understanding the unique nature and challenges of this realm, as well as the U.S.’s policies and the capabilities of its allies, is important to an assessment of the U.S. military’s ability to conduct military operations in the 21st century.

Cyberspace can be defined as “the manmade domain and information environment we create when we connect together all computers, wires, switches, routers, wireless devices, satellites, and other components that allow us to move large amounts of data at very fast speeds.”⁹⁷ Looking even closer, cyberspace is composed of four layers:

- **Physical systems.** These include computers, machines connected to or controlled by a remote source, wires and cables, routers, and other pieces of physical hardware that allow for the interconnectivity between and operation of devices.
- **Logical systems.** Beyond hardware lie the important logic and software that make up the current Internet and cyber domain. The current system is defined by certain protocols and rules that allow different programs to be compatible and communicate with each other. From this logic come various forms of software and applications, all of which build on each other and work together to complete certain tasks.
- **Information.** To some extent, each system in cyberspace stores, sends, and receives information. Before the interconnectivity of computers, this information was still stored digitally but was not easily accessible to other individuals or devices. Cyberspace is defined by the unlocking of this information from its physical location and allowing it to transit the world for analysis, use, and even theft or exploitation at a rapid pace.
- **People.** Ultimately, cyberspace serves the needs of individuals and groups by providing the ability to communicate or analyze information, start or stop a process, or engage in countless other activities across the world and in conjunction with others. The customs, needs, organization, and training of different peoples affects the way in which cyberspace is used.⁹⁸

Together, these four layers, interconnected around the world, form the foundations of cyberspace as it is known today. Flowing from this construct, cyberspace contains three unique features that not only support U.S. civilian and military activities, but can also be used against the U.S. Specifically, cyberspace is:

- Ubiquitous,
- Anonymous, and
- Offense-dominated.

Ubiquitous. Cyberspace is defined largely by its vast reach and the ability of an individual to communicate with any computer in the world and vice versa.⁹⁹ According to various estimates, at the end of 2008, there were at least 1 billion personal computers in use around the world—a number that it is estimated will double to 2 billion by 2015. Additionally, there were an estimated 1.4 billion smartphones in use at the end of 2013 and countless other cyberspace-connected devices, both in the civilian world and in the military, known as the “Internet of things.”¹⁰⁰

Each of these devices has the ability to access information and send commands across the Internet, interacting with any number of other devices. In most cases, this capability is peaceful and productive. However, it also allows hackers or those who seek to exploit unauthorized access to a computer system or network, whatever their allegiance and wherever they are, to abuse cyberspace and use it for their own ends.

As the world’s most technologically advanced military, the U.S. military uses cyberspace in numerous ways. In some areas, cyberspace has not only enhanced, but profoundly changed the way in which the U.S. military operates. Several of the most critical areas include:

- Command and control systems;
- Communications;
- Guidance and navigation systems;
- Intelligence and information-gathering, information-analyzing, and information-sharing systems;
- Vehicle, aircraft, and ship operations;
- Offensive cyber operations;
- Logistics, or the sustainment of military operations; and
- Research.

Most of these areas affect critical warfighting capabilities spread across all four branches of the U.S. military.

Additionally, the U.S. homeland depends on 16 sectors of interdependent critical infrastructure, most of which are reliant on cyberspace. The Department of Homeland Security, together with other government agencies, is responsible for protecting these sectors. The 16 critical infrastructure sectors are:

- Chemical;
- Commercial facilities;
- Communications;
- Critical manufacturing;
- Dams;
- Defense industrial base;
- Emergency services;
- Energy;
- Financial services;
- Food and agriculture;
- Government facilities;
- Health care and public health;
- Information technology;
- Nuclear reactors, materials, and waste;
- Transportation systems; and
- Water and wastewater systems.¹⁰¹

Most of these sectors depend either directly or indirectly on cyberspace. For example, a power plant and other parts of the electric grid are managed and controlled by Internet-based communication and control systems, such as Industrial Control Systems (ICS) and Smart Grid technologies.¹⁰² Should these systems be disabled, a cascade of failures could

begin. For example, a grocery store depends on electricity to use cash registers, run refrigerators, and order more food. The supply chain depends on communications and logistics systems that rely on electricity and Internet-based communications. Even farm irrigation systems may require electricity.

Such interdependence within critical infrastructure and widespread reliance on cyberspace creates serious vulnerabilities that can be exploited. Compounding these vulnerabilities, much of the critical infrastructure in the U.S. is owned and operated by the private sector, meaning that the government does not control their operations—even if it is charged with their protection.

Anonymous. Perhaps the most often remarked feature of cyberspace is its anonymity.¹⁰³ It is difficult to determine the origin of a cyber attack or probe. First, an attack or penetration must be noticed. Then, forensic analysis of the attack mechanism must be undertaken to pinpoint the source of the intrusion and trace it back to the attacker. Depending on the complexity or type of attack, this process could take a significant amount of time. Even if the geographic origin of the attack is confirmed, it may be difficult to determine who exactly is responsible.¹⁰⁴

This problem is exacerbated by the ability of hackers to redirect their attacks through other locations, making it difficult to pinpoint the true origin of the attack. For example, an attack by China could be routed through U.S. systems to appear as though the attack originated within the U.S.¹⁰⁵ While not impossible to solve, misdirections require time and resources that might not be available during a period of crisis.

For all of the difficulty ascribed to attributing cyber attacks to the correct actor, the “attribution problem” may in some circumstances be overstated.¹⁰⁶ The ability to break through the anonymity of cyber attacks is improving as defenders are using the vulnerabilities and mistakes of hackers to track them down faster and more effectively.¹⁰⁷ (For example, in December 2014, the U.S. government determined within a number of days that a cyber-attack on Sony Pictures Entertainment originated with the government of North Korea.) In some cases, a devastating cyber attack could be sourced by placing the attack in the context of other global affairs. For example, if the West Coast power grid and U.S. military systems in the Asia-Pacific theater were disrupted, and if China at the same time began aggres-

sive or coercive action against Taiwan or Japan, such events could inform the U.S. attribution process.

Similar examples can be seen with other actors that might be expected to pair their cyber attack with physical attacks or coercion—for example, as seen during Russia’s invasion of Georgia in 2008.¹⁰⁸ Additionally, while any one cyber attack may be difficult to attribute to an actor, a series or campaign of attacks gives more data points with which to identify an attacker. Nevertheless, the attribution challenge and anonymous nature of cyberspace do still complicate U.S. responses to cyber attacks.

Offense-Dominated. For multiple reasons, cyberspace is currently considered an offense-dominated domain. It is easier, cheaper, and generally more effective to engage in offense rather than in defense. Cyber action is both instantaneous and constantly changing, which makes defense difficult. The dissemination of interconnected systems means that millions of potential targets are vulnerable to exploitation. And because the attacker has to find just one hole to exploit, cyber aggression is an appealing and cheap form of asymmetric warfare. Each of these reasons deserves greater explanation.

First, a main feature of cyberspace that contributes to the superiority of offense is its speed and dynamic nature.¹⁰⁹ Though it can take months to find and exploit a vulnerability, the actual cyber attack occurs instantly. Furthermore, danger in the cyber-sphere is constant. Of the weapons in the arsenals of potential enemies, cyber weapons are the fastest and often provide little or no warning, making it difficult for defenses to be prepared and reinforcements brought to bear.¹¹⁰

Compounding these challenges, new types of cyber attacks and vulnerabilities are constantly being discovered and developed by hackers. As a result, cybersecurity defenders are constantly playing catch-up.¹¹¹ Of course, this assumes that defenders are even aware of a potential intrusion. Incomplete security systems or brand-new types of threats could evade the watchful eye of cybersecurity professionals until well after significant damage has been done.

Second, the wide variety of targets means that defenders have a lot to defend.¹¹² As noted, the military and critical infrastructure sectors of the U.S. and other nations are all largely dependent on cyberspace.¹¹³ Worse, cyber attacks have the capability to target important systems indirectly by instead

assaulting different systems on which the original systems rely. For example, attacking the command and control system of a B-2 might be easier than attacking the B-2 itself. Given the constantly evolving nature of cyberspace, it is practically impossible to secure every system perfectly—especially since the vast majority of critical infrastructure belongs to the private sector, with companies all at different places in their cybersecurity development.

Third, cyberspace is filled with potential adversaries who either have or could relatively easily acquire significant offensive cyber capabilities.¹¹⁴ This is driven by the low cost of entry for cyber warfare and the great potential for damage, making it similar to other inexpensive forms of asymmetric warfare.¹¹⁵ An opponent may not be able to field a global navy or large squadrons of advanced fighter jets, but it can still wreak significant levels of destruction with a much less expensive cyber force.¹¹⁶

Many militaries and nations around the world are therefore interested in developing cyber capabilities that can help them to level the playing field. This is certainly true of potential cyber adversaries such as North Korea, Iran, Russia, and China, not to mention terrorists. Thus, the U.S. should expect to see a continued buildup of cyber capabilities by actors around the world as an asymmetric challenge to U.S. capabilities.

Cyber Attacks and Their Effects. Given these features of the cyber environment, cyber attacks are a serious avenue through which attacks can be launched, affecting the confidentiality, integrity, and availability of information or systems. If information is not private, the commands flowing from a system are not trusted, or a system is unavailable, then capabilities are weakened.¹¹⁷







Part of having a comprehensive grasp of the cyber-operational environment is an understanding of what cyber attacks are and what effects they can have. It is worth repeating that for purposes of this report, only cyber attacks that have severe consequences will be considered, as such attacks would threaten a critical national interest much as the large-scale use of conventional weapons would threaten them. While many military systems operate on their own closed networks, they are still vulnerable to attack.¹¹⁸ Similarly, attacks against critical infrastructure could overwhelm various systems since many sensitive control systems are insecurely connected to the Internet.¹¹⁹

TABLE 1

World Cyber Threats

The most serious threats in cyberspace come from nation-state and associated actors. With more resources and greater ambitions and objectives than most criminal organizations, nation-state attacks and hacks are among the largest, most aggressive, and most noteworthy acts of cyber-aggression.

- E Economic
- M Military
- P Political

				
Country	North Korea	Russia	Iran	China
Capability	Limited Capability	Very Capable	Moderate Capability	Very Capable
Overview	Aggressive, unpredictable, scattered across the world	Non-government and criminal "patriotic hackers," technologically advanced	Social network savvy, regional economic destabilizer	Globally diverse campaign of economic and military espionage, strategic mindset
International Attacks 	P 48,000 South Korean bank, media, and government computers and servers attacked in 2013	M P 54 government, finance, and communication websites attacked during invasion of northern Georgia in 2008	E P Oil company Saudi Aramco attacked in 2012, destroying 30,000 computers	E Theft of hundreds of billions of dollars in IP from numerous nations across the world
	P Various attacks on South Korean and U.S. institutions coinciding with July 4 events and annual U.S.-South Korea military exercises	P Estonian banks and government websites attacked following the moving of a Soviet war memorial in 2007	E P Qatari natural gas company Rasgas's computer networks attacked in 2012	P Hong Kong's voter registration system attacked after protests of China's involvement in selecting a new state leader in 2014
Attacks on U.S. Systems 	P 2009 attacks on U.S. and South Korean government websites, including crashing the Federal Trade Commission site	E 2012 data theft by "Energetic Bear," targeting the international energy sector, manufacturers, and defense contractors	P Crashing of major U.S. bank websites following the 2012 sanctions on Iran	E 2009 theft of F-35 plans from U.S. Department of Defense
		E P Campaign of infiltration of U.S. energy and critical infrastructure networks by the "Black Energy" malware starting in 2011 and discovered in 2014	E P Since 2012, "Operation Cleaver" has been breaching U.S. military, airline, energy, and other companies' networks, as well as a variety of other worldwide targets	E U.S. Department of Justice charges Chinese military officials in 2014 with hacking and economic espionage against six U.S. energy, mining, and manufacturing companies from 2006 to 2014

Source: Heritage Foundation research and analysis provided elsewhere in this study.

Malware. Malware stands for “malicious software” and includes viruses, worms, Trojans, rootkits, and many other types of attacks.¹²⁰ Malware often has the ability to replicate and spread with little or no help from human users. While many forms of malware, such as spyware, act surreptitiously and try to avoid being seen, such malware are generally associated with cyber espionage or crime—activities that are not hard-power uses of cyber weapons—although they can be used to create backdoors or vulnerabilities in computer systems that can later be used for other purposes.

On the other hand, some malware can be highly destructive to the functioning of a system. Trojans can take over control of a computer, obviously a dangerous capability in the hands of an adversary. Viruses and worms are the most easily spread forms of malware as they can replicate on their own. Among their more malicious capabilities, viruses and worms can disable computers by deleting critical data and preventing correct operation.¹²¹

For some, disabled military platforms are merely an annoyance; for others, successful operation depends entirely on a working computer system or program. Even systems that are “air gapped,” or not connected to the Internet, are at risk via the supply chain when infected devices are connected to the closed system during updating or just by accident, or through other clever forms of transmission.¹²² Malware’s ability to spread, permanently disable, or even control a system makes it a dangerous cyber weapon in the hands of a dedicated opponent.

Denial of Service. Billions of computers are connected to the Internet with access to millions of other computers and websites.¹²³ When too many computers try to connect with a website or computer, the target will slow down or even fail as scarce resources are used up trying to process these requests.

Denial-of-service (DOS) attacks send a flood of partial or flawed communications to a target system or site, leaving the target unable to respond effectively. These requests build up and eventually cause the target to slow down or crash. DOS attacks can be strengthened when a hacker places malware on thousands of other computers, thereby allowing the hacker to control these computers or “bots.” These otherwise innocent computers will then do the hacker’s bidding, multiplying the faulty requests sent to a website or system in what is known as a distributed DOS or DDOS attack.¹²⁴

While DOS attacks can blind and disrupt, they are generally temporary in nature and do not leave any permanent cyber damage, though some advanced techniques, known as “phlashing” or “bricking,” can render hardware inoperable.¹²⁵ Prolonged DOS attacks have been used to great effect, notably in Russia’s campaign against Georgia in 2008, in which debilitating DOS attacks froze the websites of Georgian government and media organizations. These attacks, in addition to limiting Georgia’s ability to communicate with its citizens and the outside world, coincided with a Russian military incursion in different areas of Georgia.¹²⁶ DOS attacks will likely be part of any coordinated cyber attack against the U.S. or its allies, but they are generally the least harmful.

Malicious Hardware. Military and some critical infrastructure systems are at least somewhat protected from cyber attack because they reside on closed systems. Hardware threats avoid this potential defense, however, by being physically built into a computer system so that, regardless of how connected a device is to cyberspace, malicious instructions can be carried out. Given the interconnected nature of the technology industry’s supply chain, a single device can be made of thousands of parts, each built by a different contractor in a different country, making it difficult to be assured of a device’s security and integrity.

Hardware threats are generally less known and can be difficult to identify because they often go unnoticed until activated.¹²⁷ Finding malicious hardware can be extremely difficult, since computer systems are often created from a multitude of parts, all potentially originating from different countries and different companies, with multiple contractors and subcontractors. Furthermore, testing hardware to find potential flaws or malicious circuitry is extremely problematic because testing cannot be exhaustive enough to cover all potential inputs or commands that a computer or individual chip might be given.¹²⁸

If hardware contains malicious circuitry, it can be activated at certain times, in certain places, or on demand. Once activated, malicious hardware can fail outright or just operate in an impaired manner.¹²⁹ Hardware can also serve as a backdoor for the introduction of malware.¹³⁰ Malicious hardware can build up over time, waiting for a potential conflict, and serve as a strategic way for an adversary to compromise another nation’s cyber systems.

Insider Attacks and Social Engineering. It is worth mentioning that a potential attacker may use employees, contractors, or other people with inside access to an organization to provide the opportunity for an attack. This can occur directly, in the case of insider attacks where a mole creates a vulnerability through which attackers can unleash an attack, or indirectly, in the case of social engineering that tries to trick individuals into giving up sensitive information or unknowingly enable a larger attack to come through.

Targeted and Advanced Persistent Threats (APT). While not a type of attack itself, it should be noted that advanced bad actors could use a combination of sophisticated and specifically tailored attack mechanisms to attack a target or group of targets persistently. Such strategies are often the work of nation-states or large criminal-hacker enterprises with significant amounts of resources.¹³¹ Importantly, these attacks can often bypass security measures and exploit holes in cyber defenses known as “zero-day” vulnerabilities, or vulnerabilities that were not known until they were used by hackers to exploit a system.

Additionally, many APT attacks follow an attack sequence that includes initial reconnaissance, the initial attack that breaches a system, building additional backdoors into the compromised system, gaining privileges and command and control powers, finding information, and exfiltrating information, all while continuing to hide one’s presence and establishing additional backdoors and privileges. This process can continue for years as the victim is continually robbed or harmed.¹³²

Advanced attacks can even result in physical damage. One of the first examples of such an attack occurred in 1982 when the U.S. introduced faulty software into the pipeline control program of a Soviet

gas pipeline. The program caused excessively high pressures within the pipes, causing what *The Washington Post* called “the most monumental non-nuclear explosion and fire ever seen from space.”¹³³

More recently, Stuxnet, one of the most complex pieces of malware the world has ever seen, caused the centrifuges at the Iranian nuclear facilities to spin occasionally at speeds that would damage the sensitive machinery.¹³⁴ Stuxnet did so subtly, thereby concealing its actions from the Iranians for over a year. Physical damage from advanced cyber attacks is likely to become more common as more and more physical items are connected to the Internet of things.¹³⁵

The military, like any other community, is reliant on the cyber domain in everything it does, from simple administrative tasks to conducting war. Every feature of cyber is dynamic, from the scope and breadth of the domain itself to the tools used to conduct legitimate business and for malicious purposes, as well as for offense and defense in military affairs.

It took armies 50 years to digest the implications of industrialized warfare, from the time high-volume firepower and nearly instantaneous communications were introduced to the battlefield in the U.S. Civil War to their slaughtering effects on Europe’s battlefields in the First World War, and 25 years to understand the implications of airpower and the mechanization of forces as they evolved from their first appearances in World War I to their full manifestation in World War II.

The U.S., its friends, and its competitors are likewise trying to understand the nature and implications of the cyber domain. There is no question, however, that competence in this field, both to defend one’s own cybersystems and to challenge enemy cybersystems in wartime, is critical. America’s investments in this field should be made accordingly.

Endnotes:

1. Israel likely possesses nuclear weapons capabilities, although it has never officially admitted to possessing them. Pakistan openly demonstrated its nuclear capabilities in 1998, with a series of six tests in response to testing by India. North Korea conducted tests in 2006, 2009, and 2013, and is thought to possess a few weapons.
2. Amy F. Woolf, "Nonstrategic Nuclear Weapons," Congressional Research Service, January 3, 2014, <http://www.fas.org/sgp/crs/nuke/RL32572.pdf> (accessed September 16, 2014).
3. Fallout is radioactive debris that results from a nuclear explosion, is carried aloft into the air at considerable distance from the detonation, and then returns to Earth and contaminates areas potentially far removed from the original blast site. Electromagnetic pulse (EMP) is also an effect created by a nuclear blast in which a massive burst of electromagnetic energy is generated and propagated through the atmosphere and possesses the ability to damage electronic equipment.
4. Baker Spring, "Congressional Commission Should Recommend a 'Damage Limitation' Strategy," Heritage Foundation *Backgrounder* No. 2172, August 14, 2008, <http://www.heritage.org/research/reports/2008/08/congressional-commission-should-recommend-damage-limitation-strategy>.
5. Bernard Baruch, "The Baruch Plan," presented to the United Nations Atomic Energy Commission, June 14, 1946, <http://www.atomicarchive.com/Docs/Deterrence/BaruchPlan.shtml> (accessed May 22, 2014).
6. "Counterforce targets" refers to a set of targets that have a political and military value (e.g., bomber bases, army battalions, or leadership). Countervalue targets are economic and civilian centers (e.g., cities or food factories).
7. Herman Kahn, *On Thermonuclear War* (Princeton, NJ: Princeton University Press, 1961), p. 96.
8. Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960), p. 233.
9. For a detailed examination of the evolution of the theory and practice of deterrence from the 1960s to the present, see Keith B. Payne, *The Great American Gamble: Deterrence Theory and Practice from the Cold War to the Twenty-First Century* (Fairfax, VA: National Institute Press, 2008).
10. William Ogle, "An Account of the Return to Nuclear Weapons Testing by the United States after the Test Moratorium 1958-1961," United States Department of Energy, Nevada Operations Office, October 1985.
11. George H. Miller, Paul S. Brown, and Carol T. Alonso, *Report to Congress on Stockpile Reliability, Weapon Remanufacture, and the Role of Nuclear Testing*, Lawrence Livermore National Laboratory, October 1987, p. 3, <http://www.osti.gov/scitech/servlets/purl/6032983> (accessed November 20, 2014).
12. Thomas Scheber, "Reliable Replacement Warheads: Perspectives and Issues," United States Nuclear Strategy Forum, August 2007, pp. 4-5, <http://www.nipp.org/Publication/Downloads/Publication%20Archive%20PDF/RRW%20final%20with%20foreword%207.30.07.pdf> (accessed September 16, 2014).
13. Kathleen C. Bailey, "The Comprehensive Test Ban Treaty: The Costs Outweigh the Benefits," Cato Institute *Policy Analysis* No. 330, January 15, 1999, p. 9, <http://www.cato.org/pubs/pas/pa330.pdf> (accessed September 16, 2014).
14. Transcript, "National Defense Industrial Association, Air Force Association and Reserve Officers Association Capitol Hill Breakfast Forum with Don Cook, Deputy Administrator for Defense Programs, National Nuclear Security Administration, on Nuclear Weapons Sustainment," July 7, 2012, <http://secure.afa.org/HBS/transcripts/2012/7-10-2012%20Dr.%20Donald%20Cook.pdf> (accessed November 20, 2014).
15. David H. Sharp, "Nuclear Testing: Deterrence, Stewardship, and Arms Reduction," Los Alamos National Laboratory, Report No. LA-UR-08-06803, p. 10.
16. Kathleen C. Bailey, "The Comprehensive Test Ban Treaty: An Update on the Debate," National Institute for Public Policy, March 2001, p. 10, <http://www.nipp.org/National%20Institute%20Press/Archives/Publication%20Archive%20PDF/CTBT%20Update.pdf> (accessed September 16, 2014).
17. Sharp, "Nuclear Testing: Deterrence, Stewardship, and Arms Reduction," p. 11.
18. Ambassador C. Paul Robinson, John Foster, and Thomas Scheber, "The Comprehensive Test Ban Treaty: Questions and Challenges," Heritage Foundation *Lecture* No. 1218, November 7, 2012, <http://www.heritage.org/research/lecture/2012/11/the-comprehensive-test-ban-treaty-questions-and-challenges> (accessed June 25, 2014).
19. The Comprehensive Test Ban Treaty does not define what constitutes a nuclear weapons experiment.
20. Michaela Dodge and Baker Spring, "Keeping Nuclear Testing on the Table: A National Security Imperative," Heritage Foundation *Backgrounder* No. 2770, February 27, 2013, <http://www.heritage.org/research/reports/2013/02/keeping-nuclear-testing-on-the-table-a-national-security-imperative> (accessed September 16, 2014).
21. Office of Technology Assessment, *The Effects of Nuclear War*, May 1979, <http://ota.fas.org/reports/7906.pdf> (accessed September 16, 2014).
22. General Larry Welch, USAF, transcript of remarks, Air Force Association Huessy Congressional Breakfast Series, May 25, 2012, <http://secure.afa.org/HBS/transcripts/2012/5-25-2012%20Gen%20Larry%20Welch%20v2.pdf> (accessed September 16, 2014).

23. The Heritage Foundation "Nuclear Powers Emerge as U.S. Stockpiles Shrink," May 25, 2010, <http://www.heritage.org/multimedia/infographic/nuclear-powers-emerge-as-us-stockpile-shrinks>; U.S. Department of State, "Fact Sheet: New START Treaty Aggregate Numbers of Strategic Offensive Arms," April 1, 2014, <http://www.state.gov/t/avc/rls/224236.htm> (accessed October 7, 2014). It is important to recognize that arms control treaties since the end of the Cold War have used different counting rules. The U.S. currently maintains around 2,000 real nuclear warheads.
24. Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms (START Treaty), signed July 31, 1991, <http://www.state.gov/t/avc/trty/146007.htm> (accessed November 20, 2014).
25. These transparency measures remained in effect until START I's expiration in 2009.
26. Treaty Between the United States of America and the Russian Federation on Strategic Offensive Reductions (SORT / Treaty of Moscow), signed May 24, 2002, <http://cns.miis.edu/inventory/pdfs/aptsort.pdf> (accessed September 16, 2014).
27. Julian Borger, "Nuclear Weapons: How Many Are There in 2009 and Who Has Them?" *The Guardian Online*, September 25, 2009, <http://www.theguardian.com/news/datablog/2009/sep/06/nuclear-weapons-world-us-north-korea-russia-iran> (accessed June 6, 2014).
28. Treaty Between the United States of America and the Russian Federation on Measures for the Further Reduction and Limitation of Strategic Offensive Arms (New START Treaty), signed April 8, 2010, <http://www.state.gov/documents/organization/140035.pdf> (accessed September 16, 2014).
29. Keith B. Payne, "Evaluating the U.S.-Russia Nuclear Deal," *The Wall Street Journal Online*, updated April 8, 2010, <http://online.wsj.com/news/articles/SB20001424052702303720604575169532920779888> (accessed June 11, 2014).
30. Paula DeSutter, "Verification and the New START Treaty," Heritage Foundation *Lecture* No. 1160, July 12, 2010, <http://www.heritage.org/research/lecture/verification-and-the-new-start-treaty>.
31. New START Working Group, "New START: Potemkin Village Verification," Heritage Foundation *Backgrounder* No. 2428, June 24, 2010, <http://www.heritage.org/Research/Reports/2010/06/New-START-Potemkin-Village-Verification>.
32. News release, "Key Facts About the New START Treaty," The White House, March 26, 2010, <http://www.whitehouse.gov/the-press-office/key-facts-about-new-start-treaty> (accessed September 16, 2014).
33. Michaela Dodge, "U.S. Nuclear Weapons in Europe: Critical for Transatlantic Security," Heritage Foundation *Backgrounder* No. 2875, February 18, 2014, <http://www.heritage.org/research/reports/2014/02/us-nuclear-weapons-in-europe-critical-for-transatlantic-security>.
34. Ibid.
35. John T. Cappello, Gwendolyn M. Hall, and Stephen P. Lambert, "Tactical Nuclear Weapons: Debunking the Mythology," USAF Institute for National Security Studies *Occasional Paper* No. 46, August 2002, p. 11.
36. Dodge, "U.S. Nuclear Weapons in Europe: Critical for Transatlantic Security."
37. U.S. Department of Defense, *Nuclear Posture Review Report*, April 2010, p. iii, <http://www.defense.gov/npr/docs/2010%20nuclear%20posture%20review%20report.pdf> (accessed September 16, 2014).
38. News release, "Fact Sheet: Nuclear Weapons Employment Strategy of the United States," The White House, June 19, 2013, <http://www.whitehouse.gov/the-press-office/2013/06/19/fact-sheet-nuclear-weapons-employment-strategy-united-states> (accessed September 16, 2014).
39. U.S. Department of State, "Fact Sheet: Transparency in the U.S. Nuclear Weapons Stockpile," April 29, 2014, <http://www.state.gov/t/avc/rls/225343.htm> (accessed September 16, 2014).
40. International Atomic Energy Agency, "Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran," Report by the Director General, GOV/2011/65, November 8, 2011, <http://www.iaea.org/Publications/Documents/Board/2011/gov2011-65.pdf> (accessed September 16, 2014).
41. We must not forget that the newly armed nations are already "using" their nuclear weapons in a nonmilitary sense: for example, to prevent significant intrusions into their political structure despite massive human rights violations or to limit retaliation in response to their aggressive behaviors. See Paul Bracken, *The Second Nuclear Age: Strategy, Danger, and the New Power Politics* (New York: Henry Holt and Company, 2012).
42. Spring, "Congressional Commission Should Recommend a 'Damage Limitation' Strategy."
43. Dodge, "U.S. Nuclear Weapons in Europe: Critical for Transatlantic Security."
44. North Atlantic Treaty Organization, "Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization," Adopted by Heads of State and Government at the NATO Summit in Lisbon, November 19-20, 2010, http://www.nato.int/strategic-concept/pdf/Strat_Concept_web_en.pdf (accessed September 16, 2014).
45. Ibid.
46. Press release, "Deterrence and Defence Posture Review," North Atlantic Treaty Organization, May 20, 2012, http://www.nato.int/cps/en/natolive/official_texts_87597.htm (accessed September 16, 2014).
47. News release, "Fact Sheet on U.S. Missile Defense Policy: A 'Phased, Adaptive Approach' for Missile Defense in Europe," The White House, September 17, 2009, http://www.whitehouse.gov/the_press_office/FACT-SHEET-US-Missile-Defense-Policy-A-Phased-Adaptive-Approach-for-Missile-Defense-in-Europe (accessed September 16, 2014).

48. Amaani Lyle, "Hagel: U.S. Bolstering Missile Defense," American Forces Press Service, March 15, 2013, <http://www.defense.gov/news/newsarticle.aspx?id=119543> (accessed September 16, 2014).
49. U.S. Department of Defense *Nuclear Posture Review Report*, April 2010.
50. "Fact Sheet: Nuclear Weapons Employment Strategy of the United States."
51. Ibid.
52. Ibid.
53. News release, "Fact Sheet: An Enduring Commitment to the U.S. Nuclear Deterrent," The White House, November 17, 2010, <http://www.whitehouse.gov/the-press-office/2010/11/17/fact-sheet-enduring-commitment-us-nuclear-deterrent> (accessed September 16, 2014).
54. U.S. Department of Defense, *Nuclear Posture Review Report*, April 2010.
55. Transcript, "2013 Carnegie International Nuclear Policy Conference: Morning Plenary Session: Prague 2.0? Deterrence, Disarmament, and Nonproliferation in Obama's Second Term," April 8, 2013, <http://carnegieendowment.org/files/0410carnegie-morning-plenary.pdf> (accessed September 16, 2014).
56. Michael Dowd, "How Rad Hard Do You Need? The Changing Approach to Space Parts Selection?" Maxwell Technologies White Paper, January 21, 2012, http://www.maxwell.com/images/documents/case_study_micro_e_how_rad_hard.pdf (accessed August 19, 2014); Eagle Picher Technologies, LLC, "Sar-10197 Aerospace Battery," <http://www.eaglepicher.com/images/Li-Ion/EP-SAR-10197-DATA-SHEET.pdf> (accessed August 19, 2014).
57. *Encyclopedia Britannica*, "Satellite Communication," December 26, 2013, <http://www.britannica.com/EBchecked/topic/524891/satellite-communication/288217/How-satellites-work> (accessed August 19, 2014).
58. Intelsat, "Tools & Resources: Satellite Station-Keeping," <http://www.intelsat.com/tools-resources/satellite-basics/satellite-station-keeping/> (accessed August 19, 2014).
59. News release, "Lockheed Martin-Built GPS Satellite Exceeds 10 Years On-Orbit," Lockheed Martin, February 15, 2011, <http://www.lockheedmartin.com/us/news/press-releases/2011/february/gps-10yr-anny.html> (accessed August 19, 2014).
60. GPS.gov, "Space Segment," August 2, 2014, <http://www.gps.gov/systems/gps/space/#generations> (accessed August 19, 2014).
61. Aerospace-Technology.com, "Wideband Global SATCOM (WGS) Satellite, United States of America," <http://www.aerospace-technology.com/projects/wgs-satellite/> (accessed August 19, 2014).
62. National Aeronautics and Space Administration, "Milstar 1," <http://nssdc.gsfc.nasa.gov/nmc/spacecraftDisplay.do?id=1994-009A> (accessed August 19, 2014); National Aeronautics and Space Administration, "Milstar 2," <http://nssdc.gsfc.nasa.gov/nmc/spacecraftDisplay.do?id=1995-060A> (accessed August 19, 2014); fact sheet, "Milstar," U.S. Air Force, Los Angeles Air Force Base, February 11, 2014, <http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5328> (accessed August 19, 2014).
63. News release, "Military Communications Satellite Built by Lockheed Martin Achieves 10 Years in Service," Lockheed Martin, February 26, 2010, <http://www.lockheedmartin.com/us/news/press-releases/2010/february/DSCS-10-YR.html> (accessed August 19, 2014).
64. News release, "Northrop Grumman-Built DSP Flight 14 Celebrates 20 Years On-Orbit," Northrop Grumman, June 12, 2009, http://www.globenewswire.com/newsarchive/noc/press/pages/news_releases.html?d=167062 (accessed August 19, 2014); news release, "Defense Support Program Satellite Decommissioned," Northrop Grumman, July 31, 2008, http://www.globenewswire.com/newsarchive/noc/press/pages/news_releases.html?d=147496 (accessed August 19, 2014).
65. GPS.gov, "Space Segment."
66. News release, "Lockheed Martin Delivers Third SBIRS HEO Satellite Payload to U.S. Air Force," Lockheed Martin, July 1, 2013, <http://www.lockheedmartin.com/us/news/press-releases/2013/july/0701-ss-sbirs.html> (accessed August 19, 2014).
67. Fact sheet, "Defense Support Program (DSP) Satellites," U.S. Air Force, Los Angeles Air Force Base, February 11, 2014, <http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5323> (accessed August 19, 2014); Missile Threat, "Defense Support Program (DSP)," last updated April 29, 2013, <http://missilethreat.com/defense-systems/defense-support-program-dsp/> (accessed August 19, 2014).
68. News release, "6th Boeing-built Wideband Satellite Expands Tactical Communications," Boeing, August 7, 2013, <http://boeing.mediaroom.com/2013-08-07-6th-Boeing-built-Wideband-Satellite-Expands-Tactical-Communications> (accessed August 19, 2014).
69. Fact sheet, "Wideband Global SATCOM Satellite," U.S. Air Force Space Command, June 8, 2012, <http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=5582> (accessed August 19, 2014).
70. Lockheed Martin, "Advanced Extremely High Frequency (AEHF)," <http://www.lockheedmartin.com/us/products/advanced-extremely-high-frequency--aehf-.html> (accessed August 19, 2014); fact sheet, "Advanced Extremely High Frequency (AEHF) Satellite System," U.S. Air Force, Los Angeles Air Force Base, February 11, 2014, <http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5319> (accessed August 19, 2014).
71. Ibid.

72. Lockheed Martin, "Mobile User Objective System (MUOS)," <http://www.lockheedmartin.com/us/products/mobile-user-objective-system--muos-.html> (accessed August 19, 2014); U.S. Navy, Space and Naval Warfare Systems Command, "MUOS-2 Launch from Cape Canaveral Air Force Station, Fla., July 19, 2013," <http://www.public.navy.mil/spawar/Press/Pages/MUOS-2.aspx> (accessed August 19, 2014).
73. GPS.gov, "Space Segment."
74. Lockheed Martin, "Space Based Infrared System," http://www.lockheedmartin.com/content/dam/lockheed/data/space/documents/sbirs/1_SBIRSIInformationalBrochure.pdf (accessed August 19, 2014).
75. Boeing, "Transformational Wideband Communication Capabilities for the Warfighter," http://www.boeing.com/boeing/defense-space/space/bss/factsheets/702/wgs/wgs_factsheet.page (accessed August 19, 2014); U.S. Air Force Space Command fact sheet, "Wideband Global SATCOM Satellite."
76. Lockheed Martin, "Advanced EHF: Assured, Protected, Survivable," July 25, 2013, http://www.lockheedmartin.com/content/dam/lockheed/data/space/documents/AEHF/B1369220_AEHF_7.25.13.pdf (accessed August 19, 2014); Northrup Grumman, "AEHF Payload: Assured, protected, survivable communications," 2014, http://www.northropgrumman.com/Capabilities/AdvancedEHFPayloads/Documents/pageDocs/AEHF_datasheet.pdf (accessed August 19, 2014).
77. Barry Rosenberg, "DOD's Reliance on Commercial Satellites Hits New Zenith," Defense Systems, February 25, 2010, <http://defensesystems.com/articles/2010/03/11/cover-story-the-satcom-challenge.aspx> (accessed September 18, 2014).
78. Lockheed Martin, "Mobile User Objective System (MUOS)."
79. International GNSS Service, "BeiDou Constellation Status Information," February 25, 2014, http://igs.org/mgex/Status_BDS.htm (accessed August 19, 2014); BBC News, "China's Beidou GPS-Substitute Opens to Public in Asia," December 27, 2012, <http://www.bbc.com/news/technology-20852150> (accessed August 19, 2014).
80. Dean Cheng, "Prospects for U.S.-China Space Cooperation," testimony before the Committee on Commerce, Science, and Transportation, U.S. Senate, April 9, 2014, <http://www.heritage.org/research/testimony/2014/04/prospects-for-us-china--space-cooperation>.
81. Dean Cheng, "China's Space Program: A Growing Factor in U.S. Security Planning," Heritage Foundation *Backgrounder* No. 2594, August 16, 2011, <http://www.heritage.org/research/reports/2011/08/chinas-space-program-a-growing-factor-in-us-security-planning>.
82. Stephen Clark, "Third Soyuz Launch in a Week Bolsters Glonass System," *Spaceflight Now*, April 26, 2013, <http://www.spaceflightnow.com/news/n1304/26soyuz/#.U-uxP2Oa-0Y> (accessed August 19, 2014).
83. Anatoly Zak, "Spooky World of Military Satellites," RussianSpaceWeb.com, August 3, 2014, http://www.russianspaceweb.com/spacecraft_military.html (accessed August 19, 2014); Stephen Clark, "Russia Launches 3 New Military Satellites," Space.com, January 17, 2013, <http://www.space.com/19307-russia-launches-military-satellites.html> (accessed August 19, 2014).
84. Jeff Kueter and John B. Sheldon, "An Investment Strategy for National Security Space," Heritage Foundation *Special Report* No. 129, February 20, 2013, p. 3, http://thf_media.s3.amazonaws.com/2013/pdf/SR129.pdf.
85. Rosenberg, "DOD's Reliance on Commercial Satellites Hits New Zenith."
86. Ibid.
87. Kueter and Sheldon, "An Investment Strategy for National Security Space," p. 15.
88. The phrase "able to do what they need to do" is a relative condition in that requests for support will likely always exceed available resources. Space-based platforms are limited in number, while the intelligence targets on which one might want to collect information or the global activities of the U.S. military for which one likely needs support are expansive. Thus, demands for satellite support are prioritized, and resources are allocated accordingly. If a higher-priority request arises, some ongoing task of lesser priority gets "bumped." Still, in general terms, the U.S. military is able to execute the missions assigned to it. Whether the U.S. intelligence community is likewise able to do so is a matter of conjecture given the high levels of classification that accompany intelligence collection operations. It is also important to note that the role of warning/intelligence becomes even more critical when the size and capabilities of one's armed forces shrinks.
89. Robert Butterworth, "In Space, Doing More with Less Much Scarier than Budget Cuts," George C. Marshall Institute, March 5, 2012, <http://marshall.org/space-policy/in-space-doing-more-with-less-much-scarier-than-budget-cuts/> (accessed September 18, 2014).
90. Mark Ward, "Celebrating 40 Years of the Net," BBC News, October 29, 2009, <http://news.bbc.co.uk/2/hi/technology/8331253.stm> (accessed February 7, 2014).
91. Rupert Goodwins, "Ten Computer Viruses that Changed the World," ZDNet, August 3, 2011, <http://www.zdnet.com/ten-computer-viruses-that-changed-the-world-3040093590/> (accessed August 8, 2014)
92. Barry M. Leiner et al., "Brief History of the Internet," Internet Society, <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet> (accessed July 23, 2014).

93. The cyber community lacks a clear, agreed-upon definition of “cyber weapon.” That said, one prominent definition put forward by security researchers at London’s King’s College defines a cyber weapon as “computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings.” This definition allows for a range of cyber weapons, from the weak denial of service attack to the advanced attacks that cripple or destroy physical devices. Some have argued that such a definition remains too broad and ought to be limited to more severe attacks with physical effects. Be that as it may, this *Index* uses one broad definition so as to not miss a cyber attack that could be considered a cyber weapon. For more information, see Thomas Rid and Peter McBurney, “Cyber-Weapons,” *The RUSI Journal*, Vol. 157, Issue 1 (2012), pp. 6–13, <http://www.tandfonline.com/doi/full/10.1080/03071847.2012.664354#tabModule> (accessed August 8, 2014).
94. “What Is Cybercrime?,” Norton by Symantec, <http://us.norton.com/cybercrime-definition> (accessed July 23, 2014); “Cyberespionage,” Oxford Dictionaries, http://www.oxforddictionaries.com/us/definition/american_english/cyberespionage (accessed July 23, 2014); Dimitar Kostadinov, “Cyber Exploitation,” InfoSec Institute, February 25, 2013, <http://resources.infosecinstitute.com/cyber-exploitation> (accessed July 23, 2014).
95. *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, ed. Michael N. Schmitt (Cambridge, UK: Cambridge University Press, 2013), p. 54, http://issuu.com/nato_ccd_coe/docs/tallinmanual?e=5903855/1802381 (accessed August 8, 2014).
96. As illustrated by these experts’ division on the issue (see *Tallinn Manual*, p. 56), ascertaining where exactly hard power ends and softer forms of power such as espionage and sabotage begins is difficult. This index will not try to solve this definitional and legal problem but will merely consider a viable but not overbroad definition that could be used by the U.S. or other nations in determining their response to serious cyber attacks.
97. Brett T. Williams, “The Joint Force Commander’s Guide to Cyberspace Operations,” *Joint Force Quarterly*, Vol. 73, Second Quarter 2014, pp. 12–19, <http://ndupress.ndu.edu/News/NewsArticleView/tabid/7849/Article/8461/jfq-73-the-joint-force-commanders-guide-to-cyberspace-operations.aspx> (accessed August 8, 2014).
98. David Clark, “Characterizing Cyberspace: Past, Present and Future,” MIT CSAIL, Version 1.2 of March 12, 2010, https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf (accessed July 23, 2014); Department of the Army, *The U.S. Army’s Cyberspace Operations Concept Capability Plan 2016–2028*, TRADOC Pamphlet No. 525-7-8, February 22, 2010, <http://fas.org/irp/doddir/army/pam525-7-8.pdf> (accessed August 8, 2014).
99. Robert Belk and Matthew Noyes, *On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy*, Harvard University, John F. Kennedy School of Government, Belfer Center for Science and International Affairs, March 20, 2012, http://belfercenter.ksg.harvard.edu/publication/22046/on_the_use_of_offensive_cyber_capabilities.html (accessed July 23, 2014).
100. Heather Leonard, “There Will Soon Be One Smartphone for Every Five People in the World,” *Business Insider*, February 7, 2013, <http://www.businessinsider.com/15-billion-smartphones-in-the-world-2013-2> (accessed July 23, 2014); “Computers Sold This Year Worldwide,” Worldometers, <http://www.worldometers.info/computers/> (accessed July 23, 2014).; Emily Adler, “Here’s Why ‘The Internet of Things’ Will Be Huge, and Drive Tremendous Value for People And Businesses,” *Business Insider*, December 7, 2013, <http://www.businessinsider.com/growth-in-the-internet-of-things-2013-10#ixzz39ojCP5oL> (accessed August 8, 2014).
101. News release, “Presidential Policy Directive—Critical Infrastructure Security and Resilience,” The White House, February 12, 2013, <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (accessed July 23, 2014).
102. Steven P. Bucci and Andy Bochman, “Plotting a More Confident Course: Rethinking Oversight of the Electric Sector and Critical Infrastructure Cybersecurity,” Heritage Foundation *Special Report* No. 150, January 29, 2014, <http://www.heritage.org/research/reports/2014/01/plotting-a-more-confident-course-rethinking-oversight-of-the-electric-sector-and-critical-infrastructure-cybersecurity>.
103. Belk and Noyes, *On the Use of Offensive Cyber Capabilities*, p. 16.
104. In the event of a serious attack, however, nations that are attacked might attach certain levels of responsibility to the nation that is the source of the attack, depending on the perceived complicity of the source country’s government in such attacks. For more information, see Jason Healey, “Beyond Attribution: Seeking National Responsibility for Cyber Attacks,” Atlantic Council *Issue Brief*, January 2012, https://www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf (accessed August 8, 2014).
105. Nicole Perloth, “Chinese Hackers Infiltrate New York Times Computers,” *The New York Times*, January 30, 2013, <http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&r=0> (accessed July 23, 2014).
106. Stewart Baker, “The Attribution Revolution,” *Foreign Policy*, June 17, 2013, http://www.foreignpolicy.com/articles/2013/06/17/the_attribution_revolution_plan_to_stop_cyber_attacks (accessed July 23, 2014); Alexander Melnitzky, “Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses,” *Cardozo Journal of International and Comparative Law*, Vol. 20, Issue 2 (Winter 2012), pp. 537–570, http://www.cjicl.com/uploads/2/9/5/9/2959791/cjicl_20.2_melnitzky_note.pdf (accessed July 23, 2014).
107. Baker, “The Attribution Revolution.”

108. David M. Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, <http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008> (accessed July 23, 2014).
109. Belk and Noyes, *On the Use of Offensive Cyber Capabilities*.
110. Maren Leed, "Offensive Cyber Capabilities at the Operational Level: The Way Ahead," Center for Strategic and International Studies and Georgia Tech Research Institute, September 2013, http://csis.org/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf (accessed July 23, 2014).
111. William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, Vol. 89, No. 5 (September/October 2010), <http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain> (accessed July 23, 2014).
112. U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, p. 2, <http://www.defense.gov/news/d20110714cyber.pdf> (accessed July 23, 2014).
113. Lewis Page, "Upgrade Drags Stealth Bomber IT Systems into the 90s," *The Register*, July 11, 2008, http://www.theregister.co.uk/2008/07/11/stealth_bomber_upgrades/ (accessed July 23, 2014); David Noland, "Could One Email Have Stopped a \$1.4B Stealth Bomber Crash?" *Popular Mechanics*, July 2, 2008, <http://www.popularmechanics.com/technology/military/planes-uavs/4271563> (accessed July 23, 2014); U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, p. 3.
114. James A. Lewis and Katrina Timlin, Center for Strategic and International Studies, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization*, United Nations Institute for Disarmament Research, 2011, <http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf> (accessed August 8, 2014)
115. Lynn, "Defending a New Domain."
116. Leed, "Offensive Cyber Capabilities at the Operational Level," p. 1.
117. Margaret Rouse, "Confidentiality, Integrity, and Availability (CIA Triad)," WhatIs.com, May 2013, <http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA> (accessed August 8, 2014); Shirley Radack, "Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems," National Institute of Standards and Technology, <http://www.itl.nist.gov/lab/bulletns/bltnmar04.htm> (accessed August 8, 2014).
118. Pranita Joshi, Gajendra Singh Chandel, and Subham Joshi, "A Survey on: Resource Consumption Index of Denial of Service Attack in MANET," *International Journal of Science, Engineering and Technology Research*, Vol. 2, No. 2 (February 2013), <http://ijsetr.org/wp-content/uploads/2013/07/IJSETR-VOL-2-ISSUE-2-314-318.pdf> (accessed July 23, 2014).
119. Edison Electric Institute, "Frequently Asked Questions About Cybersecurity and the Electric Power Industry," June 2013, http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Cybersecurity_FAQweb_June2013.pdf (accessed July 23, 2014); Bucci and Bochman, "Rethinking Oversight of the Electric Sector and Critical Infrastructure Cybersecurity"; U.S. Department of Homeland Security, "Securing Industrial Control Systems in the Chemical Sector," April 2011, <http://www.dhs.gov/xlibrary/assets/oip-chemsec-case-for-action-042011.pdf> (accessed July 23, 2014).
120. These colorful terms all have rather specific meanings. Some, like "ransomware," one can understand from the name itself. Others, like "rootkit," are more technical and obscure. For a useful guide to the bestiary of malware, see Roger A. Grimes, "Your Quick Guide to Malware Types," *InfoWorld*, December 23, 2012, <http://www.infoworld.com/d/security/your-quick-guide-malware-types-205450?page=0,0> (accessed September 30, 2013), and Symantec Corporation, *Internet Security Threat Report*, Vol. 18, April 2013, http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr-18 (accessed September 30, 2013).
121. Veracode, "Common Malware Types: Cybersecurity 101," October 12, 2012, <http://blog.veracode.com/2012/10/common-malware-types-cybersecurity-101/> (accessed July 23, 2014).
122. Rachael King, "Why 'Air Gaps' Don't Always Work in Cybersecurity," *The Wall Street Journal*, July 3, 2014, <http://blogs.wsj.com/cio/2014/07/03/why-air-gaps-dont-always-work-in-cybersecurity/> (accessed August 8, 2014); David Inserra and Steven Bucci, "Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," *Heritage Foundation Backgrounder* No. 2880, March 6, 2014, <http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace>.
123. Rod Soderbery, "How Many Things Are Currently Connected to the 'Internet of Things' (IoT)?" *Forbes*, January 7, 2013, <http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot/> (accessed September 30, 2013); Julie Bort, "How Many Web Sites Are There?" *Business Insider*, March 8, 2012, <http://www.businessinsider.com/how-many-web-sites-are-there-2012-3> (accessed September 30, 2013).
124. U.S. Computer Emergency Readiness Team, "Security Tip (ST04-015): Understanding Denial-of-Service Attacks," last revised February 6, 2013, <http://www.us-cert.gov/ncas/tips/ST04-015> (accessed September 30, 2013).
125. Cory Janssen, "What Is Phlashing?" *Techopedia*, <http://www.techopedia.com/definition/15270/phlashing> (accessed July 23, 2014).
126. Hollis, "Cyberwar Case Study: Georgia 2008."
127. Inserra and Bucci, "Cyber Supply Chain Security."

-
128. John Villasenor, "Compromised by Design: Securing the Defense Electronics Supply Chain," Brookings Institution, Center Technology Innovation and Center for 21st Century Security and Intelligence, November 4, 2013, <http://www.brookings.edu/research/papers/2013/11/4-securing-electronics-supply-chain-against-intentionally-compromised-hardware-villasenor> (accessed July 23, 2014).
 129. Working in an impaired manner may be just as dangerous as or even more dangerous than causing a system to fail outright. For example, a bug that made every missile miss its target by several yards might not be immediately apparent as a cyber attack, even though it is dramatically affecting the effectiveness of U.S. weapons. Systems that are not working properly, on the other hand, might pose an immediate problem, but alternative systems and replacements can mitigate this difficulty.
 130. John Villasenor, "Ensuring Hardware Cybersecurity," Brookings Institution *Issues in Technology Innovation* No. 9, May 2011, <http://www.brookings.edu/research/papers/2011/05/hardware-cybersecurity> (accessed September 30, 2013).
 131. Symantec Corporation, "Advanced Persistent Threats: A Symantec Perspective," White Paper, 2011, http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf (accessed September 30, 2013).
 132. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, February 18, 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (accessed August 8, 2014).
 133. Alec Russell, "CIA Plot Led to Huge Blast in Siberian Gas Pipeline," *The Telegraph*, February 28, 2004, <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html> (accessed July 23, 2014).
 134. David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, February 26, 2013, <http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet> (accessed July 23, 2014).
 135. One of the most notable examples of large-scale physical damage caused by a cyber attack is the "Aurora" experiment. In 2006, controlled hacking by the Idaho National Laboratory was able to cause a large electrical generator to break. For more information, see CNN, "Staged Cyber Attack Reveals Vulnerability in Power Grid," September 27, 2007, <https://www.youtube.com/watch?v=fJyWngDco3g> (accessed August 8, 2014); Rid and McBurney, "Cyber-Weapons."

Regions of Enduring Interest: Latin America, the Caribbean, and Africa

Ana R. Quintana and Charlotte M. Florance

The United States has an abiding geopolitical interest in both the Latin America/Caribbean region and Africa, an interest that derives from America's close economic, cultural, and demographic ties with these two regions. Though their security challenges do not rise to a level at which they threaten the vital national interests of the U.S., numerous destabilizing forces still plague these regions, posing substantial hurdles to their economic development and political stability.

Challenges aside, these areas also present great opportunities. The U.S. certainly remains engaged with the governments and peoples of the states that comprise Africa and greater Latin America, but so too do competitors of the U.S.—rivals who seek to gain access to these regions' markets and resources and, for good or ill, cultivate relationships that support competing security agendas. As the U.S. considers just how much it should invest in its defense, it should remain mindful of these regions and the role that they play in geostrategic affairs.

Latin America and the Caribbean

Due to geographic proximity, high levels of trade, persistently growing demographic and cultural ties, and a lengthy history of diplomatic connections, the U.S. has strong links to and strategic interests in Latin America. Although regional security threats of the type that plague the Middle East and Africa and major threat actors like China, Russia, Iran, and North Korea are absent from Latin America, the U.S. still has a vested interest in the region's economic and political stability.

Transnational organized crime continues to proliferate throughout Latin America, fueling violence, eroding the rule of law, and hindering economic development. While overall homicide rates have decreased around the world, this region has experienced a very different trend: Excluding anomalies like Chile and Costa Rica, the Central American and South American subregions are among the most dangerous in the world.

Successes in eradicating Colombian cartels and increased counter-crime initiatives in Mexico have pushed drug trafficking organizations into Central America, where smaller and poorer governments are ill-equipped to deal with such violent entities. In addition, a resurgence of illicit smuggling routes in the Caribbean corridor has raised concerns about the future of U.S. maritime interdiction efforts.

Violence and associated criminality continue in Mexico's ongoing drug war, affecting not only Mexico, but also the U.S. because of the cross-border trafficking of illicit drugs that links the Mexican cartels with U.S.-based gangs. In many regions where police have failed, vigilante and militia groups have emerged—an attempt to restore order that only highlights the deficiencies of the central government. Venezuela has emerged as a major regional and international drug trafficking hub, with established networks throughout Central and South America, the Caribbean, and West Africa.

U.S. instruments of foreign policy vary throughout the region. Free trade agreements and bilateral economic assistance play an important role

in expanding markets for U.S. exports as well as in building partner capacity. While security cooperation between the U.S. and regional partners plays a critical role in combating transnational criminal organizations, such arrangements are quite uneven across the region as a whole, with the bulk of assistance going to Colombia and Mexico.

Current U.S. Military Presence in Latin America and the Caribbean

The United States' Northern and Southern Commands (USNORTHCOM and USSOUTHCOM) handle U.S. military engagement with the countries of Latin America and the Caribbean.

- **U.S. Northern Command.** NORTHCOM, headquartered at Peterson Air Force Base, Colorado, focuses on Mexico and much of the Caribbean: the U.S. Virgin Islands, British Virgin Islands, Bermuda, Puerto Rico, The Bahamas, and the Turks and Caicos Islands. NORTHCOM's Joint Task Force North (JTF North), based at Biggs Army Airfield, Fort Bliss, Texas, provides support to federal law enforcement agencies interdicting potential transnational threats within and along approaches to the U.S. (e.g., narco-trafficking, alien smuggling, and international terrorism).
- **U.S. Southern Command.** USSOUTHCOM's area of responsibility for U.S. security interests includes the continental landmass south of Mexico, its surrounding waters, and the Caribbean Sea. Headquartered in Doral, Florida, USSOUTHCOM oversees the coordination of U.S. military efforts with 31 countries and 15 territories. USSOUTHCOM focuses on supporting federal and foreign agencies countering transnational organized crime, working with the militaries of the region, contingency planning, and terrorist detention (Naval Station Guantanamo Bay).

Trade and Energy in Latin America

High levels of trade and integrated economies have created strong connections between Latin America and the United States. The region is America's fastest-growing regional trade partner: The U.S. sells more goods to Latin America and the Caribbean than it sells to the entire European Union (EU). Out of the 20 free trade agreements (FTAs) that the U.S. has entered into force, 11 are with countries in Latin America.

Approaching its 20th anniversary, the North American Free Trade Agreement (NAFTA) with Canada and Mexico surpasses America's trade with the EU and Japan combined—and even with China. The U.S. is also party to the Dominican Republic–Central America–United States Free Trade Agreement (CAFTA–DR) with Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, and the Dominican Republic. Bilateral FTAs with Colombia, Chile, Peru, and Panama also have been implemented.

Aside from trade, the U.S. energy sector is heavily reliant on the Latin America/Caribbean region. The U.S. imports about 40 percent of the crude oil and petroleum that it consumes, and more than half of this 40 percent comes from the Western Hemisphere.¹ The largest suppliers of these imports are Canada (28 percent); Mexico (10 percent); and Venezuela (9 percent). In comparison, Persian Gulf countries Bahrain, Iraq, Kuwait, Qatar, Saudi Arabia, and the United Arab Emirates supply 29 percent.

Strategically, the region's geographic proximity to the U.S. increases its importance to America's national interests. The U.S. shares an almost 2,000-mile border with Mexico that spans Texas, New Mexico, Arizona, and California. In 2013, the U.S.–Mexico border was crossed by over 166 million people and nearly 72 million vehicles, making it the most heavily trafficked border in the world.²

Mexico: Transnational Criminal Organizations, Gangs, and Violence

With the dismantling of Colombian cartels in the 1990s, the illicit drug trade in Latin America shifted northward. Mexico is a large producer, supplier, and transit zone for U.S.-bound cocaine, heroin, methamphetamine, and marijuana. Over 95 percent of the cocaine sold in the U.S. is transported through Mexico. At the helm of this destabilizing threat are transnational criminal organizations (TCOs) and gangs that operate throughout Mexico. Competing TCOs—in this case, Mexican cartels—vie for control of key smuggling routes into the U.S. and critical transshipment points within Mexico.

Mexican cartels operate as full-scale criminal enterprises, controlling vast systems of illicit networks throughout the U.S., Mexico, Central America, and the Caribbean. In addition to wholesale distribution of the majority of illicit drugs in the U.S., Mexican cartels also engage in human smuggling and trafficking, kidnapping, extortion, and arms trafficking.

The illegal drug trade alone accounts for roughly \$30 billion in annual revenue for the cartels,³ an amount equal to the gross domestic products of Honduras and Nicaragua combined,⁴ thus enabling them to corrupt local authorities or overwhelm them by force. While noteworthy cartel-related violence has yet to spill over into the U.S., the corrosive effect that these criminal organizations have on the rule of law, citizen security, and good governance affects U.S. security and national interests.

High-level corruption within the Mexican government and security forces continues to undermine U.S.–Mexico cooperation. The United States has provided Mexico with counter-drug assistance since the 1970s, but after the assassination of a U.S. Drug Enforcement Agency agent in 1985, bilateral cooperation slowed. Following the signing of a Binational Drug Control Strategy in 1998, however, collaboration improved.

To date, the most significant cooperation between the U.S. and Mexico has come through the Mérida Initiative, which emphasized the shared responsibility of both countries to combat drug trafficking and organized crime. Between fiscal year 2008 and FY 2014, over \$2.4 billion was allocated to Mexico for this security initiative, with additional supplements as needed.⁵

Central America's Northern Triangle

All three of Central America's Northern Triangle countries—Guatemala, Honduras, and El Salvador—are facing a number of chronic crises. Rampant corruption and weak state institutions have rendered central governments incapable of combating threats posed by violent transnational gangs and organized criminal groups. These illicit groups have embedded themselves into these governments and are creating criminalized states. All three countries have been unable to respond effectively to their security problems.

Located along a critical trafficking route, Honduras alone is a layover spot for upwards of 79 percent of northward-bound drug flights. Much of the U.S.-bound methamphetamine supply is produced in Central America.

Historically, this region is also one of the most violent in the world. Honduras has the world's highest annual homicide rate, averaging 91 deaths per 100,000 people. El Salvador is fourth with an average of 41 per 100,000, and Guatemala is fifth at 40

per 100,000. In comparison, the U.S. registers five homicides for every 100,000 people. A shaky gang truce in El Salvador reduced overall homicide rates from March 2012 to mid-2014, but these gangs still perpetrated other violent crimes. A multitude of transnational criminal organizations like the Mexican Zetas and Sinaloa drug cartels have capitalized on the weak governments of the Northern Triangle and are now fully operational within the region.

Much like the trend seen in Central America, islands like Puerto Rico and the Dominican Republic are increasingly becoming layover spots for U.S.-bound illicit drugs. Because it is a U.S. territory, shipments coming in from Puerto Rico are subject to less scrutiny than are international shipments, a fact that further undermines maritime interdiction.⁶

Interference of Foreign Adversaries and Countering of U.S. Influence

America's geopolitical foes have exploited and will continue to exploit the region's proximity to the U.S. homeland by seeking relationships with willing regional partners to counter U.S. influence. Although these activities do not pose a direct security threat at the moment, these foreign adversaries are finding receptive hosts within countries that view the U.S. as an ideological opponent: specifically, the Bolivarian Alliance (ALBA) countries of Venezuela, Cuba, Ecuador, Nicaragua, and Bolivia.

One of America's primary adversaries, Russia, is developing strategic regional partnerships in the form of military cooperation, arms sales, trade agreements, and even cooperation in counternarcotic operations. In addition to high-profile visits by the Russian Navy's Interfleet Surface Action Group to Cuba, Nicaragua, and Venezuela, Russia used a regional exercise to deploy two long-range strategic bombers to Venezuela and Nicaragua and, following its annexation of Crimea, announced plans to build military bases in Nicaragua, Cuba, and Venezuela.

Activities like these have not been seen for over three decades. Venezuela has purchased a noteworthy amount of weapons from Russia, including tanks, "Sukhoi fighter jets, combat helicopters, and over 100,000 light weapons" as well as "a license to produce them in Venezuela."⁷ Reports also indicate that in 2008, Russia sold a batch of Igla-S (SA-24) shoulder-fired anti-aircraft missiles to Venezuela.⁸

The People's Republic of China (PRC) has been another active player in the region. Much of Chi-

na's engagement has focused on expanding bilateral economic relations and major investments in infrastructure development projects. Currently, the PRC has proposed to invest \$40 billion in constructing an interoceanic canal in Nicaragua that is set to rival the Panama Canal. Joint military exercises have largely been of a humanitarian nature, such as exercises with regional armed forces in which medical services are provided in rural villages.

In 2013, the Chinese People's Liberation Army Navy (PLAN) conducted a three-country visit and had its first naval exercise with the Argentine Navy.⁹ Visits to the region by senior PLA leaders are common, and virtually every country in Latin America maintains a permanent defense attaché in the PRC. The bulk of defense sales have gone to ALBA countries, illustrating China's intent to leverage relationships with Latin American countries that are explicitly anti-U.S.

Iran's growing presence in Latin America has raised concerns in the U.S. Tehran has spent the past decade increasing its regional economic relations and diplomatic presence, particularly in the ALBA countries. Within Venezuela, Ecuador, Bolivia, and Argentina, it has found hospitable allies and has developed favorable relations.

Credible unclassified reporting indicates that Hezbollah's presence in Latin America is limited to ideological or religious sympathizers and criminal facilitators who see opportunity in linking drug, contraband, and weapons trafficking to the illicit network and external market access managed by Hezbollah.¹⁰ Regional supporters of other international terrorist organizations engage in money laundering and, quite possibly, even recruiting.

Financed by Venezuela and initiated by late Venezuelan President Hugo Chávez, the socialist ALBA bloc has spearheaded a wave of anti-Americanism throughout Latin America. Uniting the countries of Latin America to reduce the U.S.'s regional power and presence has been the core tenet of the 21st century socialist movement. ALBA member countries Cuba, Nicaragua, Ecuador, and Bolivia have expelled some U.S. diplomats, shut down U.S.-led counternarcotic programs, and hampered bilateral trade negotiations. In 2011, the president of Ecuador revoked the U.S.'s access to its Manta military base—the only forward operating location in Latin America, from which U.S. forces have worked alongside the Ecuadorian military on Andean counternarcotic and surveillance programs.

The rise of regional groups that purposefully exclude the U.S. indicates the movement's pervasiveness. Multilateral organizations like South American Nations (UNASUR) and the Community of Latin American and Caribbean States (CELAC) seek to circumvent the power of the Organization of American States (OAS), the only one to which the U.S. is a party.

The government of Venezuela continues to sustain the Castro regime in Cuba. Caracas annually provides Havana with an average of \$10 billion in subsidized oil and currency—more than twice the amount that Cuba received from the Soviet Union at the height of the Cold War. In exchange, Cuba provides Venezuela with critical military and intelligence resources as well as civilian slave labor.

Of a more sinister nature are the government's connections to regional and international terrorist groups. For example, the Colombian narco-terrorist organization, the FARC, has long enjoyed sanctuary within Venezuelan territory, reportedly with the support of Venezuelan officials. High-ranking members of the Venezuelan government have provided support to Hezbollah as well. Venezuela's equivalents of the U.S. Attorney General, Secretary of Homeland Security, and FBI Director are considered to be "Significant Foreign Narcotics Traffickers."¹¹ In 2008, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) found that Venezuela's most senior diplomat at its embassy in Syria facilitated the travel of two Hezbollah representatives who were attempting to raise funds and open a Hezbollah community center in Venezuela.¹²

In terms of conventional military power, ALBA member countries do not pose a major threat to the U.S., but the radical form of socialist populism that they promote has undermined traditional U.S. foreign policy objectives. The regional bloc continuously seeks to create a hostile environment for the U.S., undermining America's attempts at regional cooperation. In addition to using regional proxies to unite the Americas against the U.S., ALBA nations have consistently provided sanctuary to regional and global terrorist organizations, transnational criminal organizations, and international pariahs. Currently, Iran and Syria are observer states in ALBA.

Africa

The United States has strategic, economic, and historic interests in Africa. Although there is a high probability that regional security risks will not

directly threaten the territorial integrity of the U.S. homeland or result in a major regional war or significant loss of freedom of maneuverability of the commons, the U.S. continues to have a vested interest in countering threats on the African continent and maintaining regional stability.

Small and local problems can quickly become large and regional in ways that would threaten U.S. vital national interests. One needs to look no further than Afghanistan in Central Asia or Syria in the Middle East to see the potential for states and violent non-state actors (terrorist groups) to pose such threats far beyond their local origins. Destabilized and ungoverned areas often serve as sanctuaries for organizing, planning, maturing, and training for activities that eventually reach far beyond these sanctuaries. Accordingly, religious extremism, ethnic conflicts, authoritarian regimes, ungoverned space, and insecure energy supply lines define the direct areas of concern for the United States and its partners within the region.

In 2013–2014, the African continent saw an uptick in violent conflict in the Central African Republic, Libya, Mali, and South Sudan, as well as the ongoing conflicts in Somalia, Nigeria, and the Democratic Republic of Congo. Additional areas of concern include the increase in maritime piracy in the Gulf of Guinea, illicit drugs, wildlife and arms trafficking, and terrorist groups linked to al-Qaeda. The threat of terrorism and the additional pressures from refugees on governments such as Niger and Cameroon also have added to an increasing potential for future conflict hot spots.

Current U.S. Military Presence in Africa

In October 2007, U.S. Africa Command (AFRICOM) was established to effect better coordination of all U.S. military engagements with the countries of Africa (except Egypt, for which the U.S. Central Command has responsibility), including the continent's island nations and surrounding waters. AFRICOM is responsible for the Pentagon's relations with African countries; the African Union (a regional union that consists of 53 African states but excludes Morocco);¹³ and African regional security organizations such as the Economic Commission of West African States' Department of Defense.¹⁴ While its headquarters is not physically located in Africa, AFRICOM is the primary instrument by which the U.S. works with Africa's various militaries.

AFRICOM is headquartered at Kelley Barracks in Stuttgart-Moerhingen, Germany. The newest geographic combatant command, AFRICOM, initially a sub-unified command under U.S. European Command, officially became a separate combatant command in October 2008. AFRICOM supports a broad range of U.S. agencies and supports the Department of State in outreach and relationship building.

AFRICOM addresses a multiplicity of threats emanating from Africa—challenges that require non-traditional military solutions and encouraging long-term partnerships aimed at addressing the root causes of problems that plague the region. During the initial rollout of AFRICOM, one U.S. official claimed that the command would be a success “if it keeps U.S. troops out of Africa for the next 50 years.”¹⁵

AFRICOM currently serves as a test case for the Army's program to develop regionally aligned brigades. Such brigades would focus on an assigned region and align their unit and personnel training accordingly to include language skills, cultural familiarity, exercise scheduling, and analysis of evolving security conditions. Missions assigned to these brigades would range from two-person teams working closely with local counterparts to accomplish sensitive tasks to more than 300 soldiers conducting airborne and humanitarian training with partner country forces. These units will have conducted more than 100 missions in 2014.¹⁶

AFRICOM is supported by six subordinate commands:

- U.S. Army Africa (USARAF), operating out of Vicenza, Italy;
- U.S. Naval Forces Africa (NAVAF), headquartered in Naples, Italy, and with its staff shared with U.S. Naval Forces Europe;
- U.S. Air Forces Africa (AFAFRICA), located at Ramstein Air Base, Germany, with its staff shared with U.S. Air Forces in Europe;
- U.S. Marine Corps Forces Africa (MARFORAF), located in Stuttgart, Germany, with its staff shared with U.S. Marine Corps Forces Europe;
- Combined Joint Task Force–Horn of Africa (CJTF–HOA), headquartered at Camp Lemonier, Djibouti; and

- U.S. Special Operations Command (SOCAFRI-CA), co-located with AFRICOM in Stuttgart, Germany.

Notably, CJTF-HOA serves as one of the most critical subordinate commands, both for AFRICOM and for U.S. military operations in Africa, because it is physically present in Africa. CJTF-HOA consists of approximately 2,000 military personnel from the U.S. and allied countries at its headquarters in Djibouti. Its assigned area of interest includes all of East Africa and the Horn of Africa, as well as operations in Mauritius, Comoros, Liberia, and Rwanda; its efforts are aimed at improving African countries' capacity to sustain a stable environment, including effective governance systems that provide a degree of economic and social advancement to their citizens.¹⁷ Recent missions include the East Africa Response Force (EARF) that was deployed to Juba, South Sudan, for three months to secure the U.S. embassy after conflict broke out between government and rebel forces in December 2013.

Despite the creation of AFRICOM and the diverse set of tools and programs intended to support African-led solutions to African problems, serious challenges remain. U.S. military efforts in the region face a shortage of key capabilities, including persistent wide-area intelligence, surveillance, and reconnaissance (ISR),¹⁸ that result in a severely limited understanding of what is happening on the ground in such areas as Northern Nigeria, deep in Central Africa in the Democratic Republic of Congo, or on the open Indian Ocean well beyond the Seychelles.¹⁹

The relatively small number of AFRICOM forces and engagement opportunities across the extraordinary expanse of Africa means that AFRICOM has to rely on platforms instead of people to collect intelligence and develop and maintain situational awareness of evolving security conditions. Consequently, the fewer high-endurance ISR platforms there are available to AFRICOM, the less awareness it has in high-interest areas of Africa.

While the U.S. has not involved itself with "boots on the ground" in many of Africa's civil wars, the U.S. supports many international response efforts in places like Mali and the Central African Republic indirectly, usually with airlift, reconnaissance, and refueling support. AFRICOM continues to hold large exercises with African partner nations, including the annual "Flintlock" exercise. Flintlock has

been conducted each year since 2005 and brings together about 6,000 African troops, 300 U.S. trainers, and another 200 Western partners. The 2013 exercise was conducted in Mauritania, and the exercise in 2014 was held in Niger.²⁰ And the U.S. military provided logistical, construction, and medical support in the Ebola outbreak in West Africa that began in 2014

The Arc of Instability in Africa

Africa is a global center of emerging threats. The dangerous mix of religious extremism, ethnic conflicts, authoritarian regimes, ungoverned space, and arms proliferation is driving modern-day conflict in the region. Furthermore, historical divisions manifest themselves to the benefit of global Islamist terrorists. Local grievances (whether perceived or real) that were previously believed to be locally contained conflicts in places such as northern Mali or northern Nigeria have been co-opted and exacerbated by terrorist groups and affiliates linked to al-Qaeda.

Terrorists threaten not only U.S. partners in Africa, but U.S. citizens and assets, as evidenced by the September 11, 2012, attack on the U.S. consulate in Benghazi. Al-Qaeda has a history of attacking U.S. interests in Africa, including the 1998 embassy bombings in Nairobi, Kenya, and Dar Es Salaam, Tanzania, where more than 230 people were killed, including 12 Americans.

For global terrorists, much of Africa is ripe for the picking. For example, poor governance, untrained and inexperienced militaries, and a disgruntled and growing youth population provide fertile ground for a group like al-Qaeda in the Islamic Maghreb (AQIM). Although such organizations have been frustrated in their operations as a result of the U.N.-backed French intervention in Mali (for which strategic airlift and refueling were provided by the U.S. in coordination with the United Kingdom, Canada, and Sweden), the threat from Islamist terrorists remains real and credible, particularly within the zone known as the "arc of instability" in Africa.

This arc extends from the coast of West Africa, across the Sahelian zone, along the northern reaches of the continent, and down through East Africa to include Ethiopia and Somalia. As a result of cross-border raids and kidnappings, Islamist terrorism is bleeding into Cameroon. The metamorphosis of the conflict in the Central African Republic for control of state resources and a vast

illicit economy²¹ into a conflict that is defined primarily in religious terms highlights the extent to which religious extremism and ethnic conflicts are mixing to create an even more dangerous threat to regional stability.

Given the proximity of the arc to NATO allies and the heavily trafficked waters of the Mediterranean, Red Sea, and Gulf of Aden, the region should continue to be monitored closely. Libya's rapid descent into chaos is a special cause for concern given the country's potential to become another global launching pad for terrorism akin to Yemen and Pakistan.

Of equal concern to the United States are countries that are contributing foreign fighters to the conflict in Syria, such as Libya and Tunisia, as well as countries that are serving as destination points for foreign fighters as seen in Somalia.²² Somalia is a notorious destination for American foreign fighters intent on joining the al-Qaeda-linked group al-Shabaab.²³ Reports also indicate that the Nigerian-based terrorist group Boko Haram trained alongside AQIM and the Movement for Oneness and Jihad in West Africa (MUJAO).²⁴ Such groups provide ample battle experience to committed fighters that either return home to the United States or move along to other fronts for global terrorism, thus posing significant threats to the United States at home and to its interests abroad.

Maritime Security

Africa has become a hotbed of maritime piracy and armed robbery at sea. Despite the gains made in recent years, piracy in the Gulf of Guinea has begun to draw considerable attention because it is heavily oriented around the oil sector. The theft of oil from the oil distribution infrastructure (the pipelines and storage facilities that connect drilling rigs with collection and refinery facilities), an activity known as "oil bunkering," is widespread and often occurs within the territorial waters of Nigeria. While each regional situation varies significantly from the other, both of these activities are harmful to global commerce and freedom of the seas.

The expansion of maritime piracy in Africa is closely connected to poor governance and lackluster law enforcement on land—problems that are enabled by and in turn worsen the region's widespread corruption and entrenched criminal and illicit networks. West African criminal networks are partic-

ularly well-organized and intelligence-driven and purportedly include high-powered political, business, and military participants.²⁵

The expansion of piracy in West Africa is linked not only to the expansion of the region's illicit oil market, but also to the increase in international shipping to and through the region, which has led in turn to a "backlog" of ships waiting either to load or to unload.²⁶ Growing numbers of ships waiting in territorial waters without adequate protection are vulnerable to corrupt law enforcement authorities who tip off criminal gangs.

The disruption of maritime transport and access to markets can have a direct impact not only on vital economic activity in the immediate region, but in distant markets as well. Piracy has a negative impact on economic investment in affected regions, disrupts energy flows, slows global trade, damages critical infrastructure, and hinders the protection of marine resources. Given that many of the countries in West Africa are economically dependent on energy revenues, the growing scope and effectiveness of maritime piracy directly affect overall economic security in the region and the main consumers of sub-Saharan African crude: Europe, China, and various U.S. partners in the region.

Arms Trafficking and the Illicit Economy

Several other illegal activities such as arms trafficking, drug trafficking, wildlife trafficking, and human trafficking also serve as cancers across the region, undermining governance and disrupting economic growth. Illicit trafficking networks, particularly in West Africa, Northwest Africa, and the Sahel, are funding criminal gangs and terrorists alike.

The region serves as a conduit for the transnational drug trade. Drugs are produced in Latin America, shipped to West Africa, trafficked through West and Northwest Africa, and consumed in Europe. According to the U.N. Office on Drugs and Crime (UNODC), "It is estimated that at least 50 tons of cocaine transit through West Africa annually, heading north to European cities, where they are worth almost \$2 billion...."²⁷ East Africa is also becoming an increasingly key transit route for heroin that is being trafficked to Europe from Asia.

Organized crime and the income generated from illicit activities help to fund extremist groups like Boko Haram in Nigeria and AQIM in North Africa. In April 2014, Boko Haram kidnapped nearly

300 girls and reportedly sold a number of the victims as slaves, exploiting the region's porous and unpatrolled borders. The region's terrorist heavyweights—Boko Haram, Ansar Dine, AQIM and the MUJAO—all have links to lucrative illicit activities including drugs and human trafficking.²⁸

Al-Shabaab in Somalia also engages in the illegal charcoal trade,²⁹ estimated to generate somewhere between an estimated \$38 million and \$56 million per year for the terrorist group.³⁰ The black-market charcoal trade thrives on Somalia's instability and feeds a vicious cycle that both deprives Somalia's legitimate government of revenues and funds terrorism.

Additionally, wildlife is among the five most valuable illicit commodities, with poaching generating "an estimated value of \$10 billion a year..."³¹ The illicit traffic in ivory finances al-Shabaab³² and supports other non-state actors such as Ugandan warlord Joseph Kony's Lord's Resistance Army (LRA),³³ which operates in Uganda, South Sudan, the Democratic Republic of Congo, and the Central African Republic. Sudan's Janjaweed militia also derives funding for its destabilizing activities in Darfur through illicit ivory sales.³⁴

In addition to the revenue generated by the traffic in these various commodities and the logistical network that spans the entire continent of Africa, arms trafficking and sales make it possible for criminal gangs, militias, and terrorist groups to prolong conflicts that destabilize entire regions. For example, after the fall of Libya's Muammar Qadhafi, a significant number of armory storage sites were looted, and their contents subsequently proliferated throughout the region. AQIM acquired anti-aircraft and anti-tank missiles and transferred arms to other groups in the region including Boko Haram and Ansar Dine. Arms proliferation, a strengthened AQIM, and the return of Tuareg mercenary fighters from Libya in 2011 led to the current conflict in Mali.

Arms trafficking in the Sahel and trans-Sahara region remains largely unmonitored by responsible governments and credible law enforcement entities due to a severe lack of ISR capabilities. Complicating matters is the fact that not all illicit activity occurs above ground. In Nigeria, for instance, Boko Haram uses a series of underground tunnels to traffic in weapons, drugs, and other commodities.³⁵

The growth of illicit economies in Africa and their expansion across borders and entire regions under-

mine governance and stability in Africa. Transnational criminal gangs, local violent non-state actors, and terrorists all benefit financially and materially from such illicit economies—wealth that inevitably corrupts local governments and, in particular, law enforcement. This corruption in turn fuels a distrust of government, creating a spiral of additional corruption, abuse of power, and worsened popular grievances.

Maintaining Stability and Curbing Adversarial Influence

The Arab Spring created a new dynamic in North Africa that has affected the stability and long-term future of many of the region's states: Egypt, Tunisia, and Libya among others. Many of the region's entrenched authoritarian regimes, fearing for their own survival, ruthlessly cracked down still further on their populations.

Most of these repressive governments remain under U.S. or even U.N. arms embargos, but many, such as Zimbabwe, Eritrea, and Sudan, look to such foreign partners as China, Russia, and Iran for financial and military support. While China may be pursuing economic interests through investment and resource extraction in Africa, it has risen to be the number one arms supplier to Africa, cornering 25 percent of the market.³⁶ China also supports autocratic regimes at the U.N. Security Council, blocking sanctions against Zimbabwe in 2008 and continuing to defend Sudan despite the growing spillover of violence from that country into its neighbors.

Ironically, while China's weapons sales to odious regimes enable and sustain repression and instability, the PRC also supports regional security efforts and, to some extent, is building credibility with African governments.³⁷ Notably, China committed 395 troops to the U.N. Peacekeeping operation (PKO) in Mali in June 2013. Since 2003, China has been active in PKOs in Africa, providing military observers or functional units and using the operations to gain power with local leaders and populations—and thereby gaining access to natural resources.³⁸

Congruent with U.S. security interests, China continues to engage on cooperative security initiatives, including counter-piracy efforts in the Gulf of Guinea (bilaterally with Nigeria); the Horn of Africa (international counter-piracy patrols); and the Indian Ocean (bilaterally with Tanzania and South Africa). While China's involvement does contribute

to the larger good of reducing piracy, participation in these partnerships and training opportunities ultimately provides the People's Liberation Army Navy with "a platform to enhance its expeditionary capacity" in a region of significant interest to China.³⁹

"African Solutions to African Problems"

Many of the challenges in Africa have global reach, and while they will not directly threaten the territorial integrity of the U.S. homeland, result in a major regional war, or result in the loss of freedom of movement in or access to the commons, the U.S. still has a vested interest in countering threats on the African continent and working to improve regional stability. "African solutions for African problems," a mantra repeated regularly by U.S. officials since AFRICOM was established in 2008, remains far from being a reality.

Africa's problems remain pervasive and continue to increase in virulence. Terrorism in Africa affects not only U.S. interests and citizens in Africa, but also the U.S. itself. Umar Farouk Abdulmutallab, known to many as the "Underwear Bomber," was born and raised in Lagos, Nigeria. If America does not take Africa seriously both as a security threat and as an opportunity to be seized, individuals like Abdulmutallab will continue to represent a serious threat to the U.S.

Absent a serious U.S. investment in time, attention, and resources, governments such as China and Russia will continue to build influence with Africa's authoritarian leaders—thugs who increase rather than eliminate grievances. Such oppressive regimes drive more individuals into the arms of extremists and illicit economic opportunists, ultimately downgrading the security environment of the entire continent.

Endnotes:

1. U.S. Energy Information Administration, "How Dependent Are We on Foreign Oil?" *Energy in Brief*, last updated May 10, 2013, http://www.eia.gov/energy_in_brief/article/foreign_oil_dependence.cfm (accessed September 10, 2014).
2. U.S. Department of Transportation, Research and Innovative Technology Administration, Bureau of Transportation Statistics, "Border Crossing/Entry Data: Query Detailed Statistics," December 2013, http://transborder.bts.gov/programs/international/transborder/TBDR_BC/TBDR_BCQ.html (accessed September 9, 2014).
3. Brianna Lee, "Mexico's Drug War," Council on Foreign Relations *Backgrounders*, updated March 5, 2014, <http://www.cfr.org/mexico/mexicos-drug-war/p13689> (accessed September 9, 2014).
4. World Bank, "Data: Honduras," <http://data.worldbank.org/country/honduras> (accessed September 17, 2014); World Bank, "Data: Nicaragua," <http://data.worldbank.org/country/nicaragua> (accessed September 17, 2014).
5. Clare Ribando Seelke and Kristin Finklea, "U.S.-Mexican Security Cooperation: The Mérida Initiative and Beyond," Congressional Research Service *Report for Congress*, April 8, 2014, <http://www.fas.org/sgp/crs/row/R41349.pdf> (accessed July 19, 2014).
6. Kelly, statement before the House Committee on Armed Services.
7. RIA Novosti, "Russia to Fulfill Arms Contracts with Venezuela by Yearend," April 9, 2013, http://en.ria.ru/military_news/20130410/180546405/Russia-to-Fulfill-Arms-Contracts-With-Venezuela-by-Yearend.html (accessed May 25, 2014).
8. Stratfor, "Venezuela, Russia: Noteworthy New Armor for South America," October 16, 2008; GlobalSecurity.org, "9K338 9M342 Iglá-S / SA-24 Grinch," November 7, 2011, <http://www.globalsecurity.org/military/world/russia/9k338.htm> (accessed May 25, 2014).
9. Ministry of National Defense of the People's Republic of China, "Chinese Naval Taskforce Leaves Argentina for China," November 5, 2013, http://eng.chinamil.com.cn/news-channels/photo-reports/2013-11/05/content_5632704.htm (accessed May 30, 2014).
10. Kelly, statement before the House Committee on Armed Services.
11. Press release, "Treasury Targets Venezuelan Government Official Supporting the FARC," U.S. Department of the Treasury, September 12, 2008, <http://www.treasury.gov/press-center/press-releases/Pages/hp1132.aspx> (accessed May 27, 2014).
12. Press release, "Treasury Targets Hizballah in Venezuela," U.S. Department of the Treasury, June 18, 2008, <http://www.treasury.gov/press-center/press-releases/pages/hp1036.aspx> (accessed May 27, 2014).
13. The African Union is made up of 53 member states that are generally recognized. Its membership roster also includes the Polisario Front's "Sahrawi Arab Democratic Republic," which is neither admitted as a state by the United Nations nor recognized as such by the United States or any other permanent member of the Security Council.
14. US AFRICOM Public Affairs, "Factsheet: United States Africa Command," United States Africa Command, May 24, 2012, <http://www.africom.mil/Newsroom/article/6107/fact-sheet-united-states-africa-command> (accessed August 12, 2014).
15. Lauren Ploch, "Africa Command: U.S. Strategic Interests and the Role of the U.S. Military in Africa," Congressional Research Service *Report for Congress*, July 22, 2011, p. 6, <http://www.fas.org/sgp/crs/natsec/RL34003.pdf> (accessed October 23, 2014).
16. Eric Schmitt, "U.S. Army Hones Antiterror Strategy for Africa, in Kansas," *The New York Times*, October 18, 2013, <http://www.nytimes.com/2013/10/19/world/africa/us-prepares-to-train-african-forces-to-fight-terror.html?pagewanted=all&r=0> (accessed August 10, 2014).
17. United States Africa Command, "Combined Joint Task Force—Horn of Africa," <http://www.africom.mil/about-the-command/subordinate-commands/combined-joint-task-force-horn-of-africa> (accessed June 13, 2014).
18. Persistent wide-area ISR is obtained through the use of space or aerial platforms capable of remaining over a target area of interest for an extended period of time and acquiring information at high levels of detail or resolution. See Daniel Gouré, "Wide Area Persistent Surveillance Revolutionizes Tactical ISR," Lexington Institute Early Warning Blog, November 28, 2012, <http://www.lexingtoninstitute.org/wide-area-persistent-surveillance-revolutionizes-tactical-isr/> (accessed September 8, 2014).
19. International Institute for Strategic Studies, *The Military Balance 2014* (London: Routledge, 2014), pp. 412-413.
20. Eric Schmitt, "U.S. Takes Training Role in Africa as Threats Grow and Budgets Shrink," *The New York Times*, March 5, 2014, <http://www.nytimes.com/2014/03/05/world/africa/us-takes-training-role-in-africa-as-threats-grow-and-budgets-shrink.html> (accessed July 31, 2014).
21. International Crisis Group, "The Central African Crisis: From Predation to Stabilization," *Africa Report* No. 219, June 17, 2014, <http://www.crisisgroup.org/-/media/Files/africa/central-africa/central-african-republic/219-la-crise-centrafricaine-de-la-predation-a-la-stabilisation-english.pdf> (accessed July 8, 2014).
22. James Jay Carafano, "Cutting Off ISIS Foreign Fighter Pipelines," *The National Interest*, July 1, 2014, <http://nationalinterest.org/feature/cutting-isis-foreign-fighter-pipelines-10783> (accessed July 3, 2014).
23. Raffaello Pantucci and A.R. Sayyid, "Foreign Fighters in Somalia and al-Shabaab's Internal Purge," Jamestown Foundation *Terrorism Monitor*, Vol. 11, Issue 22 (December 2, 2013), [http://www.jamestown.org/single/?no_cache=1&tx_ttnews\[tt_news\]=41705#.U7xlt7G4Ng](http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=41705#.U7xlt7G4Ng) (accessed September 17, 2014).

24. Samuel L. Aronson, "AQIM's Threat to Western Interests in the Sahel," Combating Terrorism Center at West Point, *CTC Sentinel*, Vol. 7, Issue 4 (April 2014), pp. 6–9, <https://www.ctc.usma.edu/wp-content/uploads/2014/04/CTCSentinel-Vol7Iss4.pdf> (accessed July 3, 2014).
25. James Bridger, "Oil Soaked Pirates in Gulf of Guinea," *The Maritime Executive*, March 15, 2014, <http://www.maritime-executive.com/article/Oil-Soaked-Pirates-in-Gulf-of-Guinea-2014-03-15> (accessed September 17, 2014).
26. Ibid.
27. United Nations Office on Drugs and Crime, "West Africa Coast Initiative," <http://www.unodc.org/westandcentralafrica/en/west-africa-coast-initiative.html> (accessed August 10, 2014).
28. International Crisis Group, "Curbing Violence in Nigeria (II): The Boko Haram Insurgency," *Africa Report* No. 216, April 3, 2014, p. 24, <http://www.crisisgroup.org/-/media/Files/africa/west-africa/nigeria/216-curbing-violence-in-nigeria-ii-the-boko-haram-insurgency.pdf> (accessed July 29, 2014).
29. Charcoal is a critical commodity in the region, used for cooking and heating. Those in the illicit portion of this industry slash forests that comprise fragile ecosystems. See Mugumo Munene, "KDF Funds Al-Shabaab Through Illegal Charcoal Trade, Says New Probe Report" *Daily Nation*, July 26, 2014, <http://mobile.nation.co.ke/news/KDF-funds-Al-Shabaab-through-illegal-charcoal-trade/-/1950946/2399090/-/format/xhtml/-/1yw8xz/-/index.html> (accessed September 8, 2014).
30. United States Africa Command, Sabahi English, "Al-Shabaab Rakes in \$38-\$56 Million from Illegal Charcoal Trade, UN Report Says," June 25, 2014, http://sabahionline.com/en_GB/articles/hoa/articles/newsbriefs/2014/06/25/newsbrief-01 (accessed July 31, 2014).
31. Sasha Jespersen, "Illicit Wildlife Crime: Entrenched in Crime, Conflict, and Terror Nexus," Royal United Services Institute, July 23, 2014, <https://www.rusi.org/go.php?structureID=commentary&ref=C53CFEB48EA10A#.U-kxqGO4NgG> (accessed August 10, 2014).
32. Ibid.
33. Hilary Heuler "Report Finds LRA Weakened, Surviving on Farming, Ivory," *Voice of America*, February 20, 2014, <http://www.voanews.com/content/report-finds-lords-resistance-army-weakened-surviving-on-farming-and-ivory/1855687.html> (accessed August 10, 2014).
34. Jeffrey Gettleman, "Elephants Dying in Epic Frenzy as Ivory Fuels Wars and Profits," *The New York Times*, September 3, 2012, <http://www.nytimes.com/2012/09/04/world/africa/africas-elephants-are-being-slaughtered-in-poaching-frenzy.html?pagewanted=all> (accessed August 10, 2014).
35. Gbenga Akingbule and Yinka Ibukun, "Nigerian Army Finds Boko Haram Tunnels, Graves in Borno," *Bloomberg*, July 15, 2013, <http://www.bloomberg.com/news/2013-07-15/nigerian-army-finds-boko-haram-tunnels-graves-in-borno.html> (accessed July 30, 2014).
36. Larry Hanauer and Lyle J. Morris, *Chinese Engagement in Africa: Drivers, Reactions, and Implications for U. S. Policy*, RAND Corporation, 2014, p. 17, http://www.rand.org/content/dam/rand/pubs/research_reports/RR500/RR521/RAND_RR521.pdf (accessed August 11, 2014).
37. Colum Lynch, "China's Arms Exports Flooding Sub-Saharan Africa," *The Washington Post*, August 25, 2012, http://www.washingtonpost.com/world/national-security/chinas-arms-exports-flooding-sub-saharan-africa/2012/08/25/16267b68-e7f1-11e1-936a-b801f1abab19_story.html (accessed August 11, 2014).
38. For more information, see Kent Hughes Butts and Brent Bankus, "China's Pursuit of Africa's Natural Resources," U.S. Army War College, Center for Strategic Leadership, *Collins Center Study*, Vol. 1-09 (June 2009), http://www.csl.army.mil/usacsl/publications/CCS1_09_ChinasPursuitofAfricasNaturalResources.pdf (accessed November 6, 2014), and Nicolas Cook, "Sub-Saharan Africa," in Senate Report 110-46, *China's Foreign Policy and "Soft Power" in South America, Asia, and Africa*, A Study Prepared for the Committee on Foreign Relations, United States Senate, by the Congressional Research Service, Library of Congress, April 2008, http://www.fas.org/irp/congress/2008_rpt/crs-china.pdf (accessed August 25, 2014).
39. J. Peter Pham, "Pirates and Dragon Boats: Assessing the Chinese Navy's Recent East African Deployments," *The Journal of the Middle East and Africa*, Vol. 4, Issue 1 (April 2013), p. 87, <http://www.tandfonline.com/doi/abs/10.1080/21520844.2013.773415#preview> (accessed August 25, 2014).