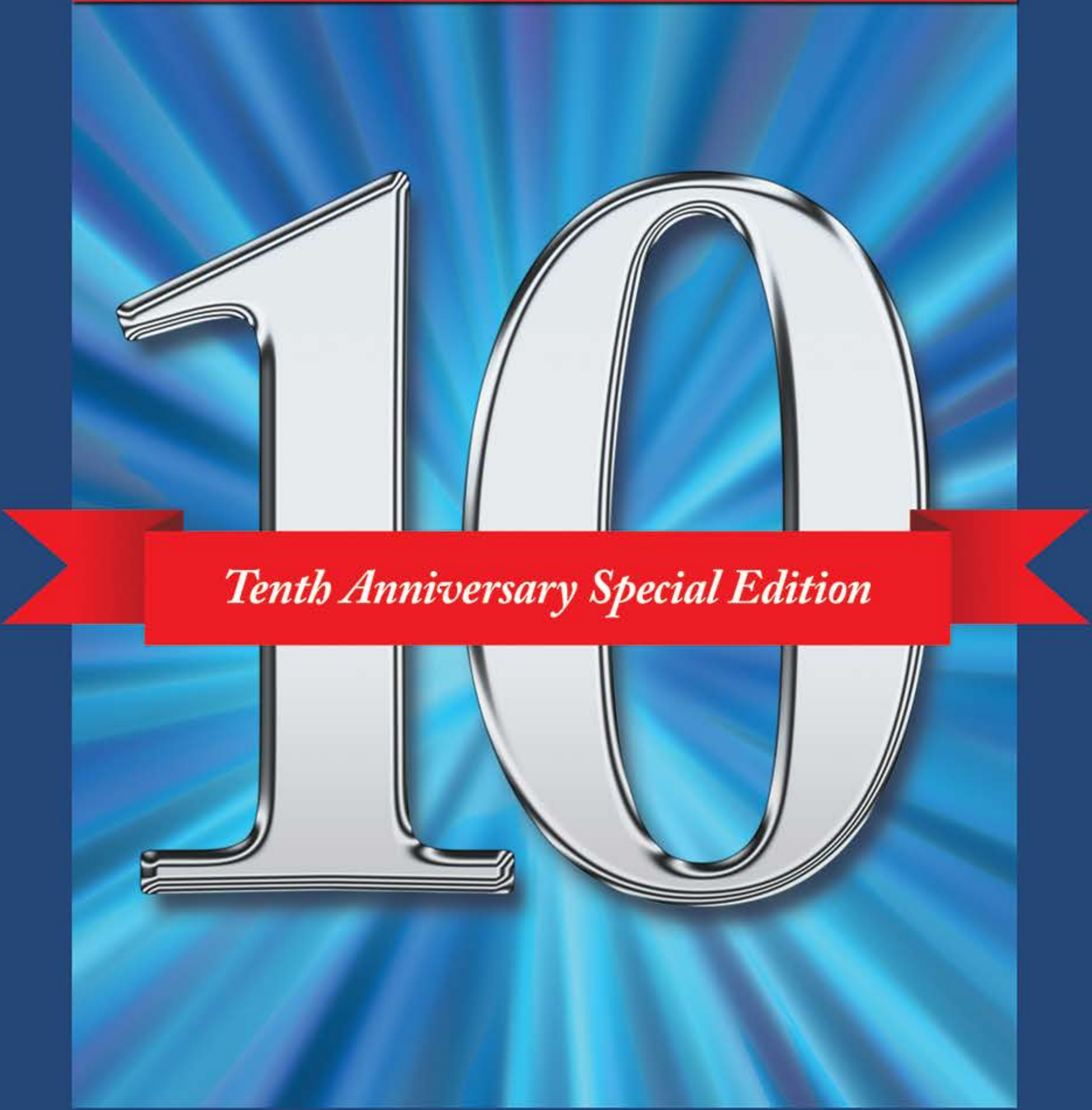
SSQ Strategic Studies Quarterly

2007–2017

Volume 11, No. 5

Celebrating a Decade of Scholarly Publishing



Tenth Anniversary Special Edition

SSQ

Strategic Studies Quarterly (*SSQ*) (ISSN 1936-1815) is published quarterly by Air University Press, Maxwell AFB, AL. Articles in *SSQ* may be reproduced free of charge. Notify editor and include a standard source credit line on each reprint.

The Best of

SSQ Strategic Studies Quarterly

2007–2017

AUP

Air University Press
Maxwell AFB, Alabama

This special edition is dedicated to all the authors published within the pages of Strategic Studies Quarterly *over the past 10 years.*

We would also like to recognize all our contributing editors who offered sound judgments toward maintaining the highest quality scholastic evaluations for Strategic Studies Quarterly.

Additionally, Strategic Studies Quarterly *wishes to thank our individual advisors for providing strategic-level thoughts and ideas that keep the journal relevant.*

Finally, to all former members of the Strategic Studies Quarterly *production team, thank you for building the foundation for success we continue to enjoy.*

Team SSQ

Strategic Studies Quarterly

An Air Force-Sponsored Strategic Forum on National and International Security

10th Anniversary 2007–2017 VOLUME 11, NO. 5

Foreword

Just over 10 years ago, I directed Air University to develop a strategic-level journal sponsored by the United States Air Force. My reasons for this decision were twofold. First, unlike the other services, the Air Force at the time was virtually absent from the strategic narrative on the national stage. As a result, Airmen's unique perspectives were relegated to only the *means* of strategy rather than policy development and the debate over the *ends* of US national security strategy. Second, it was the duty of all Airmen to engage the larger defense community by not only thinking and learning more about national security but also making contributions to the strategic discourse. In essence, the Air Force needed an intellectual recapitalization. My feature article in volume one of *Strategic Studies Quarterly* (*SSQ*) clearly explained these reasons—and the journal has satisfied both concerns.

From the beginning, *SSQ* established a strong foundation, and over the past 10 years the journal has become well respected and well read. It did so by focusing on the topics that matter most to US national security, such as cyber, nuclear, Asia–Pacific, technology, and space. The US Air Force plays a major role in each of these. *SSQ* engaged authors from a plethora of external organizations, including think tanks, research centers, and the most prestigious universities in the country. It also provided the venue for Air Force and other military authors to publish arguments that influence national security. The result is a holistic approach that captures external views and expertise for the internal Department of Defense audience while educating and informing an external audience, including the interagency, the US Congress, and senior policy makers. This special anniversary edition provides some of the best examples of the dual benefit *SSQ* provided.

The American public expects a lot from its Airmen as guardians of air, space, and cyber. With continued scholarly publishing from *SSQ*, those expectations will be met and assured. Over the past 10 years, *SSQ* has met my high expectations in honing the intellectual prowess of Airmen while influencing the national security debate. As long as war remains the ultimate security challenge, there will be a need for strategy and strategists. The continued success of *SSQ* is essential in ensuring the United States has its fighting and thinking done by warrior scholars rather than cowards and fools.

Gen T. Michael Moseley, USAF, Retired
18th USAF Chief of Staff

Preface

As the strategic journal of the US Air Force, *Strategic Studies Quarterly* (*SSQ*) has provided intellectual enrichment for national and international security professionals during the past 10 years. The journal is instrumental in meeting the goals of Air University (AU) and bolstering our reputation as the intellectual and leadership center of the Air Force. The scholarly works in *SSQ* connect AU to academia, government, think tanks, industry, national laboratories, and the other services. It provides meaningful, relevant evidence to senior leaders, policy makers, and the larger defense community. *SSQ* helps marshal brilliant and at times controversial ideas that engage strategic thinkers to solve our nation's most challenging strategic problems. Over the past 10 years, *SSQ* has published more than 250 scholarly works, including those devoted to grand strategy, cyber, technology, nuclear issues, space, civil-military relations, defense affordability, and the moral-social aspects of war. The entire collection of articles continues to inform, educate, and influence US national security.

As the journal celebrates its tenth anniversary, it is our pleasure to offer this limited-edition "Best of *Strategic Studies Quarterly*" volume as a sample of quality, scholarly research published by AU. The choice of articles in this anniversary edition results from considering each article's impact, aggregated downloads, follow-on use in academia, and overall interest at the national and international level.

Any journal is only as good as the profound ideas from the authors within it—ideas such as those represented here and hundreds more in the *SSQ* archive. On behalf of the entire Air University *SSQ* team, I would like to thank our authors and our subscriber audience. Your support, dedication, and feedback have made *Strategic Studies Quarterly* a trusted source of ideas, thinking, and solutions.

Lt Gen Steven L. Kwast, USAF
Commander and President, Air University

Spring 2010

Remembrance of Things Past

The Enduring Value of Nuclear Weapons

James Wood Forsyth Jr.
Col B. Chance Saltzman, USAF
Gary Schaub Jr.

> *So long as there is a finite chance of war, we have to be interested in outcomes; and although all outcomes would be bad, some would be very much worse than others.*
>
> —Bernard Brodie

Much has been written about nuclear weapons, but what has been learned? Once an essential element of American foreign and defense policy, these matters were neglected after the Cold War and all but forgotten after September 11th. As the Schlesinger Commission concluded, "Because nuclear weapons have been less prominent since the end of the Cold War and have not been used since World War II, their importance and unique role as a deterrent have been obscured though not diminished."[1] Recent incidents of mismanagement of the US nuclear weapons enterprise, the acquisition of atomic weapons by North Korea, Iran's

James Wood Forsyth Jr., PhD, currently serves as professor of national security studies, USAF School of Advanced Air and Space Studies, Maxwell AFB, Alabama. He earned his PhD at the Josef Korbel School of International Studies, University of Denver. He has written on great-power war, intervention, and nuclear issues.

Col B. Chance Saltzman is chief, Strategic Plans and Policy Division, Headquarters Air Force. His career includes ICBM and satellite operations and squadron command as chief of combat operations at the Joint Space Operations Center. He holds master's degrees in strategic management from the University of Montana and George Washington University and in strategic studies from the School of Advanced Air and Space Studies and was a recent National Security Fellow at Harvard's Kennedy School of Government.

Gary Schaub Jr., PhD, is an assistant professor in the Leadership and Strategy Department, Air War College, Maxwell AFB, Alabama. He previously taught at the School of Advanced Air and Space Studies, the University of Pittsburgh, and Chatham College. Dr. Schaub has published in the journals *International Studies Review*, *Political Psychology*, and *Refuge* and has chapters in books published by Oxford University Press and St. Martin's Press. His current research addresses theories of coercion, decision making, and civil-military relations.

apparent quest for such weapons, the expiration of the Strategic Arms Reduction Treaty (START) and negotiation of its replacement with Russia, and the decision to engage in a nuclear posture review have brought the attention of policy makers to the important question of the role that nuclear forces should play in American strategy.

This is not a new question, but it requires a renewed evaluation. Bernard Brodie pondered it long ago, and his work birthed a rich literature that informed and clarified the round of nuclear debates that resulted in America's first comprehensive nuclear policy—massive retaliation.[2] Today, however, policy makers seem befuddled by nuclear weapons. After 60 years of living with The Bomb, they seem to have forgotten its value. Nuclear weapons produce strategic effects. Their presence compels statesmen to behave cautiously in the face of grave danger. This cautiousness produces restraint, which shores up international stability. In short, nuclear weapons deter.

In this article we first address the concept of deterrence, its requirements, and alternative strategies. We then discuss the effects of nuclear deterrence in international political relations and the capabilities—both nuclear and conventional—required to produce these effects. Finally, we draw conclusions with regard to the appropriate size and composition of the US strategic nuclear arsenal, given our arguments.

What Is Deterrence?

From a theoretical standpoint, deterrence links a demand that an adversary refrain from undertaking a particular action to a threat to use force if it does not comply. Deterrence places the adversary in a situation in which it has a choice of complying with what has been demanded of it—inaction—or defying those demands and risking implementation of the deterrer's threatened sanction. What the adversary considers to generate expectations about the consequences of its alternatives has been the subject of wide and varied speculation.[3] These expectations are distilled into expected-value calculations whereby the costs and benefits of an outcome are discounted by the probability of its occurrence (i.e., [benefits – costs] * probability). Then the expected values of possible outcomes stemming from a single course of action are summed. In deterrence the adversary compares the expected value of complying with the deterrer's demand and refraining from action to defying that demand and acting anyway. For deterrence to be successful, the deterrer's threatened sanction must reduce the expected value of defiance so that it is less than the expected value of compliance. The deterrer can do that by threatening to reduce the benefits of defiance or increase its costs. The former would constitute a denial threat, while the latter would be a threat of punishment. And because the adversary will discount these threats by its assessment of the likelihood that the deterrer will implement them, the deterrer must convey these threats credibly.[4]

Deterrence is more than a theory. It is also a policy. States adopt deterrence policies for one reason—to fend off attack. The United States used deterrence to frame its approach to an apparently hostile Soviet Union and to make use of nuclear weapons by not using them. As the Schlesinger Commission put it, "Though our consistent goal has been to avoid actual weapons use, the nuclear deterrent is 'used' every day by assuring friends and allies, dissuading opponents from seeking peer capabilities to the United States, deterring attacks on the United States and its allies from potential adversaries, and providing the potential to defeat adversaries if deterrence fails."[5] Strategic nuclear weapons were used to operationalize strategies of denial and punishment. Denial strategies, generally termed *counterforce*, focused upon mitigating the ability of the adversary to use its military forces, especially nuclear forces, in the event of a conflict so as to reduce its chances of victory. Punishment strategies, generally termed *countervalue*, focused upon destroying the industrial capacity and urban centers of the adversary to impose terrible costs upon its society.[6] During the Cold War, US defense programs were designed and justified in terms of their ability to fulfill these missions.[7] Since 9/11, capabilities have been programmed in an *astrategic* manner, and many of the mundane considerations of deterrence have been cast aside, making the forging of a new deterrence policy problematic today.[8]

Deterrence theory and policy are based upon the presumption that the adversary to be deterred is rational. The *Deterrence Operations Joint Operating Concept*, which guides US deterrence doctrine and strategy, assumes that "[a]ctions to be deterred result from deliberate and intentional adversary decisions to act (i.e., not from automatic responses or unintended/accidental events). Decisions to act are based on actors' calculations regarding alternative courses of action and actors' perceptions of the values and probabilities of alternative outcomes associated with those courses of action."[9] It is often argued that deterrence is inherently flawed because no human being is perfectly rational—indeed, they often act irrationally.[10] But this is a red herring. As Robert Jervis has argued, "How rational do men have to be for deterrence theory to apply? Much less than total rationality is needed for the main lines of the theory to be valid."[11] Indeed, given that adversaries of any note lead large organizations—states—and had to pursue strategies to gain and retain power, it is difficult to argue that such persons are irrational or nonrational.[12] They may not be perfect, but they are sensible and react to the incentives of their strategic and domestic environments.[13] This holds also for terrorist groups such as al-Qaeda or Hamas, who utilize suicide terrorism to achieve strategic objectives.[14] It is on this basis that strategy and policy can be readily erected.

Political Effects of Nuclear Weapons

A key goal of any national security policy should be to enhance stability, where stability is defined as the absence of war or major crisis. Assuming the absence of a sudden change in the anarchic nature of the international system, any such policy should rely upon deterring potential aggressors at its base. Nuclear weapons enhance "general deterrence," a concept defined by Patrick Morgan. "*General deterrence* relates to opponents who maintain armed forces to regulate their relationship even though neither is anywhere near mounting an attack" (emphasis in original).[15] The goal of a general deterrent policy would be to ensure that incentives for aggression never outweigh the disincentives.

In theory, nuclear weapons are better than conventional forces in terms of enhancing general deterrence. This is so because deterrence succeeds when the costs—or, more appropriately, the risks of costs—exceed any probable gains that are to be had through armed aggression. War has been such a common international phenomenon throughout the centuries because some decision makers have concluded that the benefits of aggression would outweigh its costs.[16] Such a conclusion can be reached all the more easily when it is believed that victory on the battlefield can be attained quickly and decisively, and there are many historical examples from which decision makers can choose in order to bolster their confidence—from Bismarck's wars against Denmark, the Austrian Empire, and France to Iraq's conquest of Kuwait and its eviction by UN coalition forces.

Injecting the possible use of nuclear weapons by the defending state into the equation, however, can alter these calculations considerably. The possession of a sizable nuclear arsenal by a defender, as well as the means to deliver these weapons to the battlefield or the aggressor's homeland, makes the risks of aggression much greater and the potential costs much starker. This is because the possession of nuclear weapons tends to equalize the power of states, although not to the absolute degree that some would argue—attributes of national power such as geographic size, population, industrial capacity, GNP, and others still weigh heavily in any assessment of national power. Nonetheless, this equalizing tendency objectively manifests itself in two ways. On the battlefield, nuclear weapons can enhance the power of a smaller conventional force considerably. And in terms of absolute destructive power, only a finite amount of damage is necessary to destroy a modern state as a functioning entity.[17] Provided that two states are capable of developing the means to reliably deliver at least "enough" nuclear weapons to their adversary's homeland to "assure" its destruction, then, in a relative way, the two states can be considered equally powerful.

One could argue that the qualitative differences between nuclear and conventional forces also have certain psychological consequences that make the former a better buttress for general deterrence.[18] Given the destruction that nuclear weapons could wreak in a short temporal period, the potential costs of aggression against a nuclear-armed adversary would be "paid up front," as opposed to over a long period of mutual attrition, and are thus "clearer" to decision makers. And although some conventional munitions can approach the destructiveness of nuclear devices,[19] a certain symbolism has come to be attached to nuclear weapons that has historically enhanced their clarifying quality and induced caution in national decision makers.[20] This clarifying effect operates particularly to the advantage of states defending their vital interests. The threat of a nuclear-armed state to use its nuclear weapons in defense of vital interests, such as its survival or territorial integrity, is almost inherently credible.[21] Thus a secure nuclear arsenal has the effect of "sanctuarizing" the states that possess them. One could argue that nuclear weapons enhance general deterrence by virtually precluding acts of aggression against states that possess them,[22] and thereby greatly enhance stability.

But how large an arsenal is necessary for a state to effectively "sanctuarize" itself? While much of the more recent literature on the value of nuclear weapons as a pacifying force in international relations has implicitly assumed that any number of survivable weapons would be adequate for successful deterrence,[23] in effect arguing for existential deterrence,[24] the concept of proportional deterrence[25] would be a better theoretical guide.

Under a doctrine utilizing proportional deterrence, the defender would need to possess, at a minimum, enough survivable nuclear forces[26] to inflict damage on the aggressor roughly equivalent to the gains—in territory, industrial capacity, and so forth—that the aggressor could hope to achieve if it successfully conquered the defender.[27] This, of course, assumes a strategy of deterrence through punishment—that is, striking at the aggressor's population/industrial centers. Thus, for example, supposing the French, whose strategic doctrine rests upon proportional deterrence, desired to deter an attack by the Soviet Union during the Cold War; they would need enough survivable nuclear forces to inflict damage that was "the equivalent of France"—about 50 million people or striking, if not destroying, 100 to 150 major Soviet cities.[28] Hence, the answer to the question "how much is enough for proportional deterrence?" rests upon the rough value of the defender's territory, in a geopolitical sense.[29]

China understands this. Adopting a minimum deterrent strategy, China's nuclear numbers remain relatively small compared to the large numbers held by the United States and Russia. It is estimated that China has approximately 400 nuclear weapons, with about 200 operationally deployed. It probably possesses 30 intercontinental ballistic missiles (ICBM) capable of striking the continental United States and about 10 that are capable of striking Hawaii and Alaska. It also possesses about 100 intermediate-range weapons capable of striking US bases, friends, and allies in the Pacific region.[30] These weapons would be enough to destroy more than the value of Taiwan to the United States, the most likely stakes in any conflict between the two countries. In contrast, the United States possesses 450 ICBMs, each capable of carrying up to three warheads; 18 Trident submarines, each equipped with 24 submarine-launched ballistic missiles (SLBM) that carry as many as eight warheads each; and 100 or so nuclear bombers capable of carrying a variety of payloads to include air-launched cruise missiles (ALCM). It is assumed that Russia has a similar mix. Yet, despite these rather large nuclear inequities, China continues to modernize its conventional capabilities, extending its influence throughout the region. How does one explain this behavior?

China is confident that its small nuclear arsenal is sufficient to deter rivals. In international politics, deterrence restrains states from acting externally but affords opportunities to act internally—allowing them to pursue whatever weapons they choose. Shrewd states recognize this as well as the fact that large nuclear arsenals buy them little; as in other areas of competition, there comes a point of diminishing return, and with nuclear weapons that point comes quickly. There is little the United States or Russia can do militarily to dissuade China from pursuing its armament program. China realizes this, which explains why its nuclear appetite remains satisfied. Might China change? It might if demand were stimulated, which is why nuclear defenses are a bad idea, at least in Asia. In games of deterrence, defenses can be both stabilizing and destabilizing; deciphering when and how is one reason the United States turned its back on defenses, abandoning its civil defense program in favor of a strategy of mutually assured destruction.[31] Today, the United States and China have tacitly entered into what can only be described as a period of mutual retaliation; nothing official has been declared, but both sides know that the stakes are too high for either to make a run militarily at the other.

Nuclear weapons socialize statesmen to the dangers of adventurism, which in turn conditions them to set up formal and informal sets of rules that constrain their behavior. No statesmen want to be part of a system that constrains them, but that is the kind of system that results among nuclear powers. Each state is conditioned by the capabilities of the other, and the relationship that emerges is one that is tempered by caution despite the rhetoric of its leaders.

During the Cuban missile crisis, President Kennedy and Premier Khrushchev sought solutions short of war, despite their sharp political differences.[32] That the Soviets underestimated how the United States would react when confronted with the deployment of missiles off the coast of Florida is interesting but not as telling as how both leaders behaved when they realized what was at stake. Secretary of State Dean Rusk's comment that "We were eyeball to eyeball" is illustrative for two reasons. First, the two sides were staring into the face of grave danger. Second, there were no misperceptions. Both quickly recognized that the outcome of the crisis depended as much on the moves of one side as it did the other. War was the focal point; a threshold easily recognized, best not crossed, and worth avoiding.[33] This occurred despite the fact that the United States had overwhelming superiority in strategic and tactical nuclear forces and significant ability to blunt any Soviet retaliatory strike.[34] From that day forward, the superpowers understood that they could race to the brink but no further, lest they run the risk of nuclear war, a risk that neither side would take. Following the crisis, both sides took steps to reduce uncertainty and improve crisis stability.[35] What conclusions can be drawn? Small numbers of nuclear weapons produce dramatic effects. In times of crisis, they compel statesmen to act with restraint. In this sense, nuclear statesmen are risk averse, which also makes them vigilant.

Although it has been argued that such stable relations may have been unique to the bipolar relations between the United States and the Soviet Union,[36] they seem to apply elsewhere. Prior to Pakistan acquiring a nuclear capability, it fought three bloody wars with India. Today, in the presence of nuclear forces, the sharp differences that separate India and Pakistan are not sufficient to drive either side to war.[37] While the two sides actively engage in a game of tit-for-tat, nuclear weapons have softened both states and steadied their relationship by reducing the likelihood of interstate war. Far from perfect, relations between India and Pakistan can be summarized as tense but stable.[38]

Might this be the case within the Middle East? So it seems. Although the Arab states fought three wars to destroy Israel prior to widespread knowledge of its nuclear weapons capability, none have been fought since. Should Iran acquire a nuclear capability, the spread of nuclear weapons in the Middle East is all but certain. Although Israel's security will be challenged, given the potential for a mutual deterrent relationship to take hold thereby limiting its freedom of action, this constraint will also obtain throughout the region. Until it does, the challenge posed to Saudi Arabia in particular will be significant.[39] It is important to stress that the Iranian bomb will be a Shia bomb and the Sunni community will be hard pressed. Stabilizing the region until a Saudi weapons capability is ready will not be easy, and the options available to the United States are less than optimal. It could extend a security guarantee to the Saudis, but that would enlarge America's presence in the region, which would not sit well with extremists. Defensive systems could be deployed, but the downsides are similar to extending security guarantees. Islamic extremists would exploit their presence, holding them up as yet another example of the kingdom's dependency on the United States. A regional approach where the United States and its partners collectively provide for the defense of Saudi Arabia and the broader Sunni community might be effective, but the list of potential partners is short. Given all of this, the shrewdest thing to do might be nothing. As odd as it sounds, the United States might be better off by not acting and even allowing the Saudis to deploy a counterweapon should the Iranians decide to do so. In short, more might be better.[40]

Toward a Minimal US Nuclear Deterrent

But perhaps more is not better in arsenals that are already outsized. In the 1960s, the Kennedy administration recognized the need for a secure retaliatory capability and the desire of the services—particularly the Air Force—to purchase capabilities that far outstripped that objective.[41] It therefore sought to program capabilities that would be invulnerable to a counterforce strike and would be able to inflict unacceptable damage on the Soviet Union—but no more.[42] Looking back, Secretary of Defense McNamara had this to say: "Our goal was to ensure that they, with their theoretical capacity to reach such a first-strike capability, would not outdistance us. But they could not read our intentions with any greater accuracy than we could read theirs. The result has been that we have both built up our forces to a point that far exceeds a credible second-strike capability against the forces we each started with. In doing so neither of us has reached a first-strike capability."[43] In other words, both sides were, in fact, deterred fairly early on during the Cold War, even though that may or may not have been the intention, and the actual marginal utility of additional forces was quite small.

Therefore, as policy makers await the release of the administration's nuclear posture review, the question is not whether the United States can reduce its number of nuclear weapons to zero. Instead, the question is: What size force is needed for deterrence? Those numbers are comparatively small. Today the United States can adopt a minimum deterrence strategy and draw down its nuclear arsenal to a relatively small number of survivable, reliable weapons dispersed among missile silos, submarines, and airplanes.

Strategic air commander Gen Thomas Power said in 1965 that "the optimum deterrent must lie somewhere between the illusory minimum and the impossible maximum." To chart a course to the "illusory minimum," a pragmatic approach must be found that comforts policy makers that have come to rely on the war-deterring effects of nuclear weapons for six decades. Skeptical constituencies are more likely to embrace smaller numbers of nuclear weapons if the arsenal is reduced gradually. With this in mind, the International Commission on Nuclear Non-Proliferation and Disarmament proposed that the United States reduce to 500 nuclear weapons by 2025.[44] This represents a 90-percent reduction in the nuclear arsenal but offers more than enough deterrent capability while providing flexibility to pragmatically implement the force-structure cuts.

In fact, the United States could address military utility concerns with only 311 nuclear weapons in its nuclear force structure while maintaining a stable deterrence. These 311 weapons should include missiles that are integral to a stable deterrence because they cannot be moved, are easily detected, and can hold enemy forces at bay with pinpoint accuracy. One hundred single-warhead ICBMs, such as the Minuteman III systems currently in service, provide a dispersed, ready force that may be more politically palatable than more severe reductions. The sea leg of the triad can be constituted by 192 de-MIRVed Trident D-5 SLBMs on 12 *Ohio* class submarines, each capable of holding 24 missiles. This would allow two patrols of four boats each at any given time. These missiles are highly survivable as they can be moved, cannot be easily detected, and, with pinpoint accuracy, can hold hardened targets at risk if necessary. Furthermore, British and French nuclear capabilities remain available to assure European allies, if any perceive weakness based on this force reduction in the Atlantic. Finally, air-launched cruise missiles (ALCM) from 19 B-2s will continue to contribute standoff capability and flexibility to the triad. This is more than enough weapons to use aircraft for nuclear escalation control and political signaling while allowing all B-52Hs to convert and focus on a conventional role. As with the SLBM force, ALCMs can be shuttled from wing to wing for operational security or intermixed with conventional munitions—a solution first proposed by Brodie.[45]

In short, America's nuclear security can rest easily on a relatively small number of counterforce and countervalue weapons totaling just over 300. Moreover, it does not matter if Russia, who is America's biggest competitor in this arena, follows suit. The relative advantage the Russians might gain in theory does not exist in reality. Even if one were to assume the worst—a bolt from the blue that took out all of America's ICBMs—the Russians would leave their cities at risk and therefore remain deterred from undertaking the first move. Skeptics will rightfully attack this argument, so it is best to address a few concerns.

First, there will be those who insist that a minimum nuclear posture is of little value to the United States because it must maintain a nuclear arsenal large enough to cover all of its contingencies. In other words, while Pakistan has to contend with India, the United States has several potential contenders that, when combined, pose a large challenge. There is logic in that line of reasoning, but it ignores the vast conventional superiority of the United States. It is clear that in most circumstances conventional weapons will be preferred to nuclear ones and supplement the Global Strike mission. Indeed, Lieber and Press recognize this in their recent analysis of nuclear capabilities.[46] It is also undermined by the fact that the United States is deterred in most contingencies by China, which has a much smaller force structure. Presumably, if China can deter the United States, small numbers are effective. In fact, arguments for a large force have no meaning unless they are tied to an exclusive counterforce strategy directed against Russia, which, when all is said and done, does not appear to be necessary. During the Cold War, the superpowers raced to increase numbers in an attempt to prevent one side from acquiring either a counterforce capability or a symbolic numerical advantage. All the while, both sides lost sight of the fact that it is the political value of nuclear weapons that matters most, not their military utility. New nuclear states seem satisfied with small numbers. One wonders why. It either has something to do with the number of threats that they face or with their appreciation of the political value of nuclear weapons. A definitive answer is out of reach, which is why debate on this issue is so important.

The second criticism has to do with the future of the triad, which was the fulcrum of deterrence throughout the Cold War. Some might argue that the triad was effective and its redundancy and flexibility shored up international stability and helped keep the Cold War cold. It is, however, important to recall that the Soviets had no such operational concept. They relied heavily, almost exclusively, on missiles and still managed to deter the United States. If one accepts the basic idea that it is the political value of nuclear weapons that matters, the method of delivery is immaterial.

Lastly, there is concern over organizational competency and professional development. How small can a force become before it no longer resembles a force at all? That is a difficult question to answer. In some instances, a smaller force can be extremely competent, and increasing its size could lead to its undoing. One thinks of the Navy SEALs. What makes the SEAL program so effective is that it is highly selective, well funded, specialized, and small. Might the same hold true for nuclear warriors? That is a question for others to answer. Sizing of the nuclear force should be based primarily on the requirements for a stable, reliable, nuclear deterrent, with support issues like industrial base support, crew force management, and training only weighing in as secondary considerations.

Conclusions

Deterrence evolved throughout the Cold War, moving from massive retaliation to the intricate targeting schemes of countervailing strategies. All the while the superpowers came to understand what Brodie aptly described as "strategy in the missile age." Despite the harsh rhetoric and big words from both sides, they came to appreciate what these weapons meant and behaved accordingly. While both vied for attention and aggressively pursued international influence, neither side initiated or threatened to initiate a nuclear exchange. In short, nuclear learning occurred. Something similar is taking place in other parts of the world. China, India, Pakistan, North Korea, and, presumably, Iran understand that a small number of nuclear weapons is all that is needed for deterrence to take hold. Others will learn, too, which is why nuclear weapons ought to be the centerpiece of American strategy. That does not mean that they should be America's only concern, just the most important one.

Would the world be better off without nuclear weapons? Although it might be desirable to rid the world of nuclear weapons, it is not wise. "The web of social and political life is spun out of inclinations and incentives, deterrent threats and punishments." Take away the latter two and international society depends entirely on the former—a utopian thought impractical "this side of Eden."[47] Serious-minded men have wished it were not so. Gen Charles Horner, then head of US Space Command, explained in 1994, "I want to get rid of all [nuclear weapons]. I want to go to zero. I'll tell you why. . . . Think of the moral high-ground we secure by having none."[48] Two years later, addressing the National Press Club in December 1996, Gen Lee Butler, former commander of

Strategic Air Command, wondered if "it is possible to forge a global consensus on the propositions that nuclear weapons have no definitive role; that the broader consequences of their employment transcend any asserted military utility."[49] In both instances, what was overlooked is the role that force plays in international life. In politics, force is said to be the ultima ratio. In international politics, it is the first and constant one.[50] Force casts a long shadow and serves as an incentive to temper statesmen, moderate demands, and settle disputes. That the use of nuclear weapons is to be avoided does not render them useless. Quite the opposite—nuclear weapons might be the most politically useful weapons a state can possess, which helps explain why they are spreading.

Nuclear weapons allow international life to go on in spite of their inherent dangers because leaders of nuclear states realize that that they are constrained despite their goals, desires, or rhetoric. The international system, with its uneven distribution of material capabilities throughout the world, regulates what states can and cannot do. Nuclear weapons add to this by making the likelihood of war among nuclear powers less, not more, likely.[51] Shrewd statesmen recognize this as well as the realities of power in international life. The fact is some states will pursue nuclear weapons; others will not.

In the final analysis, security is the problem, weapons one solution. The spread of nuclear weapons is derived from the relative insecurity of some states in the world. So long as war remains a finite possibility, we have to be concerned with outcomes, and while some would be bad, others would be worse. In the age of minimum deterrence, the world will have to stand for a few more nuclear states; the majority of them will not pursue nuclear weapons. Pursuit of such weapons is contingent upon security. If states can achieve it without them, they have no need for them, which is another way of saying a nuclear-free world hinges on a more secure one. That we are not there yet is reason enough to work to make it so.

Notes

[1] *Report of the Secretary of Defense Task Force on DoD Nuclear Weapons Management, Phase I: The Air Force's Nuclear Mission* (Washington, DC: Office of the Secretary of Defense, September 2008), 1.

[2] Bernard Brodie, *The Absolute Weapon* (New York: Harcourt and Brace, 1946); *Strategy in the Missile Age* (Princeton: Princeton University Press, 1959); and *Escalation and the Nuclear*

Option (Princeton: Princeton University Press, 1966). Also see Lawrence Freedman, *The Evolution of Nuclear Strategy* (New York: Palgrave, 2003); William Fox, *The Superpowers: The United States, Britain and the Soviet Union* (New York: Harcourt and Brace, 1954); Alexander George and Richard Smoke, *Deterrence in American Foreign Policy: Theory and Practice* (New York: Columbia University Press, 1974); Morton Halperin, *Limited War in the Nuclear Age* (New York: John Wiley and Sons, 1963); Herman Kahn, *On Thermonuclear War* (Princeton: Princeton University Press, 1960); George Kennan, *Russia, the Atom and the West* (New York: Harper and Brothers, 1958); Henry Kissinger, *Nuclear Weapons and Foreign Policy* (New York: Harper, 1957); Robert Osgood, *Limited War: the Challenge to American Strategy* (Chicago: Chicago University Press, 1957); Thomas Schelling, *The Strategy of Conflict* (Cambridge: Harvard University Press, 1960); and Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966).

[3] See, for example, William W. Kaufmann, "The Requirements of Deterrence," in *Military Policy and National Security*, ed. William W. Kaufmann (Port Washington, NY: Kennikat Press, 1956); George and Smoke, *Deterrence in American Foreign Policy*; and Paul Huth and Bruce Russett, "What Makes Deterrence Work? Cases from 1900 to 1980," *World Politics* 36, no. 4 (July 1984).

[4] See Daryl G. Press, *Calculating Credibility: How Leaders Assess Military Threats* (Ithaca: Cornell University Press, 2005), for a discussion of the constituents of credibility.

[5] *Report of the Secretary of Defense Task Force*, 1.

[6] Freedman, *Evolution of Nuclear Strategy*, passim; Desmond Ball and Jeffrey Richelson, eds., *Strategic Nuclear Targeting* (Ithaca: Cornell University Press, 1986).

[7] Lawrence Freedman, "Does Deterrence Have a Future?" *Arms Control Today* 30, no. 8 (October 2000).

[8] Jonathan Schell, *The Seventh Decade: The Shape of Nuclear Danger* (New York: Metropolitan Books, 2007), 119.

[9] *Deterrence Operations Joint Operating Concept*, version 2.0 (Washington, DC: DoD, December 2006), 11.

[10] The classic statement of this critique is Stephen Maxwell, *Rationality in Deterrence*, Adelphi Paper 50 (London: International Institute for Strategic Studies, August 1968).

[11] Robert Jervis, "Deterrence Theory Revisited," *World Politics* 31, no. 2 (January 1979): 299.

[12] This is not a small point. In military circles, where one would expect to find some degree of emphasis placed upon rationality, the idea of the irrational actor has taken hold. This is especially true since 9/11. In discussing strategy with officers of all ranks, one is pressed with the retort "but you are assuming that the other guy is rational." No doubt suicide terrorists appear to be irrational at first, but even they are more than capable of reasoning. Waltz has made this point time and again. See Scott D. Sagan and Kenneth N. Waltz, *The Spread of Nuclear Weapons: A Debate* (New York: W. W. Norton and Co., 1995), 112–13, for an example.

[13] For an analysis of the motives of adversaries in deterrence situations, see Gary Schaub Jr., "When is Deterrence Necessary? Gauging Adversary Intent," *Strategic Studies Quarterly* 3, no. 4 (Winter 2009): 49–74.

[14] Robert A. Pape, *Dying to Win: The Strategic Logic of Suicide Terrorism* (New York: Random House, 2005).

[15] Patrick Morgan, *Deterrence*, 2nd ed. (Beverly Hills: Sage Publications, 1983), 30.

[16] John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983).

[17] A point first made by Brodie, "The Weapon," in *Absolute Weapon*, 25.

[18] See Schelling, *Arms and Influence*, 133.

[19] For example, fuel-air explosives or precision-guided conventional munitions capable of destroying hardened targets.

20. Nina Tannenwald, *The Nuclear Taboo: The United States and the Non-Use of Nuclear Weapons since 1945* (New York: Cambridge University Press, 2008).

21. Of course many have argued that if the aggressor also possesses nuclear weapons capable of striking the defender's territory with impunity, it would be irrational for the deterring state to carry out its retaliatory threat, particularly one directed against the adversary's population/industrial centers, as this would surely invite similar reprisals. In such a situation of mutual deterrence, it is argued, the deterrent threat would lack credibility. See, for example, Raymond Aron, *The Great Debate: Theories of Nuclear Strategy* (Garden City: Doubleday and Co., 1965), 128–30. This conundrum is generally solved, however, by claiming that the aggressor could not count upon the decision makers of the state it is attacking to be rational at a time of acute crisis; those decision makers could retaliate despite the probable consequences in a fit of anger or despair. As Glenn Snyder put it, "A thermonuclear attack based on an expectation that the victim would behave rationally would be a very dangerous gamble for the attacker." Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961), 64. There is a good deal of case study literature that suggests this is also the case in the event of a conventional attack. See Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981), for example.

22. This, of course, is direct deterrence. As discussed in many places, the protection of allies, forces overseas, or even noncontiguous possessions (such as Great Britain's crown colony, the Falkland Islands), are matters of extended deterrence, which is inherently more difficult. See Schelling, *Arms and Influence*, for an incisive discussion of this distinction.

23. For example, Stephen Van Evera discusses "states with developed nuclear arsenals [that] can annihilate each other even after absorbing an all-out attack" and provides France, Great Britain, and the Soviet Union as apparent examples of states with a mutually assured destruction capability. Stephen Van Evera, "Primed for Peace: Europe after the Cold War," *International Security* 15, no. 3 (Winter 1990/91): 13. But obviously, it would take a much larger nuclear capability to "assure" the destruction of Soviet society than that of France or Great Britain, given the much greater size, population, and resources of the Soviet Union. And while it was easily assumed that the Soviet Union possessed the capability of absorbing an "all-out" counterforce attack by either (or both) France or Great Britain, the opposite was not so easily assumed. As David Yost wrote, "The targeting objectives of France's 'enlarged anti-cities strategy' . . . call for France to be able to strike at least a hundred 'vital centers' in the USSR in a second strike. . . . France's ability to do so, even in a first strike, is minimal today," that is in 1984 when France possessed 132 deliverable strategic nuclear warheads. David Yost, *France's Deterrent Posture and Security in Europe, Part I: Capabilities and Doctrine*, Adelphi Paper 194 (London: International Institute for Strategic Studies, Winter 1984/85), 28. As for the British, they recognized their inability to assure the destruction of Soviet society and based the "independent" version of their strategic doctrine, as well as designing the performance characteristics of their Polaris force, around the "Chevaline concept" of destroying only one very important target in the Soviet Union: Moscow. Lawrence Freedman, "British Nuclear Targeting," in *Strategic Nuclear Targeting,* 112–23.

Mearsheimer makes similar omissions concerning the capability necessary to successfully bolster deterrence with nuclear weapons. Only in the context of the Ukraine does he get more specific: "128 nuclear warheads . . . should be more than enough to wreak vast destruction on Russia. Even if only 10 percent or 13 of those warheads reached Russian cities, they would leave Russia devastated." John J. Mearsheimer, "The Case for a Ukrainian Nuclear Deterrent," *Foreign Affairs* 72, no. 3 (Summer 1993): 62. Mearsheimer's 13 deliverable warheads as an adequate deterrent closely resemble McGeorge Bundy's 10-warhead "disaster beyond history" standard that is generally used as an example of a minimum deterrent capability. Michael Salman, Kevin J. Sullivan, and Stephen Van Evera, "Analysis or Propaganda? Measuring American Strategic Nuclear Capability, 1969–88," in *Nuclear Arguments: Understanding the Strategic Nuclear Arms and Arms Control Debates*, ed. Lynn Eden and Steven E. Miller (Ithaca: Cornell University Press, 1989), 210.

[24] The concept of existential deterrence is elaborated upon in McGeorge Bundy, *Danger and Survival: The Political History of the Nuclear Weapon* (New York: Random House, 1988); and Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca: Cornell University Press, 1990).

[25] The concept of proportional deterrence is elaborated upon in Pierre Gallois, *Balance of Terror: Strategy for the Missile Age* (Boston: Houghton Mifflin, 1961). Gallois' thinking is critiqued in Aron, *Great Debate*, 120–43.

[26] As well as robust, survivable command-and-control capabilities.

[27] Or, as Edward Kolodziej put it in terms of French strategic doctrine, "French military theorists . . . contended, however, that they could deter other states, even superpowers, because they possessed a destructive capability that would offset any gain envisioned by a potential aggressor. *The French force was alleged to be proportional in strategic capacity to France's political interests.* . . . France might be destroyed in the nuclear exchange, but the aggressor would presumably absorb more damage than could be reasonably offset by the anticipated benefits of his attack on France." Edward A. Kolodziej, *French International Policy under De Gaulle and Pompidou: The Politics of Grandeur* (Ithaca: Cornell University Press, 1974), 102 (emphasis added).

[28] Yost, *France's Deterrent Posture*, 15, 18.

[29] Of course the aggressor may value the defender's territory more or less given other factors, such as the symbolic value a victory over the defender would bestow, etc.

[30] See William J. Perry and James A. Schlesinger, chairmen, *America's Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States* (Washington, DC: US Institute of Peace, 2009), 10–11.

[31] A classic consideration of the problem is Donald G. Brennan, Leon W. Johnson, Jerome B. Weisner, and George S. McGovern, *Anti-Ballistic Missile: Yes or No?* (New York: Hill and Wang, 1968).

[32] Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, 2nd ed. (New York: Longman, 1999).

[33] For a discussion of strategy and focal points, see Thomas Schelling, *The Strategy of Conflict* (Cambridge: Harvard University Press, 1960).

[34] Allison and Zelikow, *Essence of Decision*, 92–95.

[35] Jack Mendelsohn, James P. Rubin, Matthew Bunn, Michèle Flournoy, and Jesse James, *Arms Control and National Security: An Introduction* (Washington, DC: Arms Control Association, 1989), 23–25; and John Lewis Gaddis, "The Long Peace Elements of Stability in the Postwar International System," *International Security* 10, no. 4 (Spring 1986).

[36] Lawrence Freedman, *Deterrence* (Cambridge: Polity, 2004), 75–83.

[37] The Kargil conflict is the case often cited as the exception to the rule. The conflict began in May 1999 and ended in July of that year. During this time, Indian army units attacked Pakistani forces, and Indian jets bombed their bases high in the Himalayan Mountains. Although Indian forces carefully stayed on their side of the line of control in Kashmir, Indian prime minister Atal Bihari Vajpayee informed the US government that he might have to order an invasion into Pakistan. Eventually, President Clinton got involved and assured both sides that he would take an interest in resolving the dispute. Although at least 1,000 Indian and Pakistani soldiers were killed during this crisis, we do not agree with those who think of Kargil as a war. If one unquestionably accepts Singer and Small's definition of war—see J. David Singer and Melvin Small, *The Wages of War 1816–1965: A Statistical Handbook* (New York: John Wiley and

Sons, 1972), which defines war as a conflict that involves one member of the interstate system on each side in which the battle-connected deaths totaled at least 1,000—the Kargil crisis was a war. However, if one thinks of war in terms of the ordinary sense of the word, its conduct more closely resembled a nasty skirmish.

[38] For interesting perspectives, see Sumat Ganguly, "Nuclear Stability in South Asia," *International Security* 33, no. 2 (Fall 2008); and S. Paul Kapur, "Ten Years of Nuclear Instability in Nuclear South Asia," ibid.

[39] It is assumed that Israel has deterrent options readily available, should it choose to unveil them. The Sunnis have no such option.

[40] See Kenneth Waltz and Scott Sagan, *The Spread of Nuclear Weapons: A Debate Renewed* (New York: W. W. Norton and Co., 2003).

[41] David Alan Rosenberg, "The Origins of Overkill: Nuclear Weapons and American Strategy, 1945–1960," *International Security* 7, no. 4 (Spring 1983).

[42] Alain Enthoven and K. Wayne Smith, *How Much Is Enough? Shaping the Defense Program, 1961–1969* (New York: Harper and Row, 1971).

[43] *The Dynamics of Nuclear Strategy*, Department of State Bulletin LVII, 9 October 1967.

[44] Gareth Evans and Yoriko Kawaguchi, *Eliminating Nuclear Threats: A Practical Guide for Global Policymakers—Report of the International Commission on Nuclear Non-Proliferation and Disarmament* (Canberra: Paragon, 2009).

[45] Brodie, "Weapon," 37.

[46] Keir A. Lieber and Daryl G. Press, "The Nukes We Need," *Foreign Affairs* 88, no. 6 (November/December 2009): 48.

[47] Kenneth Waltz, *Theory of International Politics* (Boston: McGraw Hill, 1979), 186.

[48] Gen Charles Horner (press briefing, 15 July 1994).

[49] Gen Lee Butler (speech, National Press Club, 4 December 1996).

[50] Waltz, *Theory of International Politics*, 113.

[51] This is largely a structural claim. See Waltz, *Theory of International Politics*, for the definitive account.

Winter 2011

Nuclear Lessons for Cyber Security?

Joseph S. Nye Jr.

Identifying "revolutions in military affairs" is arbitrary, but some inflection points in technological change are larger than others: for example, the gunpowder revolution in early modern Europe, the industrial revolution of the nineteenth century, the second industrial revolution of the early twentieth century, and the nuclear revolution in the middle of the last century.[1] In this century, we can add the information revolution that has produced today's extremely rapid growth of cyberspace. Earlier revolutions in information technology, such as Gutenberg's printing press, also had profound political effects, but the current revolution can be traced to Moore's law and the thousand-fold decrease in the costs of computing power that occurred in the last quarter of the twentieth century.

Political leaders and analysts are only beginning to come to terms with this transformative technology. Until now, the issue of cyber security has largely been the domain of computer experts and specialists. When the Internet was created 40 years ago, this small community was like a virtual village of people who knew each other, and they designed an open system with little attention to security. While the Internet is not new, the commercial Web is less than two decades old, and it has exploded from a few million users in the early 1990s to some two billion users today. This burgeoning interdependence has created great opportunities and great vulnerabilities, which strategists do not yet fully comprehend. As Gen Michael Hayden, former director of the CIA, says, "Rarely has something been so important and so talked about with less clarity and less apparent understanding [than cyber security]. . . . I have sat in *very* small group meetings in Washington . . . unable (along with

Joseph S. Nye Jr. is the University Distinguished Service Professor and former dean of Harvard's Kennedy School of Government. He received his bachelor's degree summa cum laude from Princeton, attended Oxford University as a Rhodes Scholar, and earned a PhD in political science from Harvard. He has served as assistant secretary of defense for international security affairs, chair of the National Intelligence Council, and a deputy undersecretary of state. He is best known for developing and expounding on the term *soft power* in a number of articles and books.

my colleagues) to decide on a course of action because we lacked a clear picture of the long-term legal and policy implications of *any* decision we might make."[2]

Governments learn slowly from knowledge, study, and experience, and learning occurs internationally when new knowledge gradually redefines the content of national interests and leads to new policies.[3] For example, the United States and the Soviet Union took decades to learn how to adapt and respond to the prior revolution in military affairs—nuclear technology after 1945. As we try to make sense of our halting responses to the current cyber revolution, are there any lessons we can learn from our responses to the prior technological transformation? In comparison to the nuclear revolution in military affairs, strategic studies of the cyber domain are chronologically equivalent to 1960 but conceptually more equivalent to 1950. Analysts are still not clear about the lessons of offense, defense, deterrence, escalation, norms, arms control, or how they fit together into a national strategy. After a short overview of the problem of cyber security in the next section, I will suggest several general lessons and then discuss a number of international lessons that can be learned from the nuclear experience. While the two technologies are vastly different, as I will argue below, there are nonetheless useful comparisons one can make of the ways in which governments learn to respond to technological revolutions.

Cyberspace in Perspective

Cyber is a prefix standing for computer and electromagnetic spectrum–related activities. The cyber domain includes the Internet of networked computers but also intranets, cellular technologies, fiber-optic cables, and space-based communications. Cyberspace has a physical infrastructure layer that follows the economic laws of rival resources and the political laws of sovereign jurisdiction and control. This aspect of the Internet is not a traditional "commons." It also has a virtual or informational layer with increasing economic returns to scale and political practices that make jurisdictional control difficult. Attacks from the informational realm, where costs are low, can be launched against the physical domain, where resources are scarce and expensive. Conversely, control of the physical layer can have both territorial and extraterritorial effects on the informational layer. Cyber power can produce preferred outcomes *within* cyberspace or in other domains *outside* cyberspace. By analogy, sea power refers to the use of resources in the oceans domain to win naval battles on the oceans, but it also includes the ability to use the oceans to influence battles, commerce, and opinions on land. Likewise, the same analogy can be applied to airpower.

The cyber domain is a complex man-made environment. Unlike atoms, human adversaries are purposeful and intelligent. Mountains and oceans are hard to move, but portions of cyberspace can be turned on and off by throwing a switch. It is cheaper and quicker to move electrons across the globe than to move large ships long distances through the friction of salt water. The costs of developing multiple carrier task forces and submarine fleets create enormous barriers to entry and make it possible to speak of American naval dominance. In contrast, the barriers to entry in the cyber domain are so low that nonstate actors and small states can play significant roles at low cost.

The Future of Power describes diffusion of power away from governments as one of the great power shifts of this century.[4] Cyberspace is a perfect example of this broader trend. The largest powers are unlikely to be able to dominate this domain as much as they have others like sea, air, or space. While they have greater resources, they also have greater vulnerabilities, and at this stage in the development of the technology, offense dominates defense in cyberspace. The United States, Russia, Britain, France, and China have greater capacity than other state and nonstate actors, but it makes little sense to speak of dominance in cyberspace. If anything, dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by nonstate actors. Four decades ago, the Pentagon created the Internet, and today, by most accounts, the United States remains the leading country in both its military and societal use. At the same time, however, because of greater dependence on networked computers and communication, the United States is more vulnerable to attack than many other countries, and the cyber domain has become a major source of insecurity.[5]

The term *cyber attack* covers a wide variety of actions ranging from simple probes, to defacing websites, to denial of service, to espionage and destruction.[6] Similarly, the term *cyber war* is used very loosely for a wide range of behaviors. In this, it reflects dictionary definitions of war that range from armed conflict to any hostile contention (e.g., "war between the sexes" or "war on poverty"). At the other extreme, some use a very narrow definition of cyber war as a "bloodless war" among states that consists only of conflict in the virtual layer of cyberspace. But this avoids important issues of the interconnection of the physical and virtual layers of cyberspace discussed above. A more useful definition of cyber war is hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence.

In the physical world, governments have a near monopoly on large-scale use of force, the defender has an intimate knowledge of the terrain, and attacks end because of attrition or exhaustion. Both resources and mobility are costly. In the virtual world, actors are diverse, sometimes anonymous, physical distance is immaterial, and offense is often cheap. Because the Internet was designed for ease of use rather than security, the offense currently has the advantage over the defense. This might not remain the case in the long term as technology evolves, including efforts at "reengineering" some systems for greater security, but it remains the case at this stage. The larger party has limited ability to disarm or destroy the enemy, occupy territory, or effectively use counterforce strategies. Cyber war, although only incipient at this stage, is the most dramatic of the potential threats. Major states with elaborate technical and human resources could, in principle, create massive disruption as well as physical destruction through cyber attacks on military as well as civilian targets. Responses to cyber war include a form of interstate deterrence (though different from classical nuclear deterrence), offensive capabilities, and designs for network and infrastructure resilience if deterrence fails. At some point in the future, it may be possible to reinforce these steps with certain rudimentary norms, but the world is at an early stage in such a process.

If one treats hacktivism as mostly a disruptive nuisance at this stage, there remain four major categories of cyber threats to national security, each with a different time horizon and different (in principle) solutions: cyber war and economic espionage are largely associated with states, and cyber crime and cyber terrorism are mostly associated with nonstate actors. For the United States, at the present time, the highest costs come from espionage and crime, but over the next decade or so, war and terrorism may become greater threats than they are today. Moreover, as alliances and tactics evolve among different actors, the categories may increasingly overlap. In the view of ADM Mike McConnell, "Sooner or later, terror groups will achieve cyber-sophistication. It's like nuclear proliferation, only far easier."[7] We are only just beginning to see glimpses of cyber war—for instance, as an adjunct in some conventional attacks, in the denial-of-service attacks that accompanied the conventional war in Georgia in 2008, or the recent sabotage of Iranian centrifuges by the Stuxnet worm. Deputy Defense Secretary William Lynn has described the evolution of cyber attacks from exploitation, to disruption of networks, to destruction of physical facilities. He argues that while states have the greatest capabilities, nonstate actors are more likely to initiate a catastrophic attack.[8] A "cyber 9/11" may be more likely than the often mentioned "cyber Pearl Harbor."

Nuclear Lessons for Cyber Security?

Can the nuclear revolution in military affairs seven decades ago teach us anything about the current cyber transformation? At first glance, the answer seems to be no. The differences between the technologies are just too great. The National Research Council cites differences in the threshold for action and attribution—nuclear explosions are unambiguous, while cyber intrusions that plant logic bombs in the infrastructure may go unnoticed for long periods before being used and, even then, can be difficult to trace.[9] Even more dramatic is the sheer destructiveness of nuclear technology. Unlike nuclear, cyber does not pose an existential threat. As Martin Libicki points out, destruction or disconnection of cyber systems could return us to the economy of the 1990s—a huge loss of GDP—but a major nuclear war could return us to the Stone Age.[10] In that and other dimensions, comparisons of cyber with biological and chemical weaponry might be more apt.

Moreover, cyber destruction can be disaggregated, and small doses of destruction can be administered over time. While there are many degrees of nuclear destruction, all are above a dramatic threshold or firebreak. In addition, while there is an overlap of civilian and military nuclear technology, nuclear originated in war, and the differences in its use are clearer than in cyber where the Web has burgeoned in the civilian sector. For example, the "dot mil" domain name is only a small part of the Internet, and 90 percent of military telephone and Internet communications travel over civilian networks. Finally, because of the commercial predominance and low costs, the barriers to entry to cyber are much lower for nonstate actors. While nuclear terrorism is a serious concern, the barriers for nonstate actors gaining access to nuclear materials remain steep; renting a botnet to wreak destruction on the Internet is both easy and cheap.

It would be a mistake, however, to neglect the past, so long as we remember that metaphors and analogies are always imperfect.[11] In words often attributed to Mark Twain, "History never repeats itself, but sometimes it rhymes." There are some important nuclear-cyber strategic rhymes, such as the superiority of offense over defense, the potential use of weapons for both tactical and strategic purposes, the possibility of first- and second-use scenarios, the possibility of creating automated responses when time is short, the likelihood of unintended consequences and cascading effects when a technology is new and poorly understood, and the belief that new weapons are "equalizers" that allow smaller actors to compete directly but asymmetrically with a larger state.[12]

Even more important than these technical and political similarities is the learning experience as governments and private actors try to understand a transformative technology—and adopt strategies to cope with it. While government reports warning about computer and Internet vulnerability date back to 1991 and the Pentagon recently released a new strategy, few observers would argue that the country has developed an adequate national strategy for cyber security. It is worth examining the uneven and halting history of nuclear learning to alert us to some of the pitfalls and opportunities ahead in the cyber domain. Ernest May once described US defense policy and the development of nuclear strategy in the first half-decade following World War II as "chaotic."[13] He would likely apply the same term to the situation in cyberspace today.

Some General Lessons

Expect continuing technological change to complicate early efforts at strategy. At the beginning, both fissile materials and atomic bombs were assumed to be scarce, and it was considered wasteful to use atomic bombs against any but countervalue targets—that is, cities. Bernard Brodie and others concluded in the important 1946 book *The Absolute Weapon* that superiority in numbers would not guarantee strategic superiority, deterrence of war was the only rational military policy, and ensuring survival of the retaliatory arsenal was crucial.[14] These postulates of "finite" or "existential" deterrence persisted throughout the Cold War and serve as the basis for the nuclear strategies of countries such as France and China to this day. In the bipolar competition of the

Cold War, however, the strategy of finite deterrence was challenged by the development of the hydrogen bomb in the early 1950s. Destructive power was no longer scarce but now unlimited. While hydrogen bombs could lead to explosions counted in the tens of megatons, their real revolutionary effect was to permit miniaturization, which allowed multiple weapons to pack huge destructive power into the nose cones of another technological surprise—intercontinental ballistic missiles—which shortened response times to less than an hour. This burgeoning explosive power produced great concern about the vulnerability of limited arsenals, an enormous increase in the number of weapons, diminished prospects for active defenses, and the development of elaborate counterforce war-fighting strategies.

Both superpowers had to confront the "usability paradox." If the weapons could not be used, they could not deter. The United States and the USSR were locked in a positive-sum game that involved avoiding nuclear war, but simultaneously they were locked in a zero-sum game of political competition. In the game of political chicken, perceptions of credibility became crucial. Some prospect of usability had to be introduced into doctrine, and for decades strategists wrestled with issues of counterforce targeting, exploring strategic defense technology, and the issues of perception that disparities in large numbers might create for extended deterrence. Elaborate war-fighting schemes and escalation ladders were invented by a nuclear priesthood of experts who specialized in arcane and abstract formulas. In 1976, Paul Nitze and the Committee on the Present Danger expressed alarm about American weakness when the United States possessed tens of thousands of weapons, and in 1979, even Henry Kissinger predicted that because of American nuclear weakness, Soviet risk-taking "must exponentially increase."[15] In fact, the opposite proved to be the case. While politicians and strategists assailed the idea of mutual assured destruction as an immoral and dangerous strategy, MAD turned out to be a fact, not a policy. As McGeorge Bundy noted in his final work, when it came to the Cuban missile crisis, existential deterrence worked, and a few Soviet bombs created deterrence despite an overwhelming American superiority in numbers.[16]

Looking at today's cyber domain, interdependence and vulnerability are twin facts that are likely to persist, but we should expect further technological change to complicate early strategies. ARPANET was created in 1969, and the domain name system and the first viruses date back to 1983;

however, as noted above, the mass use and commercial development of cyberspace date only from the invention of the World Wide Web in 1989 and widely available browsers in the mid-1990s.[17] As one expert put it, "As recently as the mid-1990s, the Internet was still essentially a research tool and the plaything of a few."[18] In other words, the massive vulnerabilities that have created the security problems we face today are less than two decades old and are likely to increase. While some experts talk about reducing vulnerability by reengineering the Internet to make attribution of attack easier, this will take time. Even more important, it will not close all vectors of attack.

Early strategies focused on the network: improving code, computer hygiene, addressing issues of attribution, and maintaining air gaps for the most sensitive systems. These steps remain important components of a strategy, but they are far from sufficient. In some ways, the invention and explosion in the usage of the web is analogous to the hydrogen revolution in the nuclear era. By leading society and the economy to a vast dependence on networked communications, it created enormous vulnerabilities that could be exploited not only through the Internet but also through supply chains, devices to bridge air gaps, human agents, and manipulation of social networks.[19] With the development of mobility, cloud computing, and the importance of a limited number of large providers, the issues of vulnerability may change again. Given such technological volatility, a cyber security strategy will have to be multifaceted and capable of continual adaptation. It should increase the ratio of work that an attacker must do compared to that of a defender and include redundancy and resilience to allow graceful degradation of complex systems so that inevitable failures are not catastrophic.[20] Strategists need to be alert to the fact that today's solutions may not suffice tomorrow.

Strategy for a new technology will lack adequate empirical content. Since Nagasaki, no one has seen a nuclear weapon used in war. As Alain Enthoven, one of Robert McNamara's "whiz kids" of the early 1960s, retorted during a Pentagon argument about war plans, "General, I have fought just as many nuclear wars as you have."[21] With little empirical grounding, it was difficult to set limits or test strategic formulations. Elaborate constructs and prevailing political fashion led to expensive conclusions based on abstract formulas and relatively little evidence. Fred Kaplan described the environment thusly:

> The method of mathematical calculation, driven mainly from the theory of economics that they had all studied, gave the strategists of the new age a handle on the colossally destructive power of the weapons they found in their midst. But over the years the method became a catechism. . . . The precise calculations and the cool, comfortable vocabulary were coming all too commonly to be grasped not merely as tools of desperation but as genuine reflections of the nature of nuclear war.[22]

In the absence of empirical evidence, these nuclear theologians were able to spend vast resources on their hypothetical scenarios.

Cyber has the advantage that with widespread attacks by hackers, criminals, and spies, there is more cumulative evidence of a variety of attack mechanisms and of the strengths and weaknesses of various responses to such attacks. It helps that cyber destruction can be disaggregated in a way that nuclear cannot. But at the same time, no one has yet seen a cyber war, in the strict sense of the word, as defined above. Denial-of-service attacks in Estonia and Georgia and industrial sabotage such as Stuxnet in Iran give some inklings of the auxiliary use of cyber attacks, but they do not test the full set of actions and reactions in a cyber war between states. The US government has conducted a number of war games and simulations and is developing a cyber test range, but the problems of unintended consequences and cascading effects have not been experienced. The problems of escalation as well as the implications for the important doctrines of discrimination and proportionality under the law of armed conflict remain unknown.

New technologies raise new issues in civil-military relations. Different parts of complex institutions like governments learn different lessons at different paces, and new technologies set off competition among bureaucracies. At the beginning of the nuclear era, political leaders developed institutions to maintain civilian control over the new technology, creating an Atomic Energy Agency separate from the military as a means of ensuring civilian control. Congress established a Joint Atomic Energy Committee. But gaps still developed in the relationship between civilians and the military. Operational control of deployed nuclear weapons came under the Strategic Air Command, which had its own traditions, standard operating procedures, and a strong leader, Curtis LeMay. In 1957, LeMay told Robert Sprague, the deputy director of the civilian Gaither Committee that was investigating the vulnerability of American nuclear forces, that he was not too concerned because "if I see that the Russians are amassing their planes for an attack, I'm going to knock the s**t out of them before they take off the ground." Sprague was thunderstruck and replied, "But General LeMay, that is not national policy," to which LeMay replied, "I don't care. It's my policy. That's what I'm going to do."[23] In 1960, when President Eisenhower ordered the development of a single integrated operational plan (SIOP-62), SAC produced a plan for a massive strike with 2,164 megatons that targeted China as well as the Soviet Union because of the "Sino-Soviet Bloc."[24] The limited nuclear options that civilian strategists theorized about as part of a bargaining process would not have looked very limited from the point of view of the Soviet bargaining partner—not to mention China.

While Cyber Command is still new and has very different leadership from the old Strategic Air Command, cyber security does present some similar problems of relating civilian control to military operations. Time is even shorter. Rather than the 30 minutes of nuclear warning and possible launch under attack, today there would be 300 milliseconds between a computer detecting that it was about to be attacked by hostile malware and a preemptive response to disarm the attack. This requires not only advanced knowledge of malware being developed in potentially hostile systems but also an automated response. What happens to the human factor in the decision loop? Obviously, there is no time to go up the chain of command, much less convene a deputies' meeting at the White House. For active defense to be effective, authority will have to be delegated under carefully thought-out rules of engagement developed in advance. Moreover, there are important questions about when active defense shades into retaliation or offense. As the head of Cyber Command has testified, such legal authorities and rules still remain to be fully resolved.[25]

Civilian uses will complicate effective national security strategies. Nuclear energy was first harnessed for military purposes, but it was quickly seen as having important civilian uses as well. In the early days of the development of nuclear energy, it was claimed that electricity would become "too cheap to meter" and cars would be fueled for a year by an atomic pellet the size of a vitamin pill.[26] The engineers' optimism about their new technology was reinforced by a political desire to promote the civilian uses of nuclear energy. Fearful that antiwar and antinuclear movements would delegitimize nuclear weapons and thus reduce their deterrent value, the Eisenhower administration promoted an Atoms for Peace program that offered to assist in the promotion of nuclear energy worldwide. Other countries joined in. The net effect was to create a powerful domestic and transnational lobby for promotion of nuclear energy that helped provide India with the materials needed for its nuclear explosion in 1974 and justified the French sale of a reprocessing plant to Pakistan and a German sale of enrichment technology to Brazil in the mid-1970s.

The Atomic Energy Commission and the Joint Atomic Energy Committee had been created to assure civilian control of nuclear technology, but over time both institutions became examples of regulatory capture by powerful commercial interests—more interested in promotion than regulation and security. Late in the Ford administration, both institutions were disbanded. However, after the oil crisis of 1974, it became an article of faith that nuclear would be the energy of the future; that uranium would be scarce, and thus widespread use of plutonium and breeder reactors would be necessary. When the Carter administration, following the recommendations of the nongovernmental Ford-Mitre Report,[27] tried to slow the development of this plutonium economy in 1977, it ran into a buzz saw of reaction not only overseas but also from the nuclear industry and its congressional allies at home.

As mentioned earlier, the civilian sector plays an even larger role in the cyber domain, and this enormously complicates the problem of developing a national security strategy. The Internet has become a much more significant contributor to GDP than nuclear energy ever was. The private sector is more than a constraint on policy; it is at the heart of the activity that policy is designed to protect. Risk is inevitable, and redundancy and resilience after attack must be built into a strategy. Most of the Internet and its infrastructure belong to the private sector, and the government has only modest levers to use. Proposals to create a central agency in the executive branch and a joint committee on cyber security in Congress might be useful, but one should be alert to the dangers of regulatory capture and the development of a cyber "iron triangle" of executive branch, congressional, and industry partners.

From a security perspective, there is a misalignment of economic incentives in the cyber domain.[28] Firms have an incentive to provide for their own security up to a point, but competitive pricing of products limits that point. Moreover, firms have a financial incentive not to disclose intrusions that could undercut public confidence in their products and stock prices. A McAfee white paper notes, "The public (and very often the industry) understanding of this significant national security threat is largely minimal due to the very limited number of voluntary disclosures by victims of intrusion activity."[29] The result is a paucity of reliable data and an underinvestment in security from the national perspective. Moreover, laws designed to ensure competition restrict cooperation among private firms, and the difficulty of ascertaining liability in complex software limits the role of the insurance market. Public-private partnerships are limited by different perspectives and mistrust. As one participant at a recent cyber security conference concluded, something bad will have to happen before markets begin to reprice security.[30]

International Cooperation Lessons

Learning can lead to concurrence in beliefs without cooperation. Governments act in accordance with their national interests, but they can change how they define their interests, both through adjusting their behavior to changes in the structure of a situation as well as through transnational and international contacts and cooperation. In the nuclear domain, the initial learning led to concurrence of beliefs before it led to contacts and cooperation. The first effort at arms control, the Baruch Plan of 1946, was rejected out of hand by the Soviet Union as a ploy to preserve the American monopoly, and the early learning was unilateral on both sides.

As we have seen, much of what passed for nuclear knowledge in the early days was abstraction based on assumptions about rational actors, which made it difficult for new information to alter prior beliefs. Yet gradually, both sides became increasingly aware of the unprecedented destructive power of nuclear weapons through weapons tests and modeling, particularly after the invention of the hydrogen bomb. As Winston Churchill put it in 1955, "The atomic bomb, with all its terrors, did not carry us outside the scope of human control," but with the H-bomb, "the entire foundation of human affairs was revolutionized."[31] In his memorable phrase, "Safety will be the sturdy child of terror." On the other side of the Iron Curtain, Nikita Khrushchev recalled: "When I was appointed First Secretary of the Central Committee and learned all the facts about nuclear power I couldn't sleep for several days. Then I became convinced that we could never possibly use these weapons, and I was able to sleep again. But all the same we must be prepared."[32] These parallel lessons were learned independently. It was not until 1985 that

Ronald Reagan and Mikhail Gorbachev finally declared jointly that "a nuclear war cannot be won and must never be fought." That crucial nuclear taboo has existed for nearly seven decades and was well ensconced before it was jointly pronounced.

A second area where concurrence in beliefs developed was in the command and control of weapons and the dangers of escalation as the two governments accumulated experience of false alarms and accidents. A third area related to the spread of nuclear weapons. Both the United States and the Soviet Union gradually realized that sharing nuclear technology and expecting that exports could remain purely peaceful was implausible. A fourth area of common knowledge concerned the volatility of the arms race and the expenses and risks that it entailed. These views developed independently and in parallel, and it was more than two decades before they led to formal cooperation. Perfect concurrence of beliefs would lead to harmony, which is very rare in world politics. Cooperation in the nuclear area responded to both some concurrence of beliefs as well as actual and anticipated discord.[33]

By its very nature, the interconnected cyber domain requires a degree of cooperation and governments becoming aware of this situation. Some analysts see cyberspace as analogous to the ungoverned Wild West, but unlike the early days of the nuclear domain, cyberspace has a number of areas of private and public governance. Certain technical standards related to Internet protocol are set (or not) by consensus among engineers involved in the nongovernmental Internet Engineering Task Force (IETF), and the domain name system is managed by the Internet Corporation for Assigned Names and Numbers (ICANN). The United Nations and the International Telecommunications Union (ITU) have tried to promulgate some general norms, though with limited success. National governments control copyright and intellectual property laws and try to manage problems of security, espionage, and crime within national policies. Though some cooperative frameworks exist, such as the European Convention on Cyber Crime, they remain weak, and states still focus on the zero-sum rather than positive-sum aspect of these games. At the same time, a degree of independent learning may be occurring on some of these issues. For example, Russia and China have refused to sign the Convention on Cyber Crime and have hidden behind plausible deniability as they have encouraged intrusions by "patriotic hackers." Their attitudes may change, however, if costs exceed benefits. For example, "Russian cyber-criminals no longer follow hands-off rules when it comes to motherland targets, and Russian authorities are beginning to drop the laissez-faire policy."[34] And China is independently experiencing increased costs from cyber crime. As in the nuclear domain, independent learning may pave the way for active cooperation later.

Learning is often lumpy and discontinuous. Large groups and organizations often learn by crises and major events that serve as metaphors for organizing and dramatizing diverse sets of experiences. The Berlin crisis and particularly the Cuban missile crisis of the early 1960s played such a role. Having come close to the precipice of war, both Kennedy and Khrushchev drew lessons about cooperation. It was shortly after the Cuban missile crisis that Kennedy gave his American University speech that laid the basis for the atmospheric test ban discussions.

Of course crises are not the only way to learn. The experience of playing iterated games of prisoner's dilemma in situations with a long shadow of the future may lead players to learn the value of cooperation in maximizing their payoffs over time.[35] Early steps in cooperation in the nuclear domain encouraged later steps, without requiring a change in the competitive nature of the overall relationship. These governmental steps were reinforced by informal "Track Two" dialogues such as the Pugwash Conferences.

Thus far there have been no major crises in the cyber domain, though the denial-of-service attacks on Estonia and Georgia and the Stuxnet attack on Iran give hints of what might come. As mentioned earlier, some experts think that markets will not price security properly in the private sector until there is some form of visible crisis. But other forms of learning can occur. For example in the area of industrial espionage, China has had few incentives to restrict its behavior because the benefits far exceed the costs. Spying is as old as human history and does not violate any explicit provisions of international law. Nevertheless, at times governments have established rules of the road for limiting espionage and engaged in patterns of tit-for-tat retaliation to create an incentive for cooperation. While it is difficult to envisage enforceable treaties in which governments agree not to engage in espionage, it is plausible to imagine a process of iterations (tit for tat) which develops rules of the road that could limit damage in practical terms. To avoid "defection lock-in," which leads to unwanted escalation, it helps to engage in discussions that can develop common perceptions about redlines, if not fully agreed norms, as gradually developed in the nuclear domain after the Cuban missile crisis.[36] Discussion helps to provide a broader context (a "shadow of the future") for specific differences, and it is interesting to note that China and the United States have begun to discuss cyber issues in the context of their broad annual Strategic and Economic Dialogue, as well as in informal Track Two settings.

Learning occurs at different rates in different issues of a new domain. While the US-Soviet political and ideological competition limited their cooperation in some areas, awareness of nuclear destructiveness led them to avoid war with each other and to develop what Zbigniew Brzezinski called "a code of conduct of reciprocal behavior guiding the competition, lessening the danger that it could become lethal."[37] These basic rules of prudence included no direct fighting, no nuclear use, and communication during crisis. More specifically, it meant the division of Germany and respect for spheres of influence in Europe in the 1950s and early 1960s and a compromise on Cuba. On the issue of command and control, concerns about crisis management and accidents led to the hotline, as well as the Accidents Measures and Incidents at Sea meetings of the early 1970s. Similarly, on the issue of nonproliferation the two sides discovered a common interest and began to cooperate in the mid-1960s, well before the bilateral arms control agreements about issues of arms race stability in the 1970s. Unlike the view that says nothing is settled in a deal until everything is settled, nuclear learning and agreements proceeded at different rates in different areas.

The cyber domain is likely to be analogous. As we have seen, there are already some agreements and institutions that relate to the basic functioning of the Internet, such as technical standards as well as names and addresses, and there is the beginning of a normative framework for cyber crime. But it is likely to take longer before there are agreements on contentious issues such as cyber intrusions for purposes like espionage and preparing the battlefield. Nevertheless, the inability to envisage an overall agreement need not prevent progress on sub-issues. Indeed, the best prospects for success may involve disaggregating the term *attacks* into specific actions that could be addressed separately.

Involve the military in international contacts. As mentioned above, the military can be under civilian control but still have an independent operational culture of its own. By its nature and function, it is charged with entertaining worst-case assumptions. It does not necessarily learn the same lessons at the same rate as its civilian counterparts. Early in the SALT talks, Soviet military leaders complained about the American habit of discussing sensitive military information in front of civilian members of the Soviet delegation. The practice had the effect of broadening communication within the Soviet side. At the same time, Soviet military leaders had little understanding of American institutions or the role of Congress and how that would affect nuclear issues. Their involvement in arms talks helped to produce a more sophisticated generation of younger leaders. As Foreign Minister Andrei Gromyko put it, "It's hard to discuss the subject with the military, but the more contact they have with the Americans, the easier it will be to turn our soldiers into something more than just martinets."[38]

In the cyber domain, the Chinese People's Liberation Army plays a major role in recruitment, training, and operations. China today provides more opportunities for PLA generals to have international contacts than was true for Soviet officers during the Cold War, but those contacts are still limited. Moreover, while political control over the Chinese military is strong, operational control is weak, as shown by a number of recent incidents. Indeed, seven of the nine members of the Standing Military Commission wear uniforms, and there is no National Security Council or equivalent to coordinate operational details across the government. The lessons from the nuclear era would suggest the importance of involving PLA officers in discussions of cyber cooperation.

Deterrence is complex and involves more than just retaliation. Early views of deterrence in the nuclear era were relatively simple and relied on massive retaliation to a nuclear attack. Retaliation remained at the core of deterrence throughout the Cold War, but as strategists confronted the usability dilemma and the problems of extended deterrence, their theories of deterrence became more complex. While a second-strike capability and mutual assured destruction may have been enough to prevent attacks on the homeland, they were never credible for issues at the low end of the spectrum of interests. Somewhere between these extremes lay extended deterrence of attacks against allies and defense of vulnerable positions such as Berlin. Nuclear deterrence was supplemented by other measures, such as forward basing of conventional forces, declaratory policy, changes of alert levels, and force movements.

Many analysts argue that deterrence does not work in cyberspace because of the problem of attribution, but that is also too simple. Interstate deterrence through entanglement and denial still exists even when there is inadequate attribution. Even when the source of an attack can be successfully disguised under a "false flag," other governments may find themselves sufficiently entangled in symmetrically interdependent relationships that a major attack would be counterproductive—witness the reluctance of the Chinese government to dump dollars to punish the United States after it sold arms to Taiwan in 2010.[39] Unlike the single strand of military interdependence that linked the United States and the Soviet Union during the Cold War, the United States, China, and other countries are entangled in multiple networks. China, for example, would itself lose from an attack that severely damaged the American economy, and vice versa.

In addition, an unknown attacker may be deterred by denial. If firewalls are strong or the prospect of a self-enforcing response ("an electric fence") seems possible, attack becomes less attractive. Offensive capabilities for immediate response can create an active defense that can serve as a deterrent even when the identity of the attacker is not fully known. Futility can also help deter an unknown attacker. If the target is well protected or redundancy and resilience allow quick recovery, the risk-to-benefit ratio in attack is diminished.[40] Moreover, attribution does not have to be perfect, and to the extent that false flags are imperfect and rumors of the source of an attack are widely deemed credible (though not probative in a court of law), reputational damage to an attacker's soft power may contribute to deterrence. Finally, a reputation for offensive capability and a declaratory policy that keeps open the means of retaliation can help to reinforce deterrence. Of course, nonstate actors are harder to deter, and improved defenses such as preemption and human intelligence become important in such cases. But among states, nuclear deterrence was more complex than it first looked, and that is doubly true of deterrence in the cyber domain.

Begin arms control with positive-sum games related to third parties. Although the United States and the Soviet Union developed some tacit rules of the road about prudent behavior early on, direct negotiation and agreements concerning arms race stability or force structure did not occur until the third decade of the nuclear era. Early efforts at comprehensive arms control like the Baruch Plan were total nonstarters. And even the eventual SALT agreements were of limited value in controlling numbers of weapons and involved elaborate verification procedures which themselves sometimes became issues of contention. The first formal agreement was the Limited Test Ban Treaty, where detection of atmospheric tests was easily verifiable and it could be considered largely an environmental treaty. The second major agreement was the Non-Proliferation Treaty of 1968, which was aimed at limiting the spread of nuclear weapons to third parties. Both these agreements involved positive-sum games.

In the cyber domain, the global nature of the Internet requires international cooperation. Some people call for cyber arms control negotiations and formal treaties, but differences in cultural norms and the impossibility of verification make such treaties difficult to negotiate or implement. Such efforts could actually reduce national security if asymmetrical implementation put legalistic cultures like the United States at a disadvantage compared to societies with a higher degree of government corruption. At the same time, it is not too early to explore international talks and cooperation. The most promising early areas for international cooperation are not bilateral conflicts but problems posed by third parties such as criminals and terrorists.

For more than a decade, Russia has sought a treaty for broad international oversight of the Internet and "information security," banning deception or the embedding of malicious code or circuitry that could be activated in the event of war. But Americans have argued that arms control measures banning offense can damage defense against current attacks and would be impossible to verify or enforce. And declaratory statements of "no first use" might have restraining effects on legalistic cultures like the United States while having less effect on states with closed societies. Moreover, the United States has resisted agreements that could legitimize authoritarian governments' censorship of the Internet. Cultural differences present a difficulty in reaching any broad agreements on regulating content on the Internet. The United States has called for the creation of "norms of behavior among states" that "encourage respect for the global networked commons," but as Jack Goldsmith has argued, "Even if we could stop all cyber attacks from our soil, we wouldn't want to. On the private side, hacktivism can be a tool of liberation. On the public side, the best defense of critical computer systems is sometimes a good offense."[41] From the American point of view, Twitter and YouTube are matters of personal freedom; seen from Beijing or Tehran, they are instruments of attack. Trying to limit all intrusions would be impossible, but on the spectrum of attacks ranging from soft hacktivism to hard implanting of logic bombs in SCADA (supervisory control and data acquisition) systems, one could start with cyber crime and cyber terrorism involving nonstate third parties where major states would have an interest in limiting damage by agreeing to cooperate on forensics and controls. States might start with acceptance of responsibility for attacks that traverse their territory and a duty to cooperate on forensics, information, and remedial measures.[42] At some later points, it is possible that such cooperation could spread to state activities at the hard end of the spectrum, as it did in the nuclear domain.

Conclusion

Historical analogies are always dangerous if taken too literally, and the differences between nuclear and cyber technologies are great. The cyber domain is new and dynamic, but so was nuclear technology at its inception. It may help to put the problems of designing a strategy for cyber security into perspective, particularly the aspect of cooperation among states, if we realize how long and difficult it was to develop a nuclear strategy, much less international nuclear cooperation. Nuclear learning was slow, halting, and incomplete. The intensity of the ideological and political competition in the US-Soviet relationship was much greater than that between the United States and Russia or the United States and China today. There were far fewer positive strands of interdependence in the relationship. Yet the intensity of the zero-sum game did not prevent the development of rules of the road and cooperative agreements that helped to preserve the concurrent positive-sum game.

That is the good news. The bad news is that cyber technology gives much more power to nonstate actors than does nuclear technology, and the threats such actors pose are likely to increase. The transnational, multiactor games of the cyber domain pose a new set of questions about the meaning of national security. Some of the most important security responses must be national and unilateral, focused on hygiene, redundancy, and resilience. It is likely, however, that major governments will gradually discover that cooperation against the insecurity created by nonstate actors will require greater priority in attention. The world is a long distance from such a response at this stage in the development of cyber technology. But such responses did not occur until we approached the third decade of the nuclear era. With the World Wide Web only two decades old, may we be approaching an analogous point in the political trajectory of cyber security? SSQ

Notes

[1] Oddly, Max Boot does not list the nuclear revolution. See his *War Made New: Technology, Warfare and the Course of History, 1500 to Today* (New York: Gotham Books, 2006).

[2] Michael V. Hayden, "The Future of Things Cyber," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 3.

[3] A pioneering work on this question is Lloyd Etheredge, *Can Governments Learn*? (Elmsford, NY: Pergamon Press, 1985).

[4] Joseph S. Nye Jr., *The Future of Power* (New York: Public Affairs Press, 2011), chap. 5.

[5] This point is emphasized by Richard A. Clarke and Robert Knake in *Cyberwar* (New York: HarperCollins, 2009).

[6] For skeptical views that cyberwar is overhyped, see Michael Hirsh, "Here There Be Dragons," *National Journal* 23 (July 2011): 32–37.

[7] McConnell quoted in Nathan Gardels, "Cyberwar: Former Intelligence Chief Says China Aims at America's Soft Underbelly," *New Perspectives Quarterly* 27, no. 2 (Spring 2010): 16.

[8] Deputy Secretary of Defense William Lynn, remarks at 28th Annual International Workshop on Global Security, Paris, France, 16 June 2011, http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1586.

[9] William Owens, Kenneth Dam, and Herbert Lin, eds., *Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington: National Academies Press, 2009), 294.

[10] Martin C. Libicki, "Cyberwar as a Confidence Game," *Strategic Studies Quarterly* 5, no.1 (Spring 2011): 136. See also Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 136.

[11] Richard Neustadt and Ernest May, *Thinking in Time: The Uses of History for Decision-Makers* (New York: Free Press, 1986).

[12] Owens et al., *Technology, Policy, Law and Ethics*, 295–96.

[13] Ernest May, "Cold War and Defense," in *The Cold War and Defense*, ed. Keith Neilson and Ronald G. Haycock (New York: Praeger, 1990), 54. I am indebted to Phillip Zelikow for bringing this to my attention.

[14] Fred Kaplan, *The Wizards of Armageddon* (New York: Simon and Schuster, 1983), 30.

[15] Kissinger quoted in Robert Jervis, *The Meaning of the Nuclear Revolution* (Ithaca, NY: Cornell University Press, 1989), 102.

[16] McGeorge Bundy, *Danger and Survival: Choices about the Bomb in the First 50 Years* (New York: Vintage, 1990).

[17] Stuart Starr, "Toward a Preliminary Theory of Cyberpower," in *Cyberpower and National Security*, ed. Franklin Kramer, Starr, and Larry Wentz (Washington: NDU Press, 2009), 82–86.

[18] Joel Brenner, *America the Vulnerable* (New York: Penguin Press, 2011), 15.

[19] On supply chain vulnerability, see Scott Charney and Eric Werner, "Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust," Microsoft Corp., 25 July 2011, http://www.microsoft.com/download/en/details.aspx?id=26826.

20. I am indebted to John Mallery of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) for his work on these points.

21. Kaplan, *Wizards of Armageddon*, 254.

22. Ibid., 391.

23. Ibid., 134.

24. Ibid., 269.

25. Gen Keith Alexander, quoted in "US Lacks People, Authorities to Face Cyber Attack," *Associated Press*, 16 March 2011.

26. Brian Balogh, *Chain Reaction: Expert Debate and Public Participation in American Commercial Nuclear Power, 1945–1975* (Cambridge, UK: Cambridge University Press, 1991), 31.

27. The Nuclear Energy Policy Study Group, *Nuclear Power: Issues and Choices* (Ford-Mitre Report) (Cambridge, MA: Ballinger, 1977).

28. See Brenner, *America the Vulnerable*.

29. Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee white paper, 2011, 3, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

30. Jason Pontin, remarks at plenary panel, EastWest Institute Cybersecurity Summit, London, 2 June 2011.

31. Churchill quoted in Michael Mandelbaum, *The Nuclear Revolution* (Cambridge, UK: Cambridge University Press, 1981), 3.

32. Khrushchev quoted in Jervis, *Meaning of the Nuclear Revolution*, 20.

33. I am indebted to Robert O. Keohane for this point.

34. Joseph Menn, "Moscow gets Tough on Cybercrime," *Financial Times*, 22 March 2010.

35. See Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984).

36. For a description of the gradual evolution of such learning in the nuclear area, see Joseph S. Nye Jr., "Nuclear Learning and U.S.-Soviet Security Regimes," *International Organization* 41, no. 3 (Summer 1987). See also Graham Allison, "Primitive Rules of Prudence: Foundations of Peaceful Competition" in *Windows of Opportunity: From Cold War to Peaceful Competition in U.S.-Soviet Relations*, ed. Allison, William Ury, and Bruce Allyn (Cambridge, MA: Ballinger, 1989).

37. Zbigniew Brzezinski, *Game Plan* (Boston: Atheneum, 1986), 244.

38. Arkady Shevchenko, *Breaking With Moscow* (New York: Ballantine, 1985), 270–71. See also Raymond Garthoff, "Negotiating SALT," *Wilson Quarterly* (Autumn 1977): 79.

39. For details, see Nye, *Future of Power*, chap. 3.

40. I am indebted to the unpublished writings of Jeff Cooper on these points.

41. Jack Goldsmith, "Can We Stop the Global Cyber Arms Race," *Washington Post*, 1 February 2010.

42. See, for example, Eneken Tikk, "Ten Rules for Cyber Security," *Survival* 53, no. 3 (June–July 2011): 119–32.

Fall 2012

Internet Governance and National Security

Panayotis A. Yannakogeorgos

> *The debate over network protocols illustrates how standards can be politics by other means.*
>
> —Janet Abbate, *Inventing the Internet* (1999)

The organizing ethos of the Internet founders was that of a boundless space enabling everyone to connect with everything, everywhere. This governing principle did not reflect laws or national borders. Indeed, everyone was equal. A brave new world emerged where the meek are powerful enough to challenge the strong. Perhaps the best articulation of these sentiments is found in "A Declaration of Independence of Cyberspace." Addressing world governments and corporations online, John Perry Barlow proclaimed, "Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here."[1] Romanticized anarchic visions of the Internet came to be synonymized with cyberspace writ large. The dynamics of stakeholders involved with the inputs and processes that govern this global telecommunications experiment were not taken into account by the utopian vision that came to frame the policy questions of the early twenty-first century. Juxtapose this view with that of some Internet stakeholders who view the project as a "rational regime of access and flow of information, acknowledging that the network is not some renewable natural resource but a man-made structure that exists only owing to decades of infrastructure

Dr. Pano Yannakogeorgos is a research professor of cyber policy and global affairs at the Air Force Research Institute of Air University. His research interests include the intersection of cyberspace and global security, cyber norms, cyber arms control, violent nonstate actors, and Balkan and Eastern Mediterranean studies. He formerly held appointments as senior program coordinator at the Rutgers University Division of Global Affairs and was an adviser to the UN Security Council. He holds PhD and MS degrees in global affairs from Rutgers University and an ALB degree in philosophy from Harvard University.

building at great cost to great companies, entities that believe they ultimately are entitled to a say."[2]

The sole purpose of cyberspace is to create effects in the real world, and the US high-tech sector leads the world in innovating and developing hardware, software, and content services.[3] American companies provide technologies that allow more and better digital information to flow across borders, thereby enhancing socioeconomic development worldwide. When markets and Internet connections are open, America's information technology (IT) companies shape the world and prosper. Leveraging the benefits of the Internet cannot occur, however, if confidence in networked digital information and communications technologies is lacking. In cyberspace, security is the cornerstone of the confidence that leads to openness and prosperity. While the most potent manifestation of cyberspace, the Internet, works seamlessly, the protocols and standards that allow computers to interoperate are what have permitted this technological wonder to catalyze innovation and prosperity globally. The power of the current Internet governance model strengthens the global power of the American example and facilitates democratization and development abroad by permitting the free flow of information to create economic growth and global innovation.[4] Today, this Internet is at risk from infrastructure and protocol design, development, and standardization by corporate entities of nondemocratic states.

Cyber security discussions largely focus on the conflict created by headline-grabbing exploits of ad hoc hacker networks or nation-state-inspired corporate espionage.[5] Malicious actors add to the conflict and are indeed exploiting vulnerabilities in information systems. But there is a different side of cyber conflict that presents a perhaps graver national security challenge: that is the "friendly" side of cyber conquest, as Martin Libicki once termed it.[6] The friendly side of cyber conquest of the Internet entails dominance of the technical and public policy issues that govern how the Internet operates. Current US cyber security strategies do not adequately address the increasing activity of authoritarian states and their corporations within the technical bodies responsible for developing the protocols and standards on which current and next-generation digital networks function.

Internet governance can be defined as a wide field including infrastructure, standardization, legal, sociocultural, economic, and development issues. But the issues related to governance of critical Internet resources and their impact on US national security are often overlooked.

Foreign efforts to alter the technical management of the Internet and the design of technical standards may undermine US national interests in the long term. This article discusses the US national security policy context and presents the concept of friendly conquest and the multistakeholder format of Internet governance which allows for the free flow of information. There are many global challenges to the status quo, including the rise of alternative computer networks in cyberspace, that beg for recommendations to address those challenges.

Internet Governance and US National Cyber Strategy

Technical standards and protocols do not elicit the same attention as more visible threats to national cyber security. In a human capital and resource-constrained environment, attention has focused on crime, espionage, and other forms of cyber conflict rather than on the issues related to governance of critical Internet resources, development of technical standards, and design of new telecommunications equipment. In a domain that is already confusing to policy wonks, the complexity of Internet governance makes it even harder for policymakers to commit resources to a field that has no analogy in the physical world. In the nuclear age, there was no debate as to whether one could redesign the physical properties of uranium and apply them universally to eliminate the element's potential for weaponization. The underlying language of nuclear conflict was constrained by the laws of physics (e.g., nuclear fission, gravity). Physical limits in cyberspace exist as well by constraining information flows to the laws of physics—the wave-particle duality of radiation which, when modulated with bits, creates an information flow. However, the "logic" elements of cyber that permit information to flow across networks and appear within applications to create effects in the real world are bound only by the limits of human innovation. This affects the character of cyberspace. Its current form is free and open, but that does not necessarily mean it always will be. Understanding the strategic-level issues of Internet governance is thus just as critical as understanding the impact of vulnerabilities that attackers may exploit to cause incidents of national security concern. In the national security context, the technical management of the Internet matters because it may allow authoritarian states to exert power and influence over the underlying infrastructure. In the global security context, maintaining the values of free-flowing information within Internet governance bodies will continue to foster innovation and economic prosperity in both developed and developing states.

Several current national strategies articulate nationwide responses to cyber threats.[7] They tend to focus on catastrophic national security incidents rather than on the battles within the organizations that set technical standards or manage the day-to-day operation of the Internet. The White House does highlight the importance of current multistakeholder forums for design and standardization of the technical standards via "collaborative development of consensus-based international standards for information and communication technology . . . a key part of preserving openness and interoperability, growing our digital economies, and moving our societies forward."[8] Furthermore, the challenges we face in international standards-setting bodies are recognized in that "in designing the next generation of these systems, we must advance the common interest by supporting the soundest technical standards and governance structures, rather than those that will simply enhance national prestige or political control."[9] However, these issues are drowned out by more-sensational, hypothetical situations of a cyber doomsday.

Security demands that the language of the Internet—the underlying technical standards and protocols—continue to sustain free-flowing information. If "code is law" in cyberspace, as some posit,[10] then the standards and protocols are the fabric of cyber reality that give code meaning. In policy circles, cyberspace is already considered the "invisible domain." Technical standards and protocols are, thus, "invisible" squared. However, these protocols define the character of the Internet and its underlying critical infrastructures. As noted elsewhere, "The underlying protocols to which software and hardware design conforms represent a more embedded and more invisible form of level architecture to constrain behavior, establish public policy. . . . [I]n this sense protocols have political agency—not a disembodied agency but one derived from protocol designers and implementers."[11] In the past it was the United States that led the world in the development of protocols and standards. As a result, the values of freedom were embedded in the Internet's design and character, which incubated innovation that continues to spur socioeconomic development globally.

Within the DoD context, a single, connected, open Internet is critical to assuring its missions by facilitating collaboration within the agency and with its mission partners. Today, the department lists in its *Strategy* *for Operating in Cyberspace* its concerns about "external threat actors, insider threats, supply chain vulnerabilities, and threats to DoD's operational ability."[12] Other elements from the DoD's *Information Enterprise Strategic Plan* that articulate concerns with Internet governance and advocate for "DoD equities at international technical and governance meetings" should be added to the list.[13] However, the sheer political nature of the documents does not adequately address broader US foreign policy goals within global Internet governance bodies as much as intended. Thus, DoD computer scientists and engineers risk taking the backseat in an area where they once pioneered. Creating the Internet and maintaining the technical edge are two very different problems.

The Friendly Side of Cyber Conflict

Looming battles in Internet standards and governance bodies will determine the future character of the Internet. The advanced deployment of IPv6 in Russia and China and development of new standards by near-peer-competitor countries are creating new technical standards and deploying them into the global marketplace, thus enabling friendly cyber conflict.

Friendly conquest occurs when a noncore operator of a system enters into partnership with a core operator in exchange for access to a desired information system. Cyber theorist Martin Libicki notes,

> One who controls a system may let others access it so that they may enjoy its content, services and connections. With time, if such access is useful . . . users may find themselves not only growing dependent on it, but [also] deepening their dependence on it by adopting standards and protocols for their own systems and making investments in order to better use the content, services or connections they enjoy.[14]

The core partner in such a coalition emerges to dominate noncore members who have come to depend on the service offered, though not without some vulnerability to the core partner's network. Fears exist "that the full dependence that pervades one's internal systems may leave one open for manipulation. . . . The source of such vulnerability could range from one partner's general knowledge of how the infrastructure is secure, to privileged access to the infrastructure that can permit an attack to be bootstrapped more easily."[15]

Libicki operates with relational mechanisms to explain how coalitions leading to friendly conquest occur. Friendly conquest in cyberspace can be surmised as the willing participation of X in Y's information system. X willingly enters into a coalition with Y in cyberspace. Y's friendly conquest of X occurs when X becomes dependent on Y's system. This is not to say that X merely entering the coalition will cause the conquest. X's perceived need for access to Y's cyberspace (or inability to construct its own) causes it to willingly enter into a coalition with Y. X adopts Y's standards and protocols making up the information system architecture of Y's cyberspace in a way that allows it to interoperate within X's cyberspace. X adopts Y's cyberspace architecture and thus the necessary condition for Y's friendly conquest. It is a facilitating condition for X's hostile conquest. X might begin to use the standards and protocols of Y's cyberspace as a model for its own cyberspace. Since Y is an expert in its own standards and protocols, X's modeling of these standards in its own systems is another vulnerability, which can facilitate X's hostile conquest by Y. X does not have to be a friend. It can be a neutral or a possible future enemy of Y. There is utility in Y opening its cyberspace to X only if Y sees some benefit to itself, although Libicki does argue that Y will open its cyberspace regardless. Once friendly conquest is accomplished, Libicki argues, it can facilitate hostile conquest in cyberspace. Friendly conquest of X by Y may thus facilitate hostile conquest in cyberspace conducted by Y against X.

The Internet and its underlying technical infrastructure are a potent manifestation of how the United States, as core operator of an information system, extended friendly dominance over allies and adversaries alike through creation of the technology and setting the rules for its operation. The Internet relies on products designed and operated by US-based entities such as the Domain Name System (DNS) and Internet Corporation for Assigned Names and Numbers (ICANN), Microsoft, and Cisco. Users around the world, such as Google and Facebook, have come to rely on services offered over this platform. The dominant position that US-based entities currently have is not permanent. The Estonian-developed Skype is indicative that services may be non-US in origin. Yet, even when an Internet-based service is created by foreign entities, most of the information flowing through the said application passes through hardware in the United States. When vulnerabilities are perceived, other nations may try to exit our information system to preserve their cyber sovereignty and expand their influence by attracting customers toward their own indigenous systems and away from the Internet.[16] Thus, our strategic advantage in cyberspace is not timeless and is being contested in varying degrees by near-peer competitors. Hence, we should understand their current responses to US technological dominance to refine our cyber strategy within the context of friendly cyber conquest.

US Air Force doctrine recognizes one aspect of friendly conquest: supply-side infrastructure vulnerabilities. "Many of the COTS [commercial off the shelf] technologies (hardware and software) the Air Force purchases are developed, manufactured, or have components manufactured by foreign countries. These manufacturers, vendors, service providers, and developers can be influenced by adversaries to provide altered products that have built-in vulnerabilities, such as modified chips."[17] Friendly conquest goes beyond adversaries merely being able to infiltrate the supply chain and create backdoors on servers of national security significance before they enter the United States.[18] The threat also comes from the emergence of new technologies in which the United States is not the core operator but may become dependent. With the focus on malicious cyber attacks, not enough attention is being paid to the soft underbelly of the cyber world—the technologies and standards that have allowed cyberspace to emerge from the electromagnetic spectrum.

China is making a great leap forward in terms of sowing the seeds for global friendly conquest in cyberspace. As reported by the US-China Economic and Security Review Commission, "If current trends continue, China (combined with proxy interests) will effectively become the principal market driver in many sectors, including telecom, on the basis of consumption, production, and innovation."[19] US reliance on China as a manufacturer of computer chips and other information and communications technology (ICT) hardware has allowed viruses and backdoors in equipment used by US-based entities, including the military. Extraordinarily low-priced Chinese-made computer hardware is a lucrative buy in Asia and the developing world.[20] Furthermore, Chinese entities, such as Huawei, are on the leading edge of developing the standards of next-generation mobile 4G LTE networks.[21]

One example of how efforts at friendly conquest can backfire and make the United States vulnerable to cyber attack was demonstrated in Microsoft's experience with China. In 2003, China received access to the source code for Microsoft Windows in a partnership with Microsoft to cooperate on the discovery and resolution of Windows security issues. The China Information Technology Security Certification Center

(CNITSEC) Source Code Review Lab, described as "the only national certification center in China to adopt the international GB/T 18336, the ISO 15408 standard to test, evaluate and certify information security products, systems and Web services," was the focal point of this collaboration.[22] Undeterred by International Organization of Standards (ISO) criteria, and unanticipated by many experts in the field, Chinese computer scientists reverse-engineered the code. This allowed them to develop malicious code, including viruses, Trojan horses, and backdoors, that exploited software vulnerabilities in the operating system. These efforts resulted in the shutting down of the US Pacific Command Headquarters after a Chinese-based attack.[23] Chinese entities are also making great strides in developing core information systems upon which others will come to rely. Virtual reality (VR) technologies are one example of an emerging tool that could become as ubiquitous for social and commercial interactions as the Internet is today. Globally, people are increasingly using VR technology fused with the Internet to socially interact.[24] Experts have noted that

> any country that succeeds in dominating the VR market may also set the technical standards for the rest of the world, and may also own and operate the VR servers that give them unique access to information about future global financial transactions, transportation, shipping, and business communications that may rely on virtual worlds. . . .
>
> Global commerce is expected to "come to rely heavily on VR." Banking, transportation control, communications are all types of global commerce occurring in a virtual reality.[25]

While current strategies do address the supply-chain risks posed by foreign manufacturing, the trend of China taking the lead in the protocols that will come to underlie VR and other technologies, as well as standard setting within international bodies, is a challenge that current cyber strategies insufficiently address. This may be due in part to the cultural differences in the relations between US-headquartered multinational corporations (MNC) and the US government (USG) versus the MNCs in foreign countries that at times have very close relations to their own governments.

Multistakeholders and Internet Governance

Business entities such as multinational corporations contribute to the formation of policies regulating international communications formally within the International Telecommunications Union (ITU) and informally through the personal contributions of their employees within the ICANN, the Internet Engineering Task Force (IETF), and other organizations. Within the United States, telecommunications service providers (dating back to the era of electrical telegraph systems) were never part of a state-owned monopoly. This was not the case in the rest of the world.[26] British Telecom and Deutche Telekom, for example, were state-owned entities before being privatized in the 1990s. Granted, although there is no direct state control within the United States, telecommunications companies are regulated by the state. In international telecommunications negotiations, a state and its ICT firms have a symbiotic relationship.[27] This has been the case since the International Telegraph Union, predecessor of the International Telecommunications Union, began meeting in the mid nineteenth century to regulate telegraphy policies.[28] Thus, the view in the developing world is that "at present, it is . . . U.S. law which applies globally by default as most monopoly Internet companies are U.S.-based."[29]

If trade is a political activity, then firms are political actors. States can utilize firms to distribute or reward power to meet their own political objectives.[30] Since states and firms both cause effects on the behavior of the other, a dynamic bidirectional interaction exists between the state and the MNC.

Important policy tools that affect the behavior of MNCs include export controls, protectionism, and strategic trade policy. Export controls tend to have a political purpose since, as one expert notes, "they are designed to prevent rival states from gaining access to key resources and technologies," or to punish a state.[31] Firms manufacturing strategic goods rely on governments to adopt trade policies that will support the firm's competitive stance in the global market,[32] but states do place restrictions on what may be exported, even if it is to the detriment of a firm's competitiveness in foreign markets.[33] In the United States, the federal government lost the so-called encryption wars of the 1990s, when private industry protested policies prohibiting the export of strong encryption software for strategic reasons.[34]

In an effort to prevent criminals from communicating using unbreakable codes, some firms implement law enforcement intercept (LEI) mechanisms so national security agencies can monitor suspected criminal and terrorist communications.[35] US firms and persons associated with them, who develop, maintain, and revise the core standards and technological infrastructures, are stigmatized by such allegations which depict a rogue national security apparatus and private sector in collusion capturing all of the world's data. This does not reflect the fact that, unlike in authoritarian states, careful compliance with US laws designed to protect user privacy maintains a separation between government and the private sector.[36] Media preferring headline-grabbing allegations decrease global trust in the American private sector and validate the narratives that the Internet governance mechanisms must be internationalized. Thus, the close relationship between governments and firms in the area of strategic trade policy affects both how firms operate and how governments counteract the misuse of cyberspace.[37]

The global perception that the US government has de facto control of critical Internet resources is largely shaped by other nations' experiences of the close relationship between telecommunications companies and their national governments. Uniquely, the US government has never owned or operated any telecommunications companies. As the rest of the world shifted to the US privatized telecom model, prior experience of government control of the sector did not leave their cognitive balance. Today these experiences cast a shadow of suspicion over the special agreement between the ICANN and the US Department of Commerce.

Critical Internet Resources and Infrastructure

Technical management of the Domain Name System, invented by the DoD and governed by it in its formative years, was assumed by the Department of Commerce in 1998 and subsequently evolved into its current nongovernmental multistakeholder model.[38] The description here will not delve into the tactical- and operational-level functioning of each organization that has a role in Internet governance.[39] It will instead offer a brief recap of the underlying technology and the organizations that have a role in setting the standards which allow for technical functioning of the Internet. It is thus the purpose of this section to provide an account of Internet governance as a source of national security concern. With discussions focusing on malicious activities, there has been little consideration to the implications of the peaceful work of designing and maintaining the Internet and the implications these activities have on US interests.

Critical Internet resources (CIR) "in the context of Internet governance usually refers to Internet unique logical resources rather than physical infrastructural components or virtual resources not exclusive to the Internet. CIRs must provide a technical requirement of global uniqueness requiring some central coordination: Internet address, DNS, Autonomous System Numbers."[40] Unlike the popular conception of a limitless Internet, the underlying address space is limited. Indeed, IP address space has nearly run out. Foreseeing this Internet protocol, engineers developed IPv6, which among other improvements increased the total number of potential IP addresses from 4,294,967,296 in IPv4 to 2^{128} in IPv6. It is recognized today that "deploying IPv6 is the only perennial way to ease pressure on the public IPv4 address pool."[41] As the world begins a transition from using IPv4 to IPv6 as the dominant communications protocol for the global Internet, the United States is not leading its deployment. Russia currently enjoys the greatest deployment in terms of market penetration, and China enjoys the greatest deployment in sheer numbers.[42] The consequences of delayed deployment are related to both Internet governance and the more traditional security threats. On the latter point the National Institute for Standards notes that the "prevention of unauthorized access to IPv6 networks will likely be more difficult in the early years of IPv6 deployments."[43] Thus, competitor nations that have more experience in national-level deployments of IPv6 have greater technical understanding of its real-world operations. The Air Force NIPRNet will not be entirely enabled for IPv6 until 2014. Even then, it has been noted that the plan is to use both IPv4 and IPv6 in parallel for the next 10–15 years.[44] As deployment of IPv6 as the backbone of the Internet continues, Russia and China may have the perceived legitimacy as IPv6 leads and take advantage of that opportunity to shift control of these scarce address spaces from the ICANN toward the control of an intergovernmental body, such as the United Nations.

The ICANN and the Current Internet Governance Structure

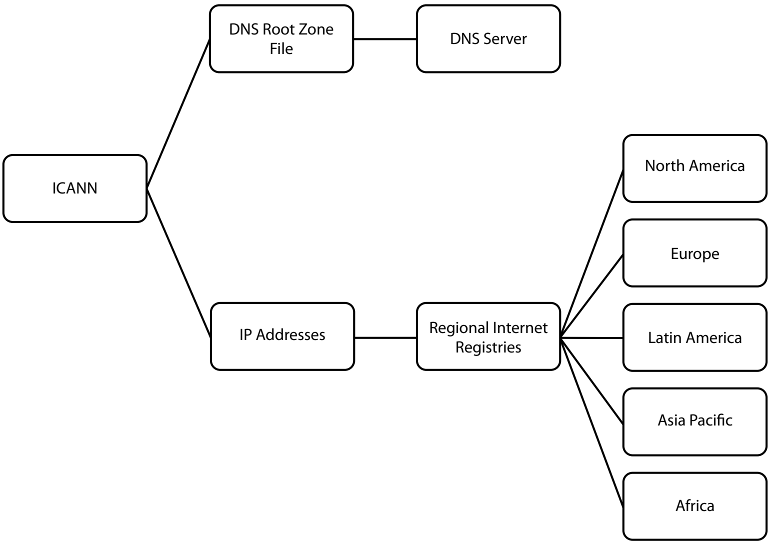
Because cyberspace is a man-made domain, infrastructure and standardization are critically important. Global bodies of computer scientists and engineers create the standards and rules on which the Internet—the most potent manifestation of cyberspace—operates. Indeed, many of these global bodies began as DISA, DARPA, or other USG programs that were privatized in the mid 1990s. Thus, the development of the next-generation Internet does not have the United States as the prime mover.[45] Instead, standards and processes are being developed by Russian, Chinese, and other foreign scientists and engineers. Today's machines speak a form of the English language to each other. If US scientific excellence continues its degenerative path, future networks may come to rely on machines speaking foreign languages. Furthermore, governance of the DNS and IP address allocation is being challenged to migrate from the current multistakeholder approach to an intergovernmental mechanism within the ITU. This is the friendly side of cyber conflict.

The DNS allows people to use Uniform Resource Locators (URL) to communicate with other machines on the Internet. Instead of having to type in the IP address of a website—a string of numbers—a person can type a natural language URL, such as www.af.mil, into a web browser to connect with the desired corresponding IP address. This makes the web user-friendly and to the common user might as well be the work of a wizard that allows information to be piped onto someone's computer. However, IP addresses are scarce, especially in IPv4. The processes for assigning scarce IP addresses and allowing the Internet to serve as a global platform are complex, both technically and, increasingly, politically.

The allocation of IPv4 address space to various registries is provided by ICANN via the Internet Assigned Numbers Authority (IANA).[46] Globally routable IP addresses reside in DNS databases on root zone databases that allow for the translation of URLs into IP addresses[47] (see figure next page). The top-level domain names, such as .com or .org, are maintained and updated by the ICANN, which was once under the Department of Commerce (DoC). Now operating under a memorandum of understanding with the DoC, the ICANN continues to be the sole source of IP address allocation to specific DNSs and regional Internet registries to assure a uniform Internet experience for all. By governing and maintaining the DNS central root zone databases and backing them up on DNS servers worldwide, the ICANN assures that if a domain name is available, someone can buy it and link it with an IP address to create an online presence.[48]

Internet Engineering Task Force: Stewards of TCP/IP

Internationally standardized communications protocol stack, called Transmission Control Protocol and Internet Protocol (TCP/IP), allows for the flow of data packets and information across computer networks, including the Internet. TCP/IP is standardized by the International Organization of Standards for the Open Systems Interconnection (OSI) model as the basis of Internet networking. A brief description of how information is sent across networks is necessary to better understand the significance of TCP/IP. Data packets are the basic units of network traffic. They are the standard means of dividing information into smaller units when sending it over a network. A significant component of computer networks is the IP header, which contains information pertaining to the source and destination addresses. Machines require these strings of numbers to connect with other computers on the Internet or other networks.[49] All networked hardware must have a valid IP address to function on a network. Data packets are recreated by the receiving machine based on information within a header of each packet that tells the receiving computer how to recreate information from the packet data. Without internationally standardized protocols such as TCP/IP, there would be no assurance that packets could be read by a receiving machine.[50]



The most esoteric of all critical Internet resources are the autonomous system numbers (ASN). These numbers are used by network providers at "peering points" to allow information to flow from, say, Verizon to AT&T, among other uses. Border gateway protocols are one aspect of ASNs.

Internet policy debates have proven the ineffectualness of multilateralism as the United States strives to lead and others fail to follow.

American technological innovation in the development and maintenance of the Internet's backbone is unquestioned. But global efforts to promote regulatory reform, such as including institutions of global governance like the ITU as entities responsible for overseeing the ICANN, are a tense political issue closely linked with the national cyber security concerns of democratic and autocratic regimes alike. In sum, American "leadership" as first among equals has led to a succession of dead ends. We are witnessing countermoves by friends and competitors alike that may gain momentum during the 2012 World Conference on International Telecommunication.[51]

Global Challenges to the Status Quo

Global information flowing through open elements of cyberspace, such as the Internet, is regulated by national and regional bodies coordinating their policies internationally. Standards that have been created for elements of cyberspace have required lengthy processes at various bodies, such as the International Organization for Standardization and ITU, to assure sufficient technical and political cooperation among nation-states. While US-based entities have traditionally set the standards for Internet technology, China-based entities, such as the ZTE Corporation, are increasingly taking on roles within the ITU to draft important international standards that will shape the world's next-generation networks. This is not a recent development. As early as 2004, Chinese personnel working in senior ITU Telecommunication Standardization Sector positions began to discuss using the transition to IPv6 as a way to correct a perceived imbalance in address allocation between the United States and the developing world: "The early allocation of IPv4 addresses resulted in geographic imbalances and an excessive possession of the address space by early adopters. This situation was recognized and addressed by the Regional Internet Registries (RIR). . . . Some developing countries have raised issues regarding IP address allocation. It is important to ensure that similar concerns do not arise with respect to IPv6."[52] This is indicative of a desire by some states to perhaps shift the governance of IPv6 address allocation into a global institution such as the ITU.

From the perspective of maintaining US national interests, the current multistakeholder framework governing critical Internet resources continues to be a good mechanism for regulating the day-to-day technical operations of the Internet. However, momentum related to Internet governance within the United Nations is gaining within political forums. Led by Russian and Chinese initiatives, competitors and partners alike have been working toward internationalizing the Internet's technical governance. China and Russia, along with India, South Africa, and Brazil, have led initiatives against US dominance of the ICANN. These efforts have been in the works for nearly a decade.[53] As the DoD ARPANET experiment emerged to become a significant component of global socioeconomic development and governments increasingly came to realize its importance, the momentum for internationalizing its backbone, the ICANN, became greater. Recall that these pushes for internationalization are due in part to the perception of US government control over ICANN via the DoC and NTIA, shaped by the history of special relationships between state telecommunication corporations existing in other countries.

The (Potential) Tyranny of the ITU over Critical Internet Resources

One battleground for debates over internationalizing the ICANN was observed during preparations for the World Summit for the Information Society (WSIS),[54] when significant opposition to the current Internet governance began to emerge.[55] For instance, in March 2004 during a UN-hosted Global Forum on Internet Governance.[56] Brazilian delegate Maria Luiza Viotti claimed that Internet governance needed reform, since it is not inclusive of developing countries and instead appears to be under the ownership of one group of countries or stakeholders.[57] Lyndall Shope-Mafole, chair of South Africa's National Commission, spoke on similar lines, arguing that the legitimacy of the ICANN's processes, rather than its functioning, was of most concern for developing countries.[58] Thus, after rigorous talks, delegates concluded on the basis of concerns from the developing world that the ICANN required further reform. Throughout the WSIS process, and continuing in other forums discussing Internet governance and global cyber security, Brazil has continued to be a vocal proponent against the US position in the ICANN. In 2011, India joined South Africa and Brazil in proposing to "operationalize the Tunis mandate" by

> bearing in mind the need for a transparent, democratic, and multilateral mechanism that enables all stakeholders to participate in their respective roles, to address

> the many cross-cutting international public policy issues that require attention and are not adequately addressed by current mechanisms and the need for enhanced cooperation to enable governments, on an equal footing, to carry out their roles and responsibilities in international public policy issues pertaining to the Internet, India proposes the establishment of a new institutional mechanism in the United Nations for global Internet related policies, to be called the United Nations Committee for Internet-Related Policies (CIRP).[59]

The CIRP idea has gained momentum within the developing world as a counter to the current technical management of the Internet. Indeed, it echoes closely Chinese concerns voiced by the China Organizational Name Administration Center (CONAC) that "the U.S. government has the sovereign power to control the Internet resources. We therefore suggest making the computer security plan available for comment by all multistakeholders, for maintaining the security of cyber space is not a mission only for the U.S. government, and it cannot be accomplished by any single nation."[60]

From Russia, then prime minister Vladimir Putin stated,

> The International Telecommunication Union is one of the oldest international organisations; it's twice as old as the United Nations. Russia was one of its cofounders and intends to be an active member. We are thankful to you for the ideas that you have proposed for discussion. One of them is establishing international control over the Internet using the monitoring and supervisory capabilities of the International Telecommunication Union (ITU).[61]

Thus, the United States faces a significant challenge within the ITU from autocratic regimes leading the developing world to move control of critical Internet resources toward a multilateral body. The underlying danger is a shift away from an Internet whose defining characteristic is the free flow of information toward a model in which the political agendas of nondemocracies attempt to exert control over the flow of information. Hence, the United States and like-minded nations must surge diplomatically to ensure the character of the Internet remains free from the political control of a multilateral institution.

This diplomatic struggle for control of the Internet has also been occurring within various other forums, like the UN Commission on Science and Technology for Development. Suggestions being made on the issue include:

> Establishment of an ad hoc working group under the Commission on Science and Technology for Development with a view to the development of an insti-

> tutional design and road map to enhance cooperation on Internet-related public policy issues with the support of the Secretary-General . . .
>
> Creation of a more permanent committee on international public policy issues pertaining to the Internet within the United Nations system, possibly modeled on the Committee on Information, Communications and Computer Policy of the Organization for Economic Cooperation and Development . . .
>
> And more concretely, global policy questions should be addressed by an entity with global representation, such as the United Nations, and regional questions by entities with regional representation, such as the Council of Europe . . . [and] the participation of relevant organizations in discussions on Internet governance at the quadrennial ITU Plenipotentiary Conference, and the public review process and Governmental Advisory Committee of ICANN.[62]

With the upcoming World Conference on Telecommunications in December 2012, such statements indicate that these ideas will resurface as part of the ITU effort to revise International Telecommunications Regulations (ITR) to include governance of next-generation critical Internet resources within the ITU's mandate and assume a greater role in Internet governance.[63]

Making Internet governance open to intergovernmental processes could put US national security at risk, given the potential for less-than-responsible state actors to take the current privatized laissez-faire approach to governing the Internet and have nation-states and their corporate entities take control of governing critical Internet resources. This would not ensure DoD equities are protected in an environment where critical decisions on underlying technical standards and Internet operation would be left to national governments that are competing with the United States.

Shadow "DNS" Rising

As described above, the critical Internet resources that allow for universally resolvable URLs and global Internet communications are possible due to the root system that is managed by the ICANN and protocols designed, developed, and debated within the IETF (among other organizations). Although this allows for a free and open Internet to function, the standards and protocols that the ICANN uses to maintain the domain name registries can be used by individuals, ad hoc networks, and nation-states to design and deploy an alternative DNS system that can either be independent of or "ride on top" of the Internet. A corporate LAN, such as ".company–name" for internal company use, is an example of the first. When a group wishes to ride over the global DNS root but incorporate its own pseudo top-level domain, core operators of the pseudo domains can use specific software resources to resolve domains that are globally accessible within their alternative DNS system. American audiences can experience what it is like to enter an alternative DNS universe via the Onion router (TOR) network. Downloading the Onion router package and navigating to websites one would prefer to visit anonymously (the typical use of TOR), one may point the TOR browser to websites on the ".onion" domain and mingle where the cyber underworld has started shifting the management of its business operations these days to avoid law enforcement and to add another layer of protection to their personas.[64]

Should significant usage of such shadow Internets occur, this could lead to the loss of confidence and utility of the Internet itself. The greatest risk comes when nation-states develop and deploy their own alternate domain-naming systems for internal use, thereby separating themselves from the global Internet. This is different from controlling access points and actually develops country-level intranets that may or may not be connected to the global Internet.[65] The discussion herein focuses on Russia and China as far as their successes in deploying potentially new intranets for in-country use. Other countries, such as Iran, are following suit.

US involvement in *openly* promoting and organizing "digital activists" by issuing up to $30 million in grant funding to increase open access to the Internet, support digital activists, and push back against Internet repression wherever it occurs in the fight for free flows of information, generates international friction that is counterproductive to promoting international cooperation on cyber security issues."[66] The "Internet Freedom Agenda" is one example of this phenomenon.[67] Such technology effectively allows citizen-activists to hack past government digital sentries to spread forbidden information. Other tools allow activists to don digital disguises and organize themselves into social movements designed to topple regimes. The result has been the emergence of alternative national networks that essentially create alternate domain name systems for in-country use, allowing for censorship of content and stifling the productivity of the current Internet topology. China is one country that has implemented this on a national scale, and Iran is closely following suit.[68] Others are sure to follow these attempts. The rise of a splintered

Internet will certainly change the character of the current Internet, with negative consequences for freedom and prosperity worldwide. Those who wish the Internet to remain free and open will benefit and draw a sharp, moral contrast with those wishing to control the master switch. Thus, maintaining the current Internet governance model, while addressing legitimate concerns of friends and allies, will help assure the Internet continues to serve as a robust platform for human economic development.

Conclusion

Failure to pay attention to our vulnerabilities from Internet governance and friendly conquest may provide our adversaries with a strategic advantage in cyber conflict. Our own cyber-attack efforts will also become complicated as networks that are not based on protocols and standards developed by US-based entities are deployed by our competitors. To aid how we conceive of cyberspace, as well as adjust to change within the cyber environment, there must be a broad dialogue on these issues. Despite the Internet's historic roots within the Department of Defense, there has not been a well-organized effort to influence the development of technical standards and policies affecting Internet governance. Currently, the DoD has remained in a reactive mode, coordinating and commenting on the various global norms and standards being considered within the USG processes related to Internet governance. Because of this approach, the DoD and the USAF may be perceived as not having the legal expertise or technical reputation in Internet governance. The DoD, and the US Air Force in particular, should exercise leadership and take a more active role in the development of information technology infrastructure standards as it once did. Furthermore, it should more carefully document its role and provide metrics on its participation and position with Internet governance bodies. The Air Force should play a leading role within the DoD and the whole of government by explicitly focusing on a broader concept of friendly conquest that implicitly exists in policies, strategies, and doctrines. The 2012 World Telecommunications Conference in December 2012 may be the right place to commence this effort.

As the hardware and software on which the global Internet is based evolve and non-US entities begin to invent new hardware, standards, and protocols, potentially taking market share away from US entities, the US position as core cyber infrastructure operator will diminish. The United States currently enjoys technological dominance through its position of developer and core provider of Internet services made possible by the ICANN and the top-level Domain Name System. But our national cyber security strategies do not adequately address threats that may stem from other countries developing the protocols, standards, and technologies on which the next generation of networks will be based. The Air Force has a key role to play given the wealth of technical excellence that resides within its community of scientists and engineers. It cannot act alone, however, and the DoD will need to focus some of its already limited cyber resources toward Internet governance. Not doing so risks allowing foreign-designed technical standards and protocols to form the backbone of next-generation IT and potentially puts DoD operations at risk by reversing what is now an Internet characterized by the free flow of information on which the DoD depends. The USAF remains the leading US military service impacting cyberspace, and thus its actions or inactions in Internet governance debates matter.

Notes

[1] John Perry Barlow, "A Declaration of Independence of Cyberspace," published online 8 February 1996.

[2] Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (New York: Alfred A. Knopf, 2010), 290.

[3] Granted, for the most part, manufacturing does not occur within the United States, which presents the national security risk of supply-chain vulnerabilities. This is a subset of friendly conquest but remains beyond the scope of the argument here.

[4] American values are a core national interest. *National Security Strategy* (Washington: The White House, May 2010), 35.

[5] See, for example, Bryan Krekel, Patton Adam, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Washington: US-China Economic and Security Review Commission, 27 March 2012); and Dmitri Alperovitch, *Revealed: Operation Shady RAT* (Santa Clara, CA: McAfee White Paper, 2011), http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

[6] Martin Libicki, *Conquest in Cyberspace* (New York: Cambridge University Press, 2007).

[7] The *National Strategy to Secure Cyberspace* (*NSSC*) (Washington: The White House, February 2003); John Rollins and Anna C. Henning, *Comprehensive National Cybersecurity Initiative* (*CNCI*) (Washington: Congressional Research Service, 10 March 2009; declassified in March 2010); the *International Strategy for Cyberspace* (Washington: The White House, May 2011); and the *Department of Defense Strategy for Operating in Cyberspace* (Washington: DoD, July 2011) are to date the leading relevant directives on cyber security. Although the White House completed a cyberspace policy review in 2009, the primary suggestions in the review amount to existing policy recommendations already in the *NSSC* and declassified *CNCI*. After the White House *Cyberspace Policy Review*, several initiatives were either launched or announced by departments and agencies of the US government. Declassification of the *CNCI*

enabled the timely development of a framework for international partnerships consistent with a common cyber security policy. In 2011, the White House released the *International Strategy for Cyberspace*. Subtitled, *Prosperity, Security, and Openness in a Networked World*, the document falls short of providing the solutions necessary to live up to its name. The simple fact is, without security there can be no prosperity or openness.

[8] *International Strategy for Cyberspace*, 12.

[9] Ibid., 15.

[10] Lawrence Lessing, "Code is Law," in *Code: And Other Laws of Cyberspace, Version 2.0* (New York: Basic Books, 2006), 11–10.

[11] Laura DeNardis, *Protocol Politics: The Globalization of Internet Governance* (Cambridge: MIT Press 2009), 11.

[12] Cyrus Farivar, "Security Researcher Unearths Plans for Iran's Halal Internet," *Ars Technica*, 17 April 2012, http://arstechnica.com/tech-policy/2012/04/iran-publishes-request-for-information-for-halal-internet-project/.

[13] *Department of Defense Information Enterprise Strategic Plan 2010–2012* (Washington: DoD, May 2010), 10, http://dodcio.defense.gov/Portals/0/Documents/DodIESP-r16.pdf. Examples contained in the plan include the Internet Engineering Task Force, ICANN, Internet Governance Forum, Réseaux IP Européens, and American Registry for Internet Numbers/North American Network Operators' Group.

[14] Libicki, *Conquest in Cyberspace*, 12.

[15] Ibid., 137.

[16] The global positioning system (GPS) is one example where control of both the software and hardware is being contested. Although access to GPS is available without a fee for the basic service, friends and competitors alike have realized their dependence on this US system makes them vulnerable. Russia is modernizing its GPS system, and the European Union and China are developing independent GPS systems of their own. The long time cycle from intent to implementation of these new systems is due to the immense financial costs of deploying a space network. Cyber time cycles may be shorter, given the lower costs associated with deploying a national computer network compared with multiple high-tech satellites launched into space. For a more complete discussion of alternate GPS systems, see Lt Col Scott W. Beidleman, *GPS versus Galileo: Balancing for Position in Space* (Maxwell AFB, AL: Air University Press, 2006).

[17] Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, 2010, 4.

[18] Bruce Rayner, "Ferreting out the Fakes," *Electronic Engineering Times*, 15 August 2011, 24. See also John Markoff, "Computer Gear may Pose Trojan Horse Threat to Pentagon," *New York Times*, 10 May 2008, 12.

[19] *The National Security Implication of Investments and Products from the People's Republic of China in the Telecommunications Sector*, U.S.-China Economic and Security Review Commission Staff Report, January 2011, 7, http://www.uscc.gov/RFP/2011/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf.

[20] LCDR A. Anand, "Threats to India's Information Environment," in *Information Technology: The Future Warfare Weapon* (New Delhi: Ocean Books Pvt. Ltd., 2000), 56–62.

[21] "Huawei Conducts World's First Commercial Network LTE Category 4 Trial," *Cellular News*, 9 May 2012, http://www.cellular-news.com/story/54329.php.

[22] "China Information Technology Security Certification Center Source Code Review Lab Opened," *Microsoft News Center*, 26 September 2003, http://www.microsoft.com/presspass/press/2003/sep03/09-26gspchpr.mspx.

23. Barrington M. Barrett Jr., "Information Warfare: China's Response to U.S. Technological Advantages," *International Journal of Intelligence and Counterintelligence* 18, no. 4 (2005): 682–706.

24. Ibid.

25. Clay Wilson, *Avatars, Virtual Reality Technology, and the U.S. Military: Emerging Policy Issues* (Washington: Congressional Research Service, April 2008), 4, 12.

26. Anton A. Huurdeman, *The Worldwide History of Telecommunications* (Hoboken, NJ: John Wiley & Sons, 2003), 91–146, 153–85. See also Jill Hills, "International Market Structure and the ITU," in *Telecommunications and Empire* (Champaign: University of Illinois Press, 2007), 91–116.

27. Edward Comor, "Communication Technology and International Capitalism: The Case of DBS and US Foreign Policy," in *The Global Political Economy of Communication: Hegemony, Telecommunication and the Information Economy*, ed. Comor (New York: St Martin's Press, 1994), 83–102.

28. Jill Hills, *The Struggle for Control of Global Communications: The Formative Century* (Champaign: University of Illinois Press, 2002.)

29. Parminder Jeet Singh, "India's Proposal Will Help Take the Web out of U.S. Control," *Hindu Online*, 17 May 2012, http://www.thehindu.com/opinion/op-ed/article3426292.ece.

30. Debora L. Spar, "National Policies and Domestic Politics," in *The Oxford Handbook of International Business*, ed. Alan M. Rugman (New York: Oxford University Press, 2008), 207.

31. Ibid., 209.

32. Ibid., 212.

33. Standard export restrictions are meant to prevent access, whereas sanctions or embargoes aim to act as punitive measures. Sanctions appear to have the greatest effects on firms. For example, firms in State I which imports from State A will be at a loss if State A subjects State I to a sanctions regime. However, firms that export from State A to State I will also be at a loss since they will suffer from a decline in sales and face the possibility of ties being severed with State I in the long term. Thus, as Spar notes, MNCs must remain aware of political developments within the countries in which they operate so as to not find themselves prohibited from accessing a market due to sanctions. Thus, export controls are one mechanism that can affect the behavior of firms and economies.

34. Richard C. Barth and Clint N. Smith, "International Regulation of Encryption: Technology Will Drive Policy," in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*, ed. Brian Kahin and Charles Nesson (Cambridge: MIT Press 1998), 283–99.

35. James Bamford, *The Shadow Factor: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2009). See also Claude Crépeau and Alain Slakmon, "Simple Backdoors for RSA Key Generation," in *CT-RSA'03: Proceedings of the 2003 RSA conference on the Cryptographers'* Track (Berlin: Springer-Verlag, 2003), 403–16; and Benjamin J. Romano, "Microsoft Device Helps Police Pluck Evidence from Cyberscene of Crime," *Seattle Times*, 29 April 2008, http://seattletimes.nwsource.com/html/microsoft/2004379751_msft law29.html.

36. See Foreign Intelligence Surveillance Act, Electronic Communications and Privacy Act, and Communications Assistance for Law Enforcement Act.

37. The crux of the argument made by those holding the opinion that states' sovereignty is at bay is that "the multinational corporation has broken free from its home economy and has become a powerful independent force determining both international and political affairs. [While] others [who] reject this argue that the multinational corporation remains a creature of its home economy." It follows that by the MNC breaking free from its home economy,

the sovereignty and autonomy of states are compromised. Those that disagree with the above claim argue that the MNC has not become fully independent from the home country but remains "a creature of the home country." Robert Gilpin, *Global Political Economy: Understanding the International Economic Order* (Princeton, NJ: Princeton University Press, 2001), 278.

38. Department of Commerce, *Management of Internet Names and Addresses,* 63 *Fed. Reg.* 31741 (1998).

39. Harold Kwalwasser, "Internet Governance," in *Cyber Power and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington: NDU Press, 2009), 491–524.

40. DeNardis, *Protocol Politics*, 11.

41. See, for example, M. Ford et al., "Issues with IP Address Sharing," Internet Engineering Task Force, Request for Comments: 6269, June 2011, http://www.hjp.at/doc/rfc/rfc6269.html.

42. Ingrid Marson, "China launches largest IPv6 network," *CNET News*, 29 December 2004, http://news.cnet.com/China-launches-largest-IPv6-network/2100-1025_3-5506914.html.

43. Sheila Frankel et al., *Guidelines for the Secure Deployment of IPv6* (Gaithersburg, MD: National Institute of Standards, December 2010).

44. Katherine Kebisek, "AFNIC prepares Air Force for IPv6 transition" Air Force Space Command, 4 April 2011, http://www.afspc.af.mil/news1/story.asp?id=123249968.

45. Indeed, one should recall that the World Wide Web, the commercial adaptation of the DARPAnet project, was a CERN (European Organization for Nuclear Research) initiative.

46. This agreement was renewed on 2 July 2012. See http://www.icann.org/en/news/announcements/announcement-2-09jul12-en.htm.

47. Robert E. Molyneux, *The Internet under the Hood: An Introduction to Network Technologies for Information Professionals* (Westport, CT: Libraries Unlimited, 2003), 86.

48. ICANN, "Memorandum of Understanding Concerning the Technical Work of the Internet Assigned Numbers Authority," 1 March 2000, http://www.icann.org/en/general/ietf-icann-mou-01mar00.htm.

49. Elihu Zimet and Edward Skoudis, "A Graphical Introduction to the Structural Elements of Cyberspace," in *Cyber Power and National Security*, 91–112. See also Molyneux, *Internet under the Hood*, 85–86.

50. Molyneux, *Internet under the Hood*, 27.

51. The Internet governance debates have a history of about a decade and certainly will continue past 2012. The next phase of the World Summit for the Information Society will occur in 2015.

52. H. Zhao, "ITU and Internet Governance—Input to the 7th meeting of the ITU Council Working Group on WSIS, 12–14 December 2004," http://www.itu.int/ITU-T/tsb-director/itut-wsis/files/zhao-netgov02.doc.

53. For a comprehensive discussion of the dynamics of Internet politics as they relate to the perceptions by foreign countries that ICANN control is a cyber security for all, see Panayotis A. Yannakogeorgos, "Cyberspace: The New Frontier and the Same Old Multilateralism," in *Global Norms, American Sponsorship, and the Emerging Pattern of World Politics*, ed. Simon Reich (New York: Palgrave, 2010).

54. The World Summit on the Information Society (WSIS) and its spin-off, the Internet Governance Forum (IGF), are the main venues where governments and all interested stakeholders debate the issues, determine the objectives, and determine principles surrounding the structure of the global information society. The first and second phases of the summit resulted in the *Geneva Declaration of Principles* and the *Tunis Plan of Action*, respectively.

[55] The ITU is the main entity tasked with organizing the WSIS. The High-Level Summit Organizing Committee was formed to "coordinate the efforts of the United Nations family in the preparation, organization and holding of WSIS." It was made up of a representative of the UN secretary-general and the executive heads of relevant UN specialized agencies. Other UN entities were included as observers. The ITU secretary-general served as the chair of this committee. One of its important functions was to "ensure that the contributions of the actors participating in the various conferences were comprehensively merged with the contributions from preparatory committees and regional meetings in a consensus document that would serve as the basis for the *Declaration of Principles* and *Plan of Action* of the WSIS."

[56] "UN ICT Task Force Global Forum on Internet Governance to be Held in March," UN press release, Paris, 13 February 2004, http://portal.unesco.org/ci/en/ev.php-URL_ID=14347&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html.

[57] "Global Internet Governance System is Working But Needs to Be More Inclusive, UN Forum on Internet Governance Told," UN press release, 26 March 2004, http://www.un.org/News/Press/docs/2004/pi1568.doc.htm.

[58] Ibid.

[59] "Statement by Mr. Dushyant Singh, Member of Parliament, on Agenda Item 16—Information and Communication Technologies for Development, at the 66th Session of the United Nations General Assembly on October 26, 2011," http://content.ibnlive.in.com/article/21-May-2012documents/full-text-indias-un-proposal-to-control-the-internet-259971-53.html.

[60] Yang Yu, Chinese response to "Further Notice of Inquiry on the Internet Assigned Numbers Authority Functions," China Organizational Name Administration Center (CONAC), http://www.ntia.doc.gov/files/ntia/conac_response_to_fnoi.pdf. CONAC is a nonprofit organization established in 2008. With the authorization of the State Commission Office for Public Sector Reform (SCPSR) and the Ministry of Industry and Information Technology (MIIT), CONAC runs the registry for ".政务.cn" (Government Affairs) and ".公益.cn" (Public Interest). CONAC also actively participates in the global Internet community.

[61] "Prime Minister Vladimir Putin meets with Secretary General of the International Telecommunication Union Hamadoun Toure," *Working Day*, 15 June 2011, http://premier.gov.ru/eng/events/news/15601/.

[62] UN General Assembly, "Enhanced Cooperation on Public Policy Issues Pertaining to the Internet," Report of the Secretary-General, http://unctad.org/meetings/en/SessionalDocuments/a66d77_en.pdf.

[63] Signed by 178 countries, the ITR is a global treaty applied around the world.

[64] Disclaimer: This is for informational use only. Any action undertaken by the reader of this article on the .onion domain is at his/her own risk, and this author is not liable for any harm caused by or to the reader.

[65] This is different from what Chris Demchak points to in "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 32–61, where the focus on sovereignty of the Internet is on access points of incoming Tier 1 ISP connections into the country and maintaining government control of those.

[66] US Department of State, "Internet Freedom Fact Sheet," 15 February 2011, http://www.state.gov/r/pa/prs/ps/2011/02/156623.htm.

[67] Spencer Ackerman, "Does Obama's 'Net Freedom Agenda' Hurt the U.S.?" *Wired*, 28 January 2011, http://www.wired.com/dangerroom/2011/01/does-obamas-internet-freedom-agenda -hurt-the-u-s-without-helping-dissidents/.

[68] Ye Tian et al., "China's Internet: Topology Mapping and Geolocating," http://cis.poly.edu/~ratan/topologymappingchinainternetshort.pdf.

Winter 2012

Virtual Patriots and a New American Cyber Strategy

Changing the Zero-Sum Game

Matthew Crosston

Most analyses on cyber deterrence draw a sharp distinction between the operational philosophy of the United States and that of authoritarian states like China and Russia. On the whole, they describe the difficulty of US efforts to maintain an effective cyber defense against brazenly offensive Chinese and Russian threats. This analysis takes an important contrarian position on this issue which has been relatively ignored: the cyber philosophy of China might offer the United States some useful insights. China's approach is more effective in ways that, for now, are apparently antithetical to the United States—amoral, overt, and proactive.

Whether Russian cyber nationalists or the Chinese Honkers Union, their guiding principles are clear: they are willing to defend their homeland through assertive and invasive techniques and will not limit their focus to defensive capabilities that only unevenly deter attacks. When defending the state from any perceived enemies—whether state, substate, or nonstate—establishing an offensive capability that instills fear is clearly a main agenda item within Russia and China. Part of this is based on their insecurities about a perceived kinetic imbalance with the United States and a willingness to be morally flexible when it comes to cyber-war norms. Arguably, the United States does not adopt a similar approach because of an apparent reluctance to mimic the policy of such distasteful regimes and an arrogance that does not concern itself with asymmetry. These stances undermine US national security.

Dr. Matthew Crosston is the Miller Endowed Chair for Industrial and International Security and founder and director of the International Security and Intelligence Studies (ISIS) program at Bellevue University. He has authored two books, several book chapters, and nearly a dozen peer-reviewed articles on counterterrorism, corruption, democratization, radical Islam, and cyber deterrence.

First, for clarification, it is necessary to parse out the so-called rogue cyber behavior of China and Russia. There are significant differences in the manner and philosophy with which the two states approach their cyber activities. China is seen as having a more "learnable" model that should creatively inspire the United States to alter and evolve its own cyber strategy to a level that would subsequently surpass the Chinese approach. Importantly, the purpose is not to copy Chinese cyber policy exactly, but rather to transform the characteristic of overt transparency into a US strategy of proactive cyber capability. This would infuse US security with a complex but capable new influence calculus where strategically overt means are used to further positive deterrence ends.

Ideally, this overt cyber strategy would create credibility in virtual weapons which employ disruptive cascading effects so powerful as to negate their use. The key would be in establishing plausible fear in the adversary. Some might argue there is limited utility in this approach because of the possibility that both China and Russia would fail to recognize the power of such a posture. Such logic subsequently declares virtual weapons do not have the same credibility as, say, nuclear weapons because the former have not achieved that level of credibility through actual usage or even testing. The efficacy evolution in cyber weaponry, however, helps support the main argument here. Given the recent revelations about Stuxnet and the effectiveness of the Duqu and Flame viruses—which quite possibly moved beyond the capabilities of Stuxnet—cyber weapons are rapidly obtaining that fearful reputation, and thus, deterrence via overt cyber strategy can no longer be considered pure fantasy.

This influence calculus turns current conventional wisdom on constraining norms within *jus in cyber bello* on its head. To date these constraints have shunned an overtly proactive US cyber strategy. A greater likelihood for peace across the global virtual commons is possible by using a strategy of facilitating restraint through fear. Please note, however, that *amoral* and *unethical* are not freely interchangeable in this analysis. For example, the Chinese may not view their cyber stances as unethical, while the United States does. The classically Machiavellian argument is that deep reflective discussions about morals and ethics should be suspended from the cyber domain if effective deterrence is to be achieved through overt strategy.

Finally, a cautious caveat: this is not an entreaty to abandon covert activities or secrecy. Rather, it is an important balancing argument for developing a fully encompassing strategy that allows both covert *and* overt US cyber power—an important evolution. It is not an argument against the need for classified operations. Simply, cyber strategy must be decoupled from a de facto zero-sum game. The building and elevating of overt cyber preemption does not take away from the relevance and reach of US covert cyber reactionary powers.

China and Russia: Cyber Cousins—Not Cyber Brothers

There seems to be a strong divergence in perception regarding China's desire to command cyberspace offensively. On the one hand is the assumption that this is a natural manifestation of its growing desire to achieve global superpower status. On the other hand is the counterargument that emphasizes China's own perception of its inability to operate effectively against the United States in a conventional military confrontation. Indeed, many Chinese writings suggest cyber warfare is considered an obvious asymmetric instrument for balancing overwhelming US power.[1] This latter argument is more compelling based on these stark military realities:

- In overall military spending, the United States spends between five and 10 times as much per year as China.
- Chinese forces are only now beginning to modernize. Just one-quarter of its naval surface fleet is considered modern in electronics, engines, and weaponry.
- In certain categories of weaponry, the Chinese do not compete. For instance, the US Navy has 11 nuclear-powered aircraft carrier battle groups. The Chinese navy only recently launched its first carrier, a refurbished Russian ship used solely for training.[2]
- In terms of military effectiveness (i.e., logistics, training, readiness), the difference between Chinese and US standards is not a gap but a chasm. The Chinese military took days to reach survivors after the devastating Sichuan earthquake in May of 2008 because it had so few helicopters and emergency vehicles.[3]

With this state of military affairs, China's perception of insecurity is not surprising. Even more logical is the Chinese resolve to grow its asymmetric cyber capabilities: such attacks are usually inexpensive and exceedingly difficult to precisely attribute. Attribution becomes even more complex for states where cyber attacks can be "launched" from neutral or allied countries.[4]

Given an authoritarian state's capacity for paranoia, it is illogical for China not to develop its offensive cyber capabilities. In this case, the weak conventional military strength is quite real. To that end, the People's Republic has endeavored to create its own set of lopsided military advantages in the cyber domain. To wit:

- The Pentagon's annual assessment of Chinese military strength determined in 2009 that the People's Liberation Army (PLA) had established information warfare units to develop viruses to attack enemy computer systems and networks.
- The PLA has created a number of uniformed cyber warfare units, including the Technology Reconnaissance Department and the Electronic Countermeasures and Radar Department. These cyber units are engaged on a daily basis in developing and deploying a range of offensive cyber and information weapons.
- China is believed to be engaged in lacing the network-dependent US infrastructure with malicious code known as "logic bombs."[5]

The official newspaper of the PRC, the *Liberation Army Daily*, confirmed China's insecurity about potential confrontation with the United States in June 2011. The Chinese government proclaimed that "the US military is hastening to seize the commanding military heights on the Internet. . . . Their actions remind us that to protect the nation's Internet security we must accelerate Internet defense development and accelerate steps to make a strong Internet Army."[6] Clearly, the Chinese have sought to maximize their technological capacity in response to kinetic realities. This is not to say the United States is therefore guaranteed to be in an inferior position (information about US virtual capabilities at the moment remains largely classified), but the overt investment, recruitment, and development of Chinese virtual capabilities presents opportunities the United States should also be willing to entertain.

How does all of this compare and contrast with the Russian approach to the cyber domain? Anyone studying cyber conflict over the last five years is well aware of Russia's apparent willingness to engage in cyber offensives. The 2007 incident in which the Estonian government was attacked and the 2008 war with Georgia are universally considered examples of Russian cyber technology as the tip of their military spear.

While it is true Russia actively encourages what has come to be known as "hacktivism" and lauds "patriotic nationalist" cyber vigilantism as part of one's "civic duty," there are still distinct differences with China.[7]

Much of Russia's cyber activity, when not in an open conflict, seems to be of the criminal variety and not necessarily tied directly into the state. Indeed, Russia seems to utilize organized crime groups as a cyber conduit when necessary and then backs away, allowing said groups continued commercial domination. Russia, therefore, almost acts as a rentier state with criminal groups: cyber weapons are the natural resource, and the Russian government is the number one consumer. This produces a different structure, style, and governance model when compared to China.

Table 1. Parsing cyber rogues

Category Breakdown	China	Russia
Purpose	Protectionist	Predatory
Psychology	Long-term/Rational	Short-term/Cynical
Style	Strategic	Anarchic
Governance Model	State-centric	Crimino-Bureaucratic

Purpose

China's purpose in developing its cyber capability seems motivated by protectionist instincts based largely on the perception that it is not able to defend itself against the United States in a straight conventional military conflict. Russia's purpose seems utterly predatory. This is no doubt influenced by the fact that most of the power dominating cyber capability in the Russian Federation is organized and controlled by criminal groups, sometimes independently and sometimes in conjunction with governmental oversight.

Psychology

The operational mind-set of China seems to be both long-term and rational. Its strategies are based on future strategic objectives and its position within the global community. Most if not all of China's goals in the cyber domain can be clearly understood in terms of rational self-interest. Russia's cyber mind-set is dominated by short-term thinking, largely motivated by the pursuit of massive profit and wielding of inequitable political power. Analyzing just how much of Russian cyber activity is in fact controlled by the desire for wealth leads to an overall impression of state cynicism.

Style

Chinese cyber activity is strategic in style. The state strives to control the cyber environment and maintain influence over all groups in the interest of the state. The Russian cyber atmosphere, unfortunately, resembles anarchy. The state engages criminal groups through an authority structure that is blurred if even existent. Consequently, there is little confidence that the Russian government exclusively controls its cyber environment.

Governance Model

It is clear that China's cyber governance model is state-centric. This may not be ideal for democracy, but it shows China does not allow competing authorities or shadow power structures to interfere with its national interests. Russia's cyber governance model is crimino-bureaucratic. It is not so much that the state is completely absent from the cyber domain in Russia, but rather the ambiguity of power and authority define the cyber domain. Russia may enjoy claiming the allegiance of its patriotic nationalist hackers, but it does not in fact tightly control its own cyber netizens, at least not in comparison to China.

While neither Russia nor China is afraid to use offensive cyber weapons, there are dramatic structural, motivational, strategic, and philosophical differences. Russia seems to embody a criminal-governmental fusion that has permeated the entire state apparatus. The cyber domain there is used for temporary forays to achieve state objectives and then returns to more permanent criminal projects. As such, it is not truly state-controlled, is relatively anarchic, and cannot establish any deterring equilibrium. China, on the other hand, may be the first state to truly embrace the importance of tech-war; it has realistically assessed its own kinetic shortcomings and looked to cyber for compensation. In short, it has fused Sun Tzu with Machiavelli—better to quietly overcome an adversary's plans than to try to loudly overcome his armies.

This analysis paints Russia in a relatively stark strategic light. While these differences do not give rise to a trusted alliance with China, the manner in which it approaches its cyber domain presents interesting new ideas about how the United States should approach the global cyber commons. These ideas would be in contrast to both academic literature and journalism, as they offer two completely divergent responses. On the one hand, the United States is not appropriately meeting this challenge, and on the other hand, it remains second-to-none in cyber offense.

The United States invests heavily in cyber security, and members of the intelligence community work to create cyber weapons meant to preserve US military predominance. However, there are still missed opportunities and weaknesses that have not been addressed or overcome by covert strategy. Namely, emphasizing covert and opaque cyber initiatives hinders the emergence of a global cyber strategy that could compel constraint without actually engaging in cyber attacks. Recall this is not about developing overt at the expense of covert. Rather, it is about ending the zero-sum cyber game to the strategic benefit of the United States. Up to now American virtual patriots have not been used for maximum impact and effectiveness. It would be wise to position offensive cyber capabilities for strategic, overt, preemptive purposes rather than as solely logistical, covert, reactionary weapons. This is a dramatic shift in strategic mind-set, arguing for a yin-yang approach toward the covert and overt aspects of cyber rather than the present view as a zero-sum game.

New Technology but not New Thinking

In 2004, the Congressional Research Service (CRS) issued a report on information warfare and cyber war. It discussed public policy oversight issues Congress should consider, including whether the United States should

- encourage or discourage international arms control for cyberweapons, as other nations increase their cyber capabilities;
- modify US cyber-crime legislation to conform to international agreements that make it easier to track and find cyber attackers;
- engage in covert psychological operations affecting audiences within friendly nations;
- encourage or discourage the US military to rely on the civilian commercial infrastructure to support part of its communications, despite vulnerabilities to threats from possible high-altitude electromagnetic pulse (HEMP) or cyber attack;

- create new regulation to hasten improvements to computer security for the nation's privately owned critical infrastructure; or
- prepare for possible legal issues should the effects of offensive US military cyberweapons or electromagnetic pulse weapons spread to accidentally disable critical civilian computer systems or disrupt systems located in other non-combatant countries.[8]

The CRS analysis focused on existing physical infrastructure and capacity. It did not explore new theoretical concepts that might achieve national interest more effectively. Most striking is the apparent assumption that the cyber domain will worsen in terms of political environment, as seen by the overreliance on cyber defensive systems. Such emphasis renders the US position reactive and late. The argument made here is for also pushing overt strategies based on devastating offensive capabilies that shift the US position into being more proactive, like China. Reactive policy simply *responds* to cyber attacks. Overt policy seeks to *deter* them.

The same CRS report highlighted the need for the Department of Defense (DoD) to achieve both decision and information superiority. This means a competitive advantage in the cognitive realm and one that enables the military to surprise an enemy.[9] Both of these advantages are best achieved with added front-end capability and not solely accomplished by reactionary policies. In short, there can be no dominant operational transfiguration without first a profound strategic transformation. An overt cyber strategy upfront makes proactive deterrence through fear more probable and gives the perception of decision and information superiority. Broadening the discussion to embrace a change in strategic mind-set greatly expands new potential deployment and deterrence options.

Many agencies within the US government have come close to espousing this transformation, only to fall short by demanding that US cyber capabilities remain exclusively covert. The National Security Agency has argued to better defend information networks by openly engaging both allies and adversaries in an open forum.[10] The Pentagon believes strongly in "active defense," which is, quite simply, cyber offense. The problem is that both remain strategically focused on *responding* to a major cyber attack through covert means. In other words, the same flaw found in the CRS report nearly a decade earlier still applies; the limited innovation remains reactive. If the United States continues to view the overt and covert aspects of cyber strategy as a zero-sum game rather than as yin-yang symmetry, then it will fail to realize its true cyber dominance.

A more disconcerting aspect of the discussion—at least for those who envision the cyber domain as a venue for instigating deterrence, not provocation—is that a capability used exclusively for covert activity becomes just another weapon among weapons. The point of maintaining total secrecy is due to the lethality of actual deployment. Any preemptive deterring power, therefore, is lost when kept covert. Remember, the argument here is not to abandon secrecy altogether; it is not about showing all the cards but voluntarily revealing some cards for strategic purposes. If the desire is to expand a capability's impact, not just in terms of winning wars but in preventing them, then overt strategy is a valuable tool.

Recall where Chinese cyber policy found its fundamental motivation: China's original intent was to deter other nations from pursuing more-traditional coercive policies. It also wanted to develop an advanced cyber warfare capacity that would allow it to asymmetrically challenge any potential adversary.[11] One must see Chinese cyber offensive strategy as a rational solution that is not simply cheap, but potentially capable of giving the United States pause before a large-scale conventional military engagement.[12] This kind of policy in US hands, focused by an overt offensive strategy, could transcend national interests and provide a framework for achieving greater cyber restraint at the global level. Keeping the aforementioned influence calculus in mind, it elevates above Chinese parochialism for the greater, more responsible global good of overt US cyber dominance.

Note this is not an entreaty to copy or mimic Chinese cyber policy. China itself does not formally admit to an explicitly overt strategic policy over the cyber domain. It is, however, undoubtedly proactive and offensive. By strategically allowing general knowledge about the existence of an offensive program and spreading the perception that it is willing to proactively use it, the United States has the opportunity to increase the fear-hesitancy of potential adversaries beforehand. In other words, adopting China's proactive policy and mutating it into something more overt and explicit (combined with superior US technological innovation and rule of law) can expand US cyber capability beyond its current covert, reactive roles. This is not an argument to disband covert action or remove reactive capacity. Rather, it is an admission that these two latter spheres simply do not equip the United States with an effective deterring cyber capability. Adding a proactive, offensive, overt "third strategic wheel" to this domain might do so.

The importance of this issue was confirmed by the head of US Cyber Command, Gen Keith Alexander, testifying before the House Armed Services Committee's Subcommittee on Emerging Threats and Capabilities in 2011:

> We believe that state actors have developed cyber weapons to cripple infrastructure targets in ways tantamount to kinetic assaults; some of these weapons could potentially destroy hardware as well as data and software. The possibilities for destructive cyber effects, having long been mostly theoretical, have now been produced outside of the lab and are proliferating into national arsenals and possibly beyond. . . . Segments of our nation's critical infrastructure are not prepared to handle this kind of threat.[13]

For those aware of the innate difficulty of cyber deterrence reactively keeping ahead of cyber attacks, this confession from General Alexander only makes it more compelling to allow discussion of a new overt mind-set in US cyber strategy that strives to prevent these deadly new weapons from being used. In some ways Alexander is close to this very conclusion but misses the final connection:

> We see frequent media reports on nations contemplating the creation of their own cyber commands. . . . *There is a rough, de facto deterrence at the strategic level of cyberspace. Although no one knows how a cyberwar would play out, even the most capable state actors seem to recognize that it is in no one's interest to find out the hard way.* This concern has led to a certain degree of restraint by states that we deem capable of causing very serious cyber effects (emphasis added).[14]

In developing offensive cyber weapons for overt strategic use, states make it known how devastating and cost-punitive a potential cyber strike would be. In essence, it is simply adjusting the general's vision—by making the costs of cyber war overtly explicit, it becomes every state's self-interest to engage in cyber restraint. Alexander intimates that such restraint has already developed to a certain degree because of the unknown fear (but clearly perceived assumption) that an all-out cyber war would be disastrous. As such, the most logical path is to try to intensify that perception through overt cyber strategy and thus raise restraint even more. The argument here seeks to answer the "why it matters" question and begin changing the original strategic mind-set. With such an argument in place, it will then be appropriate to broaden and deepen the project into blazing potential "how to" trails. This in fact makes analytical sense; namely, there can be no relevant "game planning" if the strategic state mind-set remains unaltered.

Is US Cyber Command already blazing that trail on its own? When considering the five strategic initiatives below, as detailed by General Alexander, it seems clear that it is not:

1. Treat cyberspace as a domain for the purposes of organizing, training, and equipping, so the DoD can take full advantage of its potential in military, intelligence, and business operations;
2. Employ new defense operating concepts to protect DoD networks and systems;
3. Partner closely with other US governmental departments and agencies and the private sector to enable a whole-of-government strategy and an integrated national approach to cybersecurity;
4. Build robust relationships with US allies and international partners to enable information sharing and strengthen collective security; and
5. Leverage the nation's ingenuity by recruiting and retaining an exceptional cyber work force and enable rapid technological innovation.[15]

There is nothing faulty or inappropriate with the above strategies. The issue is that the United States is not fully considering all the strategies available. US cyber policy remains too wedded to reactive defensive measures. When it considers proactive offensive measures more akin to Chinese strategy, they remain within covert operations. This is fine to facilitate the two goals of USCYBERCOM—to protect US freedom of action in cyberspace and to deny freedom of action in cyberspace to all adversaries—but it is not enough as a holistic strategy to achieve the desired change in the global cyber mind-set, where the use of cyber weapons becomes as abhorrent as using nuclear weapons.

The focus on possible cyber improvements should be strategic. Not all cyber initiatives must be reacted to in kind. Theoretically, it will always be possible to react to a cyber attack with, for example, a drone strike. Logistically, however, such reactions might be worse than the initial action. As such, while answering cyber with cyber should not be considered inevitable and exclusive, it could be the best strategic response in the end. This would be a loose inspiration from the Chinese example, where cyber often seems a preferred initiative over direct military maneuvers.

Perhaps partial explanation for this strategic flaw is that the United States does not have a healthy fear of kinetic asymmetry like China and Russia. Viewing kinetic asymmetry as "everyone else's problem," the United States could actually fall behind other states in terms of innovative cyber strategy. China's concern over conventional asymmetry clearly led to greater investment in proactive and offensive cyber measures. Since the United States does not worry about such asymmetry, it seems stuck on measures that are reactive, covert, and defensive. This overconfidence limits the potential reach and deterrent impact of a new US overt cyber strategy.

Leading cyber states excel at increasing the effectiveness of covert virtual weapons. The United States in fact is the prime leader. But it remains a poor representative in pushing forward an agenda of overt strategic cyber transparency where cyber becomes more about preemption and deterrence rather than inferior surprise and reaction.

Zero-Sum Game, Part I
The Strategic Power of Overt Transparency

The potential risks in cyberspace have always been on policymakers' minds. The stakes were made clear in the president's *National Cyberspace Policy Review*:

> With the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations . . . and individual rights. The government has a responsibility to address the strategic vulnerabilities to ensure that the US . . . together with the larger community of nations, can realize the full potential of the information technology revolution.[16]

Clearly, a constructive cyber environment—globally expansive in its positive conformity while limiting free riders and violators—is essential. Alas, the drive to create such an environment seems based on idealistic beliefs that do not conform to the real world. As stated by Mikko Hypponen at the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn in 2009, "in the end, it is just about good versus evil." The United States will not co-opt through paramilitary structures, like China, nor will it coerce through shadowy criminal networks, like Russia. So how does it motivate global cyber netizens to positive behavior? Apparently, this seems to rest on creating enough trust in states "doing the right thing."[17] Given the counterculture ethos of the cyber domain, this goal seems hyper-idealistic, if not outright irresponsible.

If the choice is between a system of deterrence based on idealistic governmental altruism or on a realist fear of retaliatory punishment and strategic first-strike restraint, the latter (again, loosely inspired by Chinese strategic thinking) is not only more easily achievable but also more effective. It would appear, however, that contemporary conventional wisdom does not agree. This is partially based on an attempt to force just war theory unchanged into the cyber domain and to misread what the rules of strategic cyber deterrence ought to be, as Randall Dipert notes:

> It is also true that Just War Theory, having been endorsed by most industrial democracies and in international law, has acquired the status of damage-minimizing convention. However, the increasing number of nations, especially non-Western ones, who show no serious effort to endorse or follow this convention—and the unwillingness of other nations to force compliance—means that the advantage of a widely accepted convention is lost; it merely handicaps nations with the developed public sense of morality and prevents them from moral intervention.[18]

This public sense of morality handicaps well-meaning nations, because they are trying to create compliance on the backend of a process, reactively and covertly, when such compliance is more likely when accompanied by an equal strategy on the frontend, proactively and overtly. Focusing on ethics, morals, and trust to motivate compliance in the cyber domain is irrational at the very least because of how easy it is to attack anonymously. Flipping this process and inverting the motivational stimuli produces a system of compliance independent of goodwill and ethical behavior: not purely defense, but offense; not purely covert, but overt; not purely reactive, but proactive; not hoping to inspire trust, but forcibly compelling fear. The cyber domain is not so different that the guiding principle of international relations cannot apply—fear plus self-interest equals peace. It is simply about realizing that covert and overt cyber activity function best not as zero-sum, but as yin-yang.

This idealistic normative thinking is even more dubious when the limitations of a so-called cyber cold war are supposedly elaborated:

> It is relatively clear what the reasonable (and thus moral) constraints on Cyber Cold War would be. There should be little targeting of strictly defensive computer control systems. There should be no attacks that disable or panic global financial or economic systems. There should be no power interference in the vital economic and security interests of a major power.[19]

These proposed behavioral rules about *jus in cyber bello* are paradoxical: with so many constraints on allowable action, the underlying motivational framework of fear—so essential in the original Cold War in moderating behavior—becomes nonexistent. Indeed, if the above parameters were observed, then a state could arguably be *more* motivated to attack. Remove the civilian population and domestic infrastructure from cyber attack, and you have sanitized cyber war to a point where there is no fear of engagement.

> A Cyber Cold War would be multilateral rather than bilateral: it would involve many nations, with different interests and not allied by treaty. Furthermore, the parties would include major non-governmental players such as private companies or even individuals or groups of individual hackers, perhaps with political interests. It is unlikely, in the more capitalistic and constitutionally free countries, that national governments can easily rein in these potential corporate and individual cyber attackers.[20]

The problem with this formulation is that it envisions a so-called cyber cold war beholden to apparently *voluntary* parameters of constraint. The parameters elaborated, however, do not honor but corrupt the true deterring force that existed in the Cold War. If an overt strategy of credible cyber debilitation were allowed to openly develop, then most of the problems mentioned above would be inconsequential to the proper functioning of the virtual global commons—multilateral or bilateral, individuals or groups, national governments or private corporations, clearly defined adversaries or anonymous, nonattributable attacks. A system that does not rely on arbitrary good behavior and instead proactively establishes overt cyber-weaponization strategies alongside continued covert capabilities creates an environment where the futility of first-strike efficacy and perceived retaliatory devastation rein in behavior globally.

The United States tends to be obsessive about keeping its technological capabilities classified. This is partially explained by the need to maintain effective surprise in retaliation to an attack rather than striving to prevent an attack initially. Yet, it is also explained by the US attempt to be the leading voice for liberally idealistic global cyber norms. This was confirmed in 2008 when former intelligence official Suzanne Spaulding testified before the House Cybersecurity Subcommittee.

> My concern is that (the Department of Defense) has been so vocal about the development and deployment of [classified] cyber-warfare capabilities that it will be very difficult for that department *to develop and sustain the trust necessary to undertake essential collaboration on defensive cybersecurity efforts* with the private sector and with international stakeholders. . . . There is significant risk

> that these vital partners will suspect that the collaboration is really aimed at strengthening our offensive arsenal (emphasis added).[21]

There are two problems with the above quote. On the one hand, policy makers continue to focus on apparent voluntary trust in a domain that is not typified by such behavior. On the other hand, the DoD remains steadfast in its worship of clandestine capability and thus loses the preemptive deterrence of overt strategy which can compel cooperation as opposed to just hoping for it. These are not small problems, as trust and collaboration between dangerous actors work when there is an element of consequence to poor action. An overt strategy of offensive cyber capability—revealing some cards while not revealing all, with no nod to ethical considerations that demand targeting constraints and a focus purely on the efficacy of preemptive deterrence—arguably has a chance to shine a light of consequence into the shadowy anarchy of cyber. This is how the United States, as mentioned at the beginning of this article, could be inspired by the essence of Chinese cyber strategy, but it must ultimately elevate to a higher capability and competence.

Further hindering this evolution, the academic community has remained too enamored with trying to connect ethical theories into the cyber domain to create a liberal, idealistic governing code. Many scholars have acknowledged that these theories, whether utilitarianism, Kantian theory, or natural rights theory, have cast relatively little new light into the cyber domain.[22] Despite such sincere if misguided efforts, the best possibility for preemptive cyber deterrence might be old-school strategic realism and not new-school ethical liberalism.

As awkward as it may be to admit publicly, the Chinese might have something for the United States to truly consider. A fusion of Sun Tzu's pragmatism with Machiavelli's overt strategic amorality carries the potential to deter negative cyber action before it ever begins. As Sun Tzu asserted, the highest realization of warfare is to attack the enemy's plans; next is to attack its alliances; next to attack the army; and the lowest is to attack its fortified cities. Machiavelli made it clear that if an injury has to be done to a man, it should be so severe that his vengeance need not be feared. This overt, amoral offensive fusion has one purpose: not to *logistically* conduct war but to *strategically* avoid it. At the present time there is no current discussion of US cyber strategy broaching these subjects, and subsequently, the zero-sum cyber game remains unchanged.

Zero-Sum Game, Part II
Cyber Domain and International Law:
Can Fear Be the Duty to Assist?

Unlike cyber crime, the international community has not achieved an agreed-upon consensus for cyber rules. This leaves existing international law no choice but to try to apply by analogy. While the application is not perfect, there are at least three general prescriptions to state conduct in cyberspace, according to law professor Duncan Hollis.

1. States must not launch a cyber attack that qualifies as a use of force absent UN Security Council authorization or pursuant to a state's inherent right to self-defense.
2. States must not employ cyber attacks within armed conflicts that violate the laws of war. States must avoid cyber attacks that target civilian objects, cause indiscriminate harm, or violate the rights of neutral states.
3. States must respect the sovereignty of other states in responding to any cyber attacks that do not constitute a use of force. . . . States cannot respond to cyber attacks directly if it would interfere with the sovereignty of another state.[23]

The most controversial argument here is the idea to purposely and openly violate the above three precepts, or at least create believability that such violation will occur, to instill the compelling credibility of fear. Such overt strategy can create compliance improvement when considering the duty to assist (DTA), as Hollis suggests, using a rescue-at-sea analogy.

> International law needs a new norm for cybersecurity: a duty to assist, or DTA. . . . As yet, there is no DTA for the Internet. But an SOS for cyberspace, an e-SOS, could both regulate *and* deter the most severe cyber threats. Unlike proscriptive approaches, a DTA would not require attribution to function effectively; those facing harm would not need to know if it came from a cyber-attack, let alone who launched it. A DTA would seek to redress unwanted harms directly, whatever their cause. It would do so by marshaling sufficient resources to avoid or at least mitigate that harm. If it does so effectively, attackers may think twice about whether it is worth the effort to attack at all (emphasis in original).[24]

The overall purpose of the DTA is correct: to deter the worst potential cyber behavior. It is by no means a false deterrence ploy; it is the rightful obligation of states to assist in an investigation not only to help, but also to improve their own trustworthiness and remove suspicion of complicity. The flaw, once again, comes in focusing on the backend of the process, seeking to reactively reduce harm. It uses the terms *deter* and *avoid*, but in actuality the DTA is truly centered on the terms *redress* and *mitigate*. An overt proactive cyber strategy is about deterrence and avoidance, which would make issues of redress and mitigation less necessary.

Hollis wanted to legally establish an e-SOS that would better deter cyber attacks by rendering states more resilient in the face of threats.[25] He is accurate in diagnosing the problem but is unable to connect to truly new strategy because of moralistic hand-wringing that restricts discussion to reactive and defensive measures of mitigation. In other words, the intellectual community has focused so exclusively on the aftermath of an attack that it basically does not consider the potential promise in overt, proactive strategies that might preempt attacks.

This becomes obvious when considering two concepts used in the law of armed conflict, reflecting the fundamental differentiation between principles that govern the legal decision to use force in international relations (*jus ad bellum*) and conduct/behavior during times of war (*jus in bello*).[26] Trying to seamlessly apply these principles to the cyber domain has proven consistently thorny.

> Both traditional elements of deterrence seem to be considered unsatisfactory for the purposes of cyber deterrence. . . . *Whilst cyber deterrence does not abandon the approach based on influencing potential adversaries' mind-sets, it will most likely have to rely on different methods to achieve this desired effect* (emphasis added).[27]

Changing the strategic mind-set of cyber thinkers requires one to recognize it is easier to leverage influence *before* conflict takes place than *after* hostilities have begun. The flaw is in the failure to connect higher-purpose ethical considerations to a harder strategic core; the argument is not that the United States must *never* consider the parameters and limitations in cyber war once underway. Rather it is about the need to address these concerns by enacting an overt strategy that can prevent cyber attacks. Perhaps one other reason this bridge-building has not been attempted is because of the general consensus that cyber weapons cannot be used for coercive purposes or do not instill fear as easily as nuclear weapons. But in reality, this might not matter.

Cyber Deterrence: Voodoo Magic or Simple Classic Realism?

Although the work of Martin Libicki is extremely well-known among cyber experts, a relatively little-emphasized point in a recent article that discussed the ability (or inability) of cyber war to have strategic impact is crucial here:

> If cyber war is going to assume strategic importance, it must be able to generate effects that are at least comparable to, and preferably more impressive than, those available from conventional warfare. . . . More to the point, for cyber to be a strategic weapon for coercive purposes, it has to be frightening to the population at large, or at least to the leaders—so frightening that the aggressors can actually read some gains from the reaction or concession of their targets. . . . It follows that if the use of cyber weapons is unimpressive at the strategic level, the fear that might come from the *threat* to use cyber weapons may be similarly unimpressive. . . . Nuclear arms fostered fear, but there was not a great deal of doubt or uncertainty in their applications. Cyber may be the opposite—incapable of inducing real fear directly, but putatively capable of raising the specter of doubt and uncertainty (emphasis in original).[28]

Libicki is right in how the fundamental debate is framed. So how can a new strategic line of thinking answer some of his concerns? Perhaps the inability of cyber to achieve true strategic importance is not based on its inability to instill fear, but rather the policy community's reluctance to cross the ethical Rubicon and consider a system whose aim is to achieve credibility in using real-time cyber lethality overtly. The goal is not to turn cyber weapons into some sort of voodoo magic. Rather, it is to fuse cyber weapons with classical realism, whether through propaganda or public testing. If the perception of a first cyber strike becomes irrational because of a "proven" retaliatory capability, then Libicki's legitimate concern about the credibility of cyber lethality will be surmounted. Overcoming this concern is essential, as it brings the deterring equilibrium of fear without having to engage in actual cyber war.

With a system that can at times overtly advertise these requisite skills, the United States would no longer need to convince adversaries of its omniscience or magic. Adversaries would only need to believe in rational self-interest that good behavior will avoid debilitation and bad behavior carries severe consequences. Ironic as it may seem, perhaps the key to developing this overt cyber strategy of preemptive deterrence, ensuring more reliable behavior across the virtual commons, comes about by being creatively inspired by an authoritarian state like China and adopting more strategically amoral rules of conduct in cyber war that so far have been relatively forbidden by the American scholarly community.

This is not to say the United States should do away with defensive efforts or covert weapons or cyber spies. Rather, it is an entreaty to allow American virtual patriots to employ offensive cyber capabilities for strategically overt preemptive purposes rather than solely as logistically covert reactionary weapons. This is not an argument against the relevance of the latter, but it is an explanation of how the former might lessen their need. The overt and covert aspects of US cyber strategy are better understood as yin and yang. They are not zero-sum. Change that strategic mind-set in the uniquely American ways discussed here, and US cyber dominance will be unchallenged for a long time to come. SSQ

Notes

1. Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4, no. 2 (Summer 2011): 1–24.

2. China's First Aircraft Carrier Enters Service," *BBC*, 25 September 2012, http://www.bbc.co.uk/news/world-asia-china-19710040.

3. James Fallows, "Cyber Warriors," *Atlantic* 305, no. 2 (March 2010).

4. Gunter Ollman, "Asymmetrical Warfare: Challenges and Strategies for Countering Botnets," in *Proceedings of ICIW 2010: The 5th International Conference on Information-Warfare & Security*, 509–14 (Reading, UK: Academic Conferences International, 2010).

5. George Patterson Manson, "Cyberwar: The United States and China Prepare for the Next Generation of Conflict, *Comparative Strategy* 30 (April–June 2011): 122–33.

6. Don Reisenger, "Chinese Military Warns of US Cyber Threat," *cnet.com*, 16 June 2011, http://news.cnet.com/8301-13506_3-20071553-17/chinese-military-warns-of-u.s-cyberwar-threat.

7. Scott D. Applegate, "Cyber Militias and Political Hackers—Use of Irregular Forces in Cyberwarfare," *Security & Privacy* 9, no. 5 (September/October 2011): 16–22, http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=6029351.

8. Clay Wilson, *Information Warfare and Cyberwar: Capabilities and Related Policy Issues* (Washington: CRS, 19 July 2004), "Summary."

9. Ibid., 3.

10. Fallows, "Cyber Warriors."

11. Manson, "Cyberwar."

12. Hjortdal, "China's Use of Cyber Warfare."

13. Gen Keith Alexander, "Building a New Command in Cyberspace," *Strategic Studies Quarterly* 5, no. 2 (Summer 2011): 5.

14. Ibid., 7.

15. Ibid., 8.

16. Quoted in Col James Cook, "Cyberation and Just War Doctrine: A Response to Randall Dipert," *Journal of Military Ethics* 9, no. 4 (December 2010): 411–23.

17. Alexander Klimburg, "Mobilising Cyber Power," *Survival* 53, no. 1 (February/March 2011): 41–60.

18. Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 4 (December 2010): 394.

19. Ibid., 403.

20. Ibid.

21. Suzanne Spaulding, quoted in Shaun Waterman, "US Needs Cyber-offensive," *Space War*, 29 September 2008.

22. Giles Trendle, "Cyberwars: The Coming Arab E-Jihad," *Middle East*, issue 322, April 2002.

23. Duncan B. Hollis, "An e-SOS for Cyberspace," *Harvard International Law Journal* 52, no. 2 (Summer 2011): 393–95.

24. Ibid., 378.

25. Ibid., 426–29.

26. Ulf Haeussler, "Cyber Strategy and the Law of Armed Conflict," in *Proceedings of ICIW 2011: The 6th International Conference on Information-Warfare & Security* (Reading, UK: Academic Conferences International, 2011), 99–105.

27. Ibid.

28. Martin Libicki, "Cyberwar as Confidence Game," *Strategic Studies Quarterly* 5, no. 1 (Spring 2011): 135–37.

Spring 2013

Energy Insecurity

The False Promise of Liquid Biofuels

CAPT T. A. "Ike" Kiefer, USN

Some prominent arguments appear almost daily in the media that biofuels will increase our domestic supply of transportation fuel, end our dependence on foreign oil, reduce military vulnerabilities on the battlefield, and generally improve national security. Biofuels are further touted to reduce fuel price volatility, polluting emissions, and greenhouse gases (GHG) and even stimulate the economy. These arguments all fall apart under scrutiny. The promise and curse of biofuels is that they are limited by the energy that living organisms harvest from the sun and suffer a fatal "catch-22": uncultivated biofuel yields are far too small, diffuse, and infrequent to displace any meaningful fraction of US primary energy needs, and boosting yields through cultivation consumes more energy than it adds to the biomass. Furthermore, the harvested biomass requires large amounts of additional energy to convert it into the compact, energy-rich, liquid hydrocarbon form required for compatibility with the nation's fuel infrastructure, transportation sector, and especially the military. The energy content of the final-product biofuel compared to the energy required to produce it proves to be a very poor investment, especially compared to other alternatives. In many cases, there is net loss of energy. When energy balance (energy output minus energy input) across the full fuel creation and combustion lifecycle is considered, cultivated liquid biofuels are revealed to be a modern-day

The author gratefully acknowledges Randall Rush, Charles Hall, Paul Wagonner, James Bartis, Jesse Ausubel, Tim Garrett, Thomas Homer-Dixon, Freeman Dyson, Andrew Marshall, David Pimentel, Tad Patzek, Jason Hill, Wayne Henson, Peter Brabeck-Letmathe, and Tom Elam for their contributions to his understanding of the issues discussed herein. Any errors are the author's alone.

CAPT T. A. "Ike" Kiefer, USN, is a naval aviator and EA-6B pilot with seven deployments to the CENTCOM AOR and 21 months on the ground in Iraq. He has a bachelor's degree in physics from the US Naval Academy and a master's in strategy from the US Army Command and General Staff College. He currently teaches strategy at the USAF Air War College as the CJCS Chair.

attempt at perpetual motion that is doomed by the laws of thermodynamics and a fatal dependence on fossil fuel energy. The United States cannot achieve energy security through biofuels, and even the attempt is ironically achieving effects contrary to "clean" and "green" environmental goals and actively threatening global security.

This article focuses on cultivated biomass converted into liquid transportation fuel, and all references to *biofuels* throughout refer to these circumstances unless specified otherwise. The overall approach is an analysis of alternatives comparing three distinct biofuels methodologies with conventional petroleum fuel to assess their relative costs and benefits. It begins by considering what energy security means in terms of fuel quality and supply, then builds an analytical framework of key parameters and evaluates how each of the biofuel methodologies fall short. Next it provides evidence that pursuit of biofuels creates irreversible harm to the environment, increases greenhouse gas emissions, undermines food security, and promotes abuse of human rights. The article concludes with specific recommendations for policy and action.

Energy Security

The ability of biofuels to truly substitute for petroleum fuels is the core question addressed here. The US Congress has authoritatively defined *energy security* in Title 10 of the US Code as "having assured access to reliable supplies of energy and the ability to protect and deliver sufficient energy to meet mission essential requirements."[1] In 2011, the United States imported 45 percent of its petroleum, and this generates concern because of US dependence on other nations for supply and unpredictable global market price volatility.[2] If a way existed to reliably supply US transportation energy exclusively from domestic sources with reasonable and stable prices, it would clearly enhance energy security.

An Appeal to Science over Politics

This research is based on an extensive literature survey of recent and reputable sources emphasizing US government agency data published in official reports and university studies published in peer-reviewed scientific journals. Since 2008, a new generation of more rigorous studies has dramatically undermined the naïve assumption that biofuels are inherently clean and green, carbon-neutral, and the world's solution to petroleum dependence. But these watershed scientific documents have so far had little impact on US government or military energy policy. The US Navy directly rejected a RAND study conducted at the direction of Congress and delivered to the secretary of defense in January of 2011 that unambiguously found biofuels of "no benefit to the military."[3] A second RAND study and a report by the US National Academy of Sciences, both severely questioning the wisdom and efficacy of current US biofuels policies, also resulted in no adjustments to US biofuels programs.[4] In August 2012, the German National Academy of Sciences, in a country very aggressive in its pursuit of alternative energy, released the report of a three-year study that concluded biofuels offer little or no benefit in reducing GHG emissions and that "the larger scale use of biomass as an energy source is not a real option for countries like Germany." The German scientists even went so far as to flatly recommend all of Europe abandon biofuel production mandates.[5] In October 2012, the National Research Council released a report which critically questioned the feasibility of sustainable production of algae-based biofuels and highlighted five areas of major concern that parallel and support arguments made in this article against all cultivated biofuels.[6] These are but a few of the studies that point out fatal flaws in pursuing biofuels as a substitute for petroleum. There are several key parameters that, when understood, help to evaluate the utility of fuels and the costs and consequences of their production and use.

The Science of Fuels

The energy carriers in fossil fuels and biofuels are hydrogen and carbon atoms. Hydrogen is abundant, is very reactive in accepting and releasing energy in its chemical bonds with other atoms, and is the lightest element, giving it a very high *gravimetric energy density* (joules per kilogram). Pure hydrogen powers everything from microorganisms to turbine engines.[7] Carbon is another common and lightweight element with very high combustion energy. It also readily forms long molecular chains and can serve as a backbone to organize many other atoms into dense and neatly organized packages. Combined with hydrogen in equal parts, it forms highly versatile and energetic liquid fuels. Carbon transforms hydrogen from a diffuse and explosive gas that will only become liquid at -423° F into an easily handled, room-temperature liquid with 63 percent more hydrogen atoms per gallon than pure liquid hydrogen, 3.5 times the *volumetric energy density* (joules per gallon), and the ideal characteristics of a combustion fuel.[8] If we did not have carbon, we would have to invent it as the ideal tool for handling hydrogen.

In 1909, Fritz Haber discovered the chemistry of converting natural gas into ammonia (i.e., converting fossil fuel into plant fuel). Ammonia (NH_3) is a potent organic fuel for most bacteria and plants which have the ability to metabolize its nitrogen and hydrogen energy.[9] Placing ammonia in the soil to fuel plant growth is known as "nitrogen fixing."[10] It can be done naturally and slowly by symbiotic soil and root bacteria using photosynthesis energy borrowed from their host plant, or it can be done artificially and quickly by humans manufacturing it and plowing it into the soil.[11] The manufacture of ammonia is second only to plastics in consumption of US industrial energy, and 80 percent of ammonia goes into making fertilizer.[12] Today, Iowa farmers pump pure liquid ammonia into the soil at the rate of 150–200 lbs/acre[13] to harvest consecutive annual crops of 160–180 bushels per acre of corn—a sixfold increase over historical yields.[14] It is largely because of the global conversion of fossil fuel energy into food that the world has avoided Robert Malthus' 1798 prophecy of global famine from population growth overtaking food production.[15]

Without the addition of artificial fertilizer energy, plants are limited to getting their energy from the sun. The devastating limiting factor for all biofuels is that photosynthesis captures solar energy with surprisingly poor speed and efficiency—only about 0.1 percent of sunlight is translated into biomass by the typical terrestrial plant,[16] and this translates into an anemic *power density* of only 0.3 watts per square meter (W/m^2).[17] This is 20 times worse than the 6.0 W/m^2 that current solar panels arrayed in large farms can collect from the same sunlight and acreage.[18] Humans must input fossil fuel energy in the form of ammonia fertilizers to overcome this solar limit on biomass production for crops. While this is a justifiable option to increase food production, it makes no sense to add energy to something that is supposed to be an energy source such as biofuel crops. It is also nonsensical to add fossil fuel energy when the objective is to *displace* fossil fuel energy.

A perfect combustion fuel possesses the desirable characteristics of easy storage and transport, inertness and low toxicity for safe handling, measured and adjustable volatility for easy mixing with air, stability across a broad range of environmental temperatures and pressures, and high energy density. Because of sweeping advantages across all these parameters, liquid hydrocarbons have risen to dominate the global economy. No materials other than very exotic and toxic substances like lithium borohydride ($LiBH_4$) or expensive rare metals like beryllium surpass the energy density of diesel and jet fuel. Biodiesel and ethanol both fall short. Hydrogen fuel cells, electrical storage batteries, and capacitors miss by a much greater margin. Other alternatives, such as wind, solar, geo-thermal, or waste-to-energy devices, can power some laptops and light some fixed facilities but simply cannot harvest enough energy to propel the tanks, jets, helos, and trucks that are by far the major battlefield fuel consumers. These can offer only an incidental decrease in overall fuel requirements for mechanized forces and then only in low-hostility circumstances where they can be set up and safeguarded.

In addition to inorganic and organic chemistry, an energy strategist must understand two unbreakable laws of the universe. The first law of thermodynamics (conservation) states that energy is neither created nor destroyed, but only changes form. The second law (entropy) distinguishes between useful energy that can perform work and useless energy that cannot. It holds that some fraction of useful energy irreversibly becomes useless every time energy is converted from one form to another. In other words, any conversion process consumes some of the useful energy and leaves less in the output products. Together, these two laws declare that the amount of useful energy that can be recovered from a system is always less than the energy that was put into the system. Every transaction, process, or conversion pays an energy tax, which is why it is impossible to construct a perpetual motion machine. The ratio of energy-out to energy-in is a critical parameter in evaluating energy sources.

Energy Return on Investment

For energy strategists to get the right answers, they must first ask the right questions. When choosing a primary energy source and a fuel to derive from it, it is essential to be sure the fuel will meet the demands of the civilization that will consume it—not only in terms of quantity, but even more fundamentally, in terms of quality. One key measure of fuel quality is how much useful energy the fuel yields divided by how much energy is required to extract the primary energy source from the environment and convert it into that fuel. This metric is known as *energy return on investment* (EROI).[19]

$$\text{EROI} = \frac{\text{Energy available in newly produced fuel}}{\text{Energy consumed in producing the new fuel}}$$

Raw primary energy sources require some energy to be consumed to process them into finished fuels. An EROI of 1:1 would mean the useful energy in a newly produced quantity of fuel is exactly equal to the energy consumed in its production. It might seem that any EROI greater than unity is of net benefit to civilization, but this is not the case. A modern civilization requires a much greater return on its investment, because survival and standard of living depend upon the size of this margin.

Civilization Is a Living Organism

Dynamic energy budget (DEB) theory is a sophisticated approach to looking at living things in terms of energy.[20] A thermodynamic analysis reveals that any organism can only afford to expend a small fraction of its current energy stores finding and processing new primary energy sources into fuel (*assimilation*) because there are many other essential energy-consuming (*dissipation*) tasks it must perform to survive; these include sustainment, repair, protection, maturing and increasing in complexity, and reproduction. Only if there is surplus energy after all of these demands are fully satisfied will the organism increase its mass (*growth*). To power all these activities, the organism needs food that is not just fractionally positive in net energy, but rather has an EROI many multiples greater than unity. A civilization is itself a high-order physical and biological organism that has tremendous overhead costs and can spare only a fraction of its energy to assimilate new energy.

Minimum EROI for Modern Civilization

A study of historical US economic performance over the last century has found that economic recessions are linked to primary energy EROIs dipping below a critical threshold of 6:1.[21] This value represents the minimum energy quality an industrial civilization must have to sustain a modern, energy-intensive quality of life. Another macroanalysis found that an EROI of 3:1 is the bare minimum quality a raw energy feedstock must have to overcome all the production costs and conversion losses and still deliver positive net energy to modern civilization.[22] A 3:1 EROI thus also represents a critical tipping point. To put these values in biological terms, a modern industrial civilization is very energy-hungry, and if undernourished on a diet of foods with lean EROIs below 6:1, it becomes catabolic, eating into the fat of its savings and the muscle tissue of its infrastructure to replace the missing calories. As long as EROI remains below 6:1, industrial civilization is locked into a death spiral where an ever increasing fraction of its economic output (GDP) is spent on energy at the cost of eroding standard of living.[23] At EROIs below 3:1, the food is so poor that digesting it into fuel takes more energy than it returns, and full starvation sets in. The only way out of this hunger trap is either to find higher-EROI energy or to decay into a preindustrial civilization with lower energy needs.

The bottom line is that a healthy modern economy must be fed by hearty primary energy sources with a collective EROI above 6:1. Purposely displacing high-EROI energy sources with anything that returns less than 6:1 is ill advised. Plotting out fuel EROI estimates versus their current energy contribution to the US economy provides a useful perspective on their relative utility (fig. 1). [24]

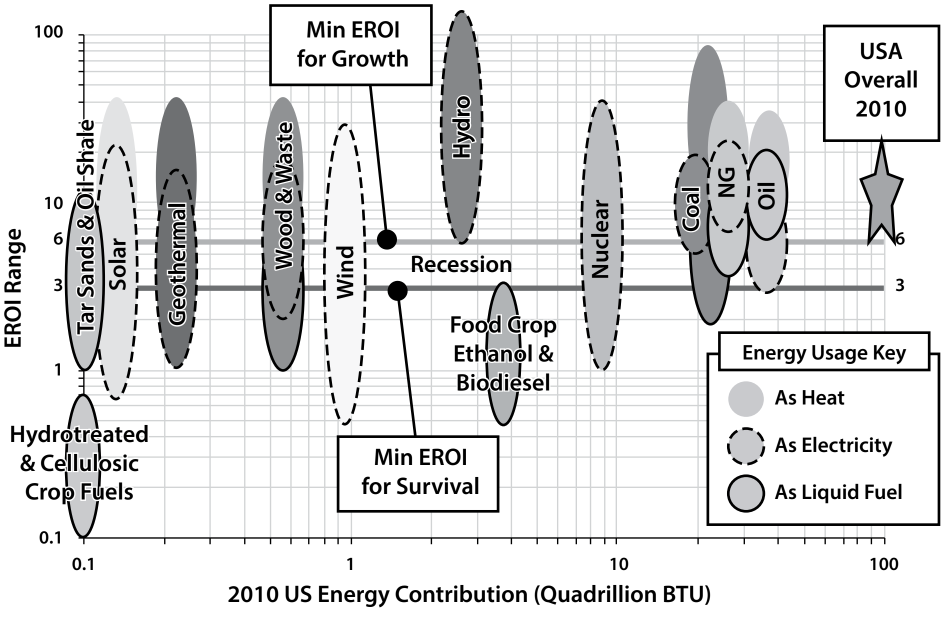


Figure 1. Energy return on investment (EROI) of US energy sources

Evaluating Biofuels

Food Crop Ethanol

Over the past 70 years, the United States has nearly perfected corn as a high-yield food and industrial starch feedstock. Unfortunately, the laws of physics exact large energy tolls from processes that require many conversions, such as producing liquid fuels from solid biomass. After decades of study and experimentation and continuously refined commercial production, the scientific literature consensus for corn ethanol EROI is a lowly value of 1.25:1.[25] Even worse, there is no net gain in liquid fuel energy—the ethanol produced contains energy barely equal to the input fossil fuel energy. The small energy profit is contained in byproducts, principally high-protein biorefinery leftovers called distillers' dry grains and solubles (DDGS) that can be used as cattle feed. More than $6 billion a year in direct federal assistance to corn growers and ethanol refiners since 2005 has served only to reduce a nonexistent foreign dependence on animal feed protein supplements.

It should be pointed out that the corn ethanol EROIs published in the literature and discussed above are not for a pure corn ethanol lifecycle, but for a hybrid lifecycle involving both fossil fuel and corn ethanol where fossil fuel provides much of the input energy. A proper corn ethanol EROI would be calculated using corn ethanol as the exclusive energy source to make more corn ethanol, but no example is available today. This is telling. It will be shown below by lifecycle analysis that making corn ethanol is a negative energy-balance process that consumes more than five-sixths of the energy invested. Civilization would get six times more output energy from the fossil fuel diverted to make corn ethanol if it were instead used directly as fuel.[26]

Modern intensively farmed corn, with its huge appetite for fossil fuel–based ammonia and agrichemicals, is making a large, net negative contribution to the nation's energy budget and working to increase rather than decrease petroleum demand. Using biomass to replace fossil fuels is futile if a large portion of the energy invested to make them is *from* fossil fuel. Applying ammonia fertilizer to any crop intended for biofuel is an indefensible waste of energy.

Cellulosic Ethanol

The facts are even less kind to liquid fuels made from cellulosic materials such as wood, switchgrass, and harvest wastes, which contain no easy sugars and starches. Cellulose can be broken down into fermentable sugars but must first be separated from the lignin. Paper manufacturers use concentrated acid and explosive steam treating known as the "Kraft process." However this one step alone consumes as much energy as exists in the final ethanol. Those who want to make energy out of lignocellulose must use much slower and more expensive enzyme or microbial processes; and then still remains fermentation, distillation, and dehydration. A rigorous thermodynamic analysis found that cellulosic ethanol is three or more times more difficult to produce than food crop ethanol, with an EROI far below 1:1.[27] However, a much-touted USDA study that assumed away many of the known difficulties and costs to predict a fanciful EROI for switchgrass of 5.4:1 (four times better than corn ethanol) has been used to justify spending billions of dollars in federal and private funds on some high-profile entrepreneurial misadventures.[28] Nevertheless, the proof is in the performance.

Despite all the subsidies, tax breaks, and fuel-mixing mandates since 2005, there is not a single commercially viable cellulosic ethanol facility in the United States today.[29] Rather, the landscape has been rocked by high-profile frauds and failures, such as Cello and Range Fuels.[30] Instead of the 500 million gallons of cellulosic ethanol a year by 2012 promised by huge federal expenditures on startups and biorefineries,[31] the Environmental Protection Agency (EPA) officially counts only one 20,000-gallon commercial transaction to date to an undisclosed buyer.[32] Nevertheless, the EPA continues to fine US oil refineries for not mixing nonexistent cellulosic ethanol into their gasoline.[33] Some of the companies that have been working on cellulosic ethanol the longest—such as Gevo, Amyris, and Cellana—have shifted to corn ethanol, industrial chemicals, and fish food.[34] British Petroleum and others have suspended construction of huge biorefineries in the United States.[35] Other companies such as Coskata and Primus Green Energy are quietly leading a mass migration away from any pretense of renewable fuels to instead boldly embrace synthetic liquid fuels made from natural gas.[36] The former CEO of Codexis, who presided over the spending of $400 million in pursuit of cellulosic ethanol, has publically confessed that making hydrocarbons from carbohydrates is a dead end. He is now at Calysta working on natural gas–to–liquid fuel.[37]

Biodiesel

Plant species which yield some biomass as lipids include soy, camelina, rapeseed, oil palm, jatropha, peanut, sunflower, cottonseed, safflower, and microalgae. All of these crops, including a nonpoisonous Mexican variant of jatropha, have provided human and animal food over the centuries. The natural lipids in these plants can be broken down by adding methanol to become fatty-acid methyl esters (FAME), commonly known as *biodiesel.* Contrary to popular belief, biodiesel is a very different chemical cocktail than conventional diesel fuel and has a lower energy density and inferior physical properties. To overcome biodiesel and other liquid biofuel shortcomings and make them more compatible with existing fuel infrastructure and high-performance engines, they must be transformed into true "drop-in" hydrocarbons by a series of processes, known as "hydrotreating," that increase the ratio of hydrogen to carbon, remove all oxygen, and change the structure and blend of the constituent molecules.[38] Hydrotreatment greatly increases the cost and reduces the renewable nature of the fuel, because the hydrogen added comes from fossil-fuel natural gas and the process releases 11 tons of CO_2 for every ton of hydrogen added. A national security energy strategist must understand such technical details as these and also be aware that all military aircraft and combat vehicles and civilian airline fleets must have hydrotreated biofuel. Even before being punished by hydrotreatment, biodiesel EROIs calculated from rigorous, full commercial-scale lifecycle studies range from 1.9:1 for soy[39] down to well below 1:1 for microalgae.[40]

Algae is the only biodiesel crop with high-enough potential yields to replace petroleum without consuming all US territory and deserves further consideration. Optimistic studies have projected algae biodiesel to achieve much higher EROIs, but a critical analysis of their assumptions reveals they depend on a host of unrealistic circumstances. These include massive supplies of free water and nutrients, a free pass on enormous environmental impact, and market economics that miraculously transform enormous accumulations of soggy biomass byproduct with a per-ton value less than the cost of transportation into a cash commodity crop. A literature survey of reported algae EROIs performed by the National Research Council found values from 0.13:1 to 7:1, but in the higher cases, energy credits from co-products dwarfed the energy delivered as liquid fuel—biodiesel was really the co-product and solid biomass the product.[41] Algae are much more efficient in producing "soylent green" than in producing green fuel. Proponents often claim that algae need only sunlight and CO_2 to grow. In practice, however, the need for high yields compels use of fossil fuel–based commodity fertilizer typically delivered as urea.[42] Solazyme Inc., the US Navy's choice for algae biofuel, actually grows its product in dark bioreactors using carbon and hydrogen energy in the form of sugar. This makes it unique in producing a biofuel 100 percent dependent upon a food crop and getting 0 percent of its energy from the sun via direct photosynthesis—a worst-case scenario.[43]

The simple but decisive math is that, even at commercial scale with generous assumptions about cellular reproduction rate and lipid fraction and oil extraction, and ignoring the costs of facilities and water, Argonne National Laboratory has calculated that it takes 12 times as much total energy and 2.6 times as much fossil fuel energy to put a gallon of algae biodiesel in a gas station pump instead of a gallon of petroleum diesel—and this is before hydrotreatment.[44] Direct comparison of alternatives is a sound evaluation technique and introduces the important economic concept of *opportunity cost*.

Fuel Lifecycles and Opportunity Cost

Not only should new fuels have an EROI greater than 6:1, they should also have an EROI greater than available alternative fuels suitable to the same purpose. If they have a lower EROI and their use is compelled, production will sap energy from higher EROI fuels and create an energy deficit to the economic sector they serve.[45] This can be demonstrated by comparing petroleum fuels to corn ethanol. Current petroleum diesel and gasoline production EROIs are variously estimated between 10:1 and 20:1. A conservative approach least favorable to petroleum is to postulate an 8:1 EROI, which represents the lowest value calculated since 1920.[46] An 8:1 EROI means that one barrel of liquid fuel energy input can support the exploration, drilling, extraction, and refining of enough crude oil to make eight new barrels of liquid fuel energy[47]—which for petroleum happens to come with a bonus of one barrel of chemical feedstock for plastics, lubricants, organic compounds, industrial chemicals, and asphalt (see fig. 2).[48] The much lower 1.25:1 EROI of corn ethanol means that to produce the same net gain of eight barrels of energy requires *not one, but 32 barrels* of input energy. And for ethanol, the output energy profit is delivered not as liquid fuel, but as 5.5 tons of cattle feed co-product. The 52 barrels of lower energy density, lower compatibility, and more corrosive ethanol produced as the primary product contain just enough energy to make up for the 32 barrels of fossil fuel energy used to make them and deliver no net energy gain. This picture looks completely different than the one in biofuels advocacy literature because it shows true lifecycle and opportunity costs, not just a misleading combustion-only comparison of a barrel of oil versus a barrel of ethanol.

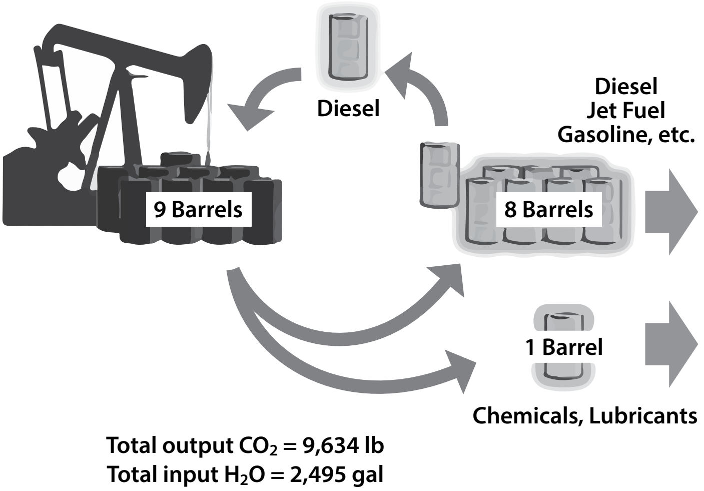
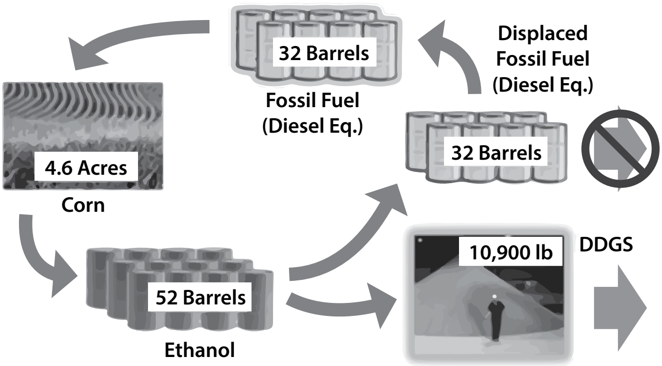


Figure 2. Petroleum motor fuel lifecycle at 8.0:1 EROI

Biofuels can only truly substitute for petroleum fuels when the EROIs of both converge, and this cannot happen if the former is an energy parasite of the latter. The parasitic dependence of biofuels upon fossil fuels precludes any chance of their reducing dependence on foreign oil, assuring domestic supply, or stabilizing prices. Liquid biofuel prices are already as volatile as oil prices and track up and down with the international oil market.[49] Deriving fuel from farming further increases price volatility by adding an additional linkage to global agricultural commodities markets. Energy security is reduced by choosing a fuel subject to floods, freezes, and droughts, and which must be recreated annually from scratch with no proven reserves.

To summarize the corn ethanol fuel lifecycle depicted in figure 3, it is the transformation of 4.7 tons (180 gigajoules) of high-quality fossil fuel and 11,000 tons of fresh water into 7.2 tons of lower-quality ethanol fuel-additive (180 gigajoules) and 18.5 tons of CO_2-equivalent, all for the net creation of 5.5 tons of protein supplement.[50] From the perspective of opportunity cost, one barrel of fossil fuel energy can either deliver 340 pounds of DDGS or 2,200 pounds (336 gallons, 1 metric ton) of petroleum fuel. The much more efficient and economical path to generate high-protein animal feed supplement chosen by US farmers in the absence of ethanol subsidies is growing soy, which fixes its own nitrogen and has 49 percent protein content vice 27 percent for DDGS.[51] Compared to the petroleum fuel lifecycle (fig. 2), the corn ethanol fuel lifecycle (fig. 3) consumes 3.5 times more fossil fuel, more than triples GHG emissions, increases water use by three orders of magnitude, adds environmental costs from agrichemical runoff while still suffering those associated with crude oil, and competes with food cultivation for cropland acreage and associated agricultural production capital and resources.



Total output CO_{2e} = 37,120 lb (3-fold increase)
Total input H_2O = 2.7M gal (1,000-fold increase)

Figure 3. Corn ethanol motor fuel lifecycle at 1.25:1 EROI

Closer examination reveals how intractable is biofuels' dependence on fossil fuel energy. Fossil fuels provide 82 percent of all US energy, including the vast majority of electric power and 94 percent of liquid transportation fuel.[52] They provide the farm machinery fuel and processing plant heat and electricity used to make biofuels from biomass. Petroleum and natural gas are also the feedstock for the massive organic chemical industry that makes the herbicides and pesticides applied to biofuel crops and the designer enzymes used in the latest high-technology approaches. The energy to prepare the giant yeast and microbe cultures that ferment the sugars into alcohol and the immense heat needed to distill the 4 percent alcohol beer into 99.5 percent pure anhydrous ethanol are overwhelmingly supplied by fossil fuel. Of course the energy used to build the biorefineries in the first place and to transport the final product to market is largely from fossil fuel as well. Some might argue that all of the above is only true because biofuels have not yet gained enough of a market share to provide these energies. However, the truth is that biofuels have been around for a century (the first US commercial cellulosic ethanol plant was opened in 1910)[53] but have failed to gain market share because they are a poor energy investment. They are crippled by the thermodynamic energy losses of all the transformations involved from making a low-energy-density, solid carbohydrate into a high-energy-density, liquid hydrocarbon. If they were used to provide the energy for their own manufacture, or even allowed to compete without subsidies, there would be little if anything profitable left at the end to market.[54]

Every fuel with an EROI less than the prevailing average drags down the average and multiplies rather than eases the burden placed on higher EROI fuels. The only way to displace imported petroleum use and thereby improve national security is to domestically produce fuels with higher EROI than refined petroleum. Any such fuel will be instantly adopted because the evidence of its higher EROI will be a lower price.[55] Without petroleum or a replacement source for massive quantities of hydrogen to make ammonia, all biomass yields, particularly food, will plummet toward what they were before Haber's monumental discovery in 1909, with devastating consequences for the world.[56] Accelerating the use of petroleum by using it to make biofuels accelerates future scarcity, undermines international food security, is counterproductive to "green" energy goals, and is not sound energy strategy.

The Real Cost of Biofuels

The Military's Cost

One of the core goals of the DoD's new *Operational Energy Strategy* is to reduce military energy costs so the department can "shift resources to other warfighting priorities, and save money for the American taxpayers."[57] The civilian leaders of the US Navy quote the statistic that a $1 rise in the cost of a barrel of oil increases annual fuel costs by $31 million.[58] Yet, the cheapest price the Navy has paid for any biofuel to date is $1,123.50 per barrel.[59] Since 2007, the military has spent $61.9 million on 1.28 million gallons of biofuel, averaging more than $48 a gallon, or $2,000 a barrel, and costing taxpayers $88 million more than if conventional fuel had been purchased (fig. 4).[60] This does not include more than $30 million paid for pure research on alternative fuels and recent additional millions for biorefineries obligated under the Defense Production Act in partnership with the Departments of Energy and Agriculture.[61]

DoD Biofuels Purchases						
Date	Contract	Vendor	Fuel	Gallons	$ Total	Per Gallon
31 Aug 2009	SP0600-09-D-0519	Sustainable Oils	Camelina JP-5	40,000	2,644,000	**$66.10**
31 Aug 2009	SP4701-09-C-0040	Solazyme	Algae F-76	20,055	8,574,022	**$427.53**
1 Sep 2009	SP0600-09-D-0518	Solazyme	Algae JP-5	1,500	223,500	**$149.00**
15 Sep 2009	SP0600-09-R-0704	UOP (Cargill)	Tallow JP-8	100,000	6,400,000	**$64.00**
15 Sep 2009	SP0600-09-D-0520	Sustainable Oils	Camelina JP-8	100,526	6,715,137	**$66.80**
29 Jun 2010	SP0600-09-D-0519	Sustainable Oils	Camelina JP-5	150,000	5,167,500	**$34.45**
26 Jul 2010	SP0600-10-D-0489	Sustainable Oils	Camelina JP-8	34,950	1,349,070	**$38.60**
4 Aug 2010	SP0600-10-D-0490	Sustainable Oils	Camelina JP-8	19,672	759,339	**$38.60**
31 Aug 2010	SP0600-09-D-0520	Sustainable Oils	Camelina JP-8	100,000	3,490,000	**$34.90**
31 Aug 2010	SP0600-09-D-0517	UOP (Cargill)	Tallow JP-8	100,000	3,240,000	**$32.40**
10 Sep 2010	SP4701-10-C-0008	Solazyme	Algae F-76	75,000	5,640,000	**$75.20**
26 Aug 2011	SP4701-10-C-0008	Solazyme	Algae F-76	75,000	4,600,000	**$61.33**
23 Sep 2011	SP0600-11-R-0703	Gevo	Alcohol to JP-8	11,000	649,000	**$59.00**
30 Sep 2011	SP0600-11-D-0530	UOP	Bio JP-8	4,500	148,500	**$33.00**
30 Nov 2011	SP0600-11-R-0705	Dynamic Fuels (Tyson+Syntroleum), Solazyme	Tallow & Algae JP-5 Tallow & Algae F-76	100,000 350,000	12,037,500	**$26.75**
23 Sep 2011	DTRT5711C10058 (DoT/FAA, not DoD)	UOP	Gevo Isobutano to Jet Fuel	100	1,124,899	**$11,248.99**
2 Feb 2012	N68936-12-P-0209	Albemarle	Cobalt n-Butanol to Jet Fuel	55	245,000	**$4,454.55**
DoD Synthetic Fuels Purchases						
6 Jun 2007	SP0600-07-D-0486	Equilon	Natural Gas to Aviation Kerosene	315,000	1,075,694	**$3.41**
26 Jun 2008	SP0600-08-D-0496	SASOL	Coal to Aviation Kerosene	60,000	225,000	**$3.75**
3 Jul 2008	SP0600-08-D-0497	SASOL	Coal to Aviation Kerosene	335,000	1,306,500	**$3.90**
30 Sep 2009	SP0600-09-D-0523	PM Group	Natural Gas to Diesel	20,000	140,000	**$7.00**
DoD Bulk Contract Conventional Fuel Purchase						
FY 2010	Various		JP-8 Jet Fuel JP-4 / Jet A-1 JP-5 Jet Fuel F-76 Fuel Oil Motor Gasoline	2,296M 1,249M 541.8M 805.7M 70.7M	5,201M 2,884M 1,175M 1,816M 174.1M	**$2.26** **$2.31** **$2.17** **$2.25** **$2.46**
FY 2011	Various		JP-8 Jet Fuel JP-4 / Jet A-1 JP-5 Jet Fuel F-76 Fuel Oil Motor Gasoline	2,079M 1,246M 529.3M 875.9M 59.0M	6,478M 4,032M 1,572M 2,590M 186.6M	**$3.12** **$3.24** **$2.97** **$2.96** **$3.16**

Figure 4. DoD comparative fuel purchases

The Nation's Cost

The per-gallon price paid by the military for biofuels is only a fraction of the US government's full cost. Government officials profess grave concern at the volatility of oil prices, and economic forecasters cite statistics that a $10 rise in the price of a barrel of oil slows the US economy 0.2 percent and kills 120,000 jobs.[62] Yet, the federal government is voluntarily paying more than $10 a barrel in biofuel subsidies (fig. 5).[63] The Department of Enegy (DoE) pumped $603 million into biofuel refinery construction in 2010 as part of $7.8 billion in annual biofuels spending.[64] Despite millennia of ethanol production as a beverage, 190 years of ethanol production as a fuel, and six years of huge subsidies and blending mandates and guaranteed markets since 2005, a joule of corn ethanol energy today is still more expensive than a joule of gasoline energy. The American Automobile Association reports as of December 2012 that the mpg-corrected price of E85 ethanol at the gas pump is 40 cents a gallon higher than premium gasoline.[65] Because of mandatory blending of lower energy density ethanol in gasoline, consumers in 2010 paid $8.1 billion at the gas pump for energy that was not put into their tanks. When added to the $6.1 billion in federal subsidies given out by the US Treasury and taxpayers as ethanol tax credits, the United States paid a $14.2 billion premium in 2010 to displace 6.4 percent of its gasoline energy with ethanol—and the cheaper gasoline that was displaced was exported. [67]

Energy Source	Federal Subsidies (millions of $)	Domestic Production (million bbl of oil equivalent)	Subsidy per barrel of energy produced
Coal	$1,358	3,793	$0.36
Oil and Gas	$2,820	6,229	$0.45
Hydro	$216	437	$0.49
Nuclear	$2,499	1,451	$1.72
Geothermal	$273	36	$7.63
Biomass/fuel	$7,761	747	$10.39
Wind	$4,986	159	$31.39
Solar	$1,134	22	$52.30
Total	**$21,047**	**12,874**	**Average = $1.63**

Figure 5. US federal government energy subsidies in 2010

The Nation's Gain

A true primary energy source, like a true food source, cannot be subsidized. It must, by definition, yield many times more energy (and wealth) than it consumes, or else it is an energy sink. Critics of petroleum often claim it is subsidized, but when both sides of the balance sheet are considered, the money is revealed to be flowing the other way. All federal subsidies and tax breaks for oil and natural gas in 2010, as officially tallied across all government agencies and reported to Congress, totaled \$2.82 billion, equaling 45 cents per barrel produced domestically. Against that outlay, the federal government collected \$56.1 billion in oil company corporate taxes and excise taxes on retail gasoline and diesel, equaling \$9.01 per barrel—a 2,000 percent return.[68] State and local governments collected similar shares in taxes and fees as well. It is not by subsidies that fossil fuels have grown to produce 82 percent of US energy, but by the merits of EROI, energy density, and power density in competition with other energy alternatives. Oil and gas are true primary energy sources that nourish rather than starve the US government and economy. Global oil and gas energy is a \$3.8 trillion industry that fully subsidizes the rentier economies of 10 petro states and partially subsidizes the economies of 70 more producers.[69] In the United States alone, there are 536,000 active crude oil wells, 504,000 active natural gas wells, dozens of continent-spanning pipelines, a colossal interstate highway system, 17 million barrels-per-day of refining capacity, 160,000 gas stations, and a \$1.5 trillion fraction of the global oil and gas industry that have all been funded out of oil and gas EROI margins.

Power Density and Land Use

If EROI and price were not fatal enough, the questions of land use and ultimate capacity must also be answered. Land is a finite national resource with many competing uses. Biofuel production is a terribly inefficient use of land, and this can best be illustrated with *power density*, a key metric for comparing energy sources. The 70 gallons of biodiesel per acre of soy and 500 gallons of ethanol per acre of corn are amazing agricultural achievements, but are dismal in terms of power density, and work out to only 0.069 and 0.315 W/m^2 respectively. While corn is 4.5 times better than soy, it is a factor of three below wind (1.13 W/m^2), 19 times worse than photovoltaic (PV) solar (6.0 W/m^2), and 300 times worse than the 90 W/m^2 delivered by the average US petroleum pumpjack well on a two-acre plot of land.[70] Thirty square meters of today's cheapest PV solar panels can capture the same amount of energy per year as is in the ethanol from 10,000 square meters (2.5 acres) of cultivated switchgrass.[71] This is, coincidentally, about the same amount of land the average American family would require as biofuels pasture for each of its cars. Alternatively, that land could sustainably grow crops to feed 20 vegans or the crops and livestock to feed 2.5 meat-eating humans.[72] To replace the 28 exajoules of energy the United States uses every year just for cars, trucks, and airplanes would require more than 700 million acres of corn. This is 37 percent of the total area of the continental United States, more than all 565 million acres of forest, and more than triple the current amount of annually harvested cropland. Soy biodiesel would require 3.2 billion acres—one billion more than all US territory including Alaska. Oil palm biodiesel yields are reported to be as high as 640 gal/acre (6,000 L/ha), which exactly double the power density of corn ethanol but still fall far short of wind and solar power. As hinted earlier, algae biodiesel has the highest potential power density of any biofuel, but the predicted best case achievable, as limited by physical laws and laboratory-perfect conditions, is 6.42 W/m2—equivalent to what is produced today from the solar farm at Nellis AFB.[73] Figure 6 contrasts the land area of oil field, solar farm, wind farm, and cornfield needed to replace the 2,000 MW of power produced by the San Onofre Nuclear Generating Station in Oceanside, California.

The high prices and environmental protections on land in developed countries make dedicating millions of acres to biofuels prohibitive, despite optimistic government studies that postulate turning most forests and arable land into agribusiness zones for biofuels.[74] Real-world economics compels energy farmers to look for cheaper cropland and water rights in less developed countries. The United States and European nations are primarily pursuing offshore land indirectly, such as through Blue Sugars' joint venture with Petrobras where Brazilian sugarcane bagasse feedstock was shipped to the United States for processing.[75] A 2010 World Bank analysis revealed that other wealthy countries, including Saudi Arabia, South Korea, and China, are pursuing a more direct strategy and have already purchased or leased more than 27 million acres of foreign land and water rights for remote cultivation of food, industrial, and biofuel crops. Chief locations for such land appropriation are Sudan, Mozambique, and Ethiopia, where millions are living hand-to-mouth on food from the UN World Food Program.[76] Even at today's small scale of production, biofuels' huge appetite for land already puts them in significant and direct competition with food production. Food must and will eventually win this competition because there is not enough suitable land for both. A recent European metastudy of 90 other studies concluded that only one-fifth of the world's energy demand could likely be met by biofuels without removing meat from the human diet or making massive land use changes beyond the 296 million acres which already must be put into cultivation to feed the population of 2050.[77]

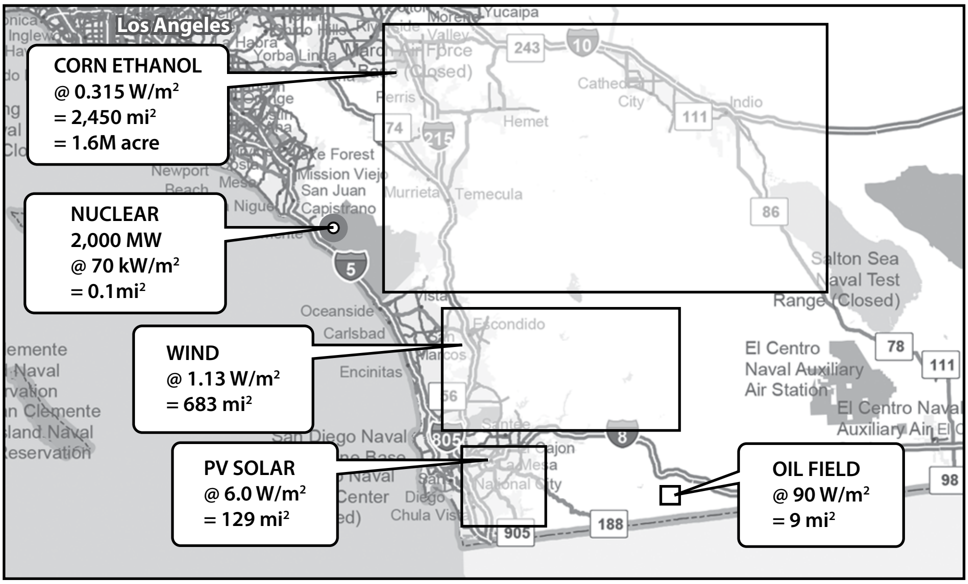


Figure 6. Power density "energy sprawl"

The Competition of Fuel and Food

Around the world, cultivated food crops (corn, sugarcane, soy, palm, and various oilseeds) account for all statistically significant liquid biofuel production.[78] In 2008, world grain market prices tripled, mirroring the spike in global oil prices and proving the linkage between food calories and energy calories in the modern world. Grain prices to the poorest consumers increased as much as 50 percent, driving 8 percent more of Africa's population toward hunger and raising the world's undernourished population to approximately 850 million.[79] Today's market prices are still double what they were in 2007. Various studies of the 2008 food price spike have attributed as much as 70 percent of the increase in corn and 100 percent of the increase in sugar prices to global diversion of food to biofuels.[80] A union of the world's preeminent food and financial assistance agencies, including the World Food Program and the Food and Agriculture Organization of the United Nations, has formally called for all G20 nations to drop their biofuels subsidies and mandates because of the impact on food prices around the world.[81] The fact is that every cultivated crop—food or nonfood—competes with every other cultivated crop for finite resources including water, land, agrichemicals, farm equipment, transportation, and financing. Putting more demand on these resources raises prices for everyone. Biofuels are becoming a huge threat to global food security, and thereby to global stability—a fact that should shape any military or political energy strategy. Many analysts now looking at the "Arab Spring" phenomenon recognize that, underlying the very real political aspirations of movements such as the revolution in Tunisia was outrage at skyrocketing food prices. What began as bread riots in Egypt due to the end of government grain subsidies became a hot-blooded revolt and coup.

As the global population sprints toward nine billion by 2050, there are 140,000 more mouths to feed every day. Food grain consumption is growing at 40 million tons per year.[82] Yet, because of enormous market-distorting subsidies, the United States today produces more corn for ethanol than for human food or cattle feed.[83] For decades past, it had surplus food crop capacity and used it to rescue other nations from famine. In 1965, Pres. Lyndon Johnson's administration shipped one-fifth of the US wheat crop to India during a devastating drought. With slack land now consumed by biofuels production, a drought such as the one that destroyed 40 percent of Russia's grain crop in 2010 would be devastating to national security—particularly because both food and fuel would be simultaneously affected. The negative consequences of biofuels on food crop production have been understood by the US government since a panel of scientists appointed by the newly formed DoE rejected gasohol for this and other sound reasons in 1980.[84] Twenty-five years later, politics trumped science with the imposition of US ethanol mixing mandates and corn ethanol subsidies. If our greater interest is truly global peace and security, US farmers should be out of the fuel business and instead increasing food production for the growing market of direct export contracts with famine-wary nations.

Biofuels versus the Environment

Despite claims of reduced GHG and pollution emissions for biofuels, the reverse is now becoming apparent. Biofuels have roughly the same tailpipe or flue gas emissions as conventional fuels, but until recently they automatically earned "green" and "reduced emissions" badges through simplistic accounting tricks that assumed all their carbon was recycled from the atmosphere and largely ignored the pollutants.[85] New, more thorough studies that consider the full fuel creation and combustion lifecycles (as in figs. 2 and 3 above) are now showing cultivated liquid biofuels to be more damaging to the environment and causing the release of more CO_2 and other greenhouse gases and pollutants per unit of energy delivered than fossil fuels.[86]

Even the overall environmental impact of adding ethanol to gasoline as an oxygenate has been shown to be negative—it does nothing to improve the emissions of US cars built since 1993, reduces the fuel economy of every gasoline vehicle, increases emissions of some smog precursors, and increases the environmental hazard of spills because of increased miscibility with water.[87] The most important change in the new studies is the proper accounting of land-use changes driven by biofuel cultivation, such as converting forests to cropland by burning. This widespread practice has been accelerated around the world by biofuels agriculture and is releasing centuries of carbon sequestered in forest biomass back into the atmosphere from these natural carbon sinks. Such burning strikes a double blow because it also destroys a dense living biome with a huge perpetual appetite for CO_2. Calculations indicate that large-scale conversion of virgin land to biofuel production has already released and continues to release so much CO_2 into the atmosphere that it may be centuries before this surge can be offset by the recycled carbon in the resulting biofuels, if at all. The continued burning of millions of acres of forest and peat lands to make room for oil palms has made Indonesia the world's third highest producer of CO_2, after the United States and China.[88]

The Water Problem

A final downside to biofuels is water demand. *Water footprint* is the term for how much fresh water is consumed or rendered unusable by a particular activity. This can happen by evaporation, by removal to inaccessible parts of the ecosystem, or by contamination with chemicals such as industrial discharges or fertilizer runoff. Water use also represents a dimension of competition with food agriculture, but it is even more urgent and fundamental in its own right. While "peak oil" continues to be elusive (global petroleum production and proven reserves both set new record highs in 2011),[89] "peak water" has already arrived for much of the world. One third of all countries are today considered "water poor." Two of every five people do not have enough water for basic sanitation, and nearly one in five do not have enough to drink.[90] Many scientists and economists observe falling water tables and depleting aquifers due to overpumping (including the massive Central Valley and High Plains aquifers in the United States) and predict this will expand to a global water crisis before 2030.[91] Much of the Middle East and a growing number of other nations, including China, Japan, Australia, and Spain, are now dependent upon desalination of seawater for a significant fraction of their fresh water needs.[92] To put this dependence into perspective, consider that a US nuclear aircraft carrier can desalinate 400,000 gallons of water a day.[93] The current desalination demand of the world exceeds 78 million cubic meters per day with 11 percent annual growth.[94] This equates to 51,500 aircraft carriers worth of desalination capacity with 5,600 more being built each year. Saudi Arabia is currently willing to spend one liter of ethanol-equivalent energy in crude oil to desalinate 200–300 liters of water.[95] How do these economics mesh with biofuels?

Conventional gasoline has a water footprint of 2.3–4.4 liters of water per liter of ethanol-equivalent energy (L/L), including water injected into the ground for enhanced oil recovery and water used in refining.[96] In contrast, global averages for biofuels range from sugar beet ethanol (1,388 L/L) to corn ethanol (2,570 L/L) to soy biodiesel (13,676 L/L) to rapeseed biodiesel (14,201 L/L) to jatropha biodiesel (19,924 L/L).[97] Current state of the art for installed seawater desalination plants ranges from 126 to 970 liters of water per liter of ethanol-equivalent energy.[98] So, under absolute best case circumstances, sugar beet feedstock cannot produce enough ethanol fuel energy to desalinate enough water to grow a replacement crop, let alone provide leftover ethanol as fuel. Biofuels' huge dependence upon water means they are not truly a renewable fuel in any location where water is being depleted. *Not one biofuel crop is renewable in desalinated seawater*. Under the president's recently published update to Executive Order 13603 that specifies responsibilities under the Defense Production Act, the secretary of defense is now responsible for the US water supply.[99] That should cause some reflection regarding the DoD's promotion of biofuels. When Saudi Arabia and a third of the world are willing to spend a liter of fuel for less than 1,000 liters of water, how long can others get away with spending 10,000 liters of water for one liter of biofuel?

Conclusions and Recommendations

Ultimately, biofuels are limited by the sun. If they rely exclusively on solar energy to make biomass without adding fossil fuel energy, the EROI can be high enough, but the power density will be far too low, even at maximum theoretical photosynthesis performance. If yield is boosted with fossil fuel hydrogen or carbon, fossil fuel use increases, biofuel EROI plummets and drags overall EROI with it, power density is still too low, and civilization ends up even more starved for power. One way out of this dilemma is to create a plentiful supply of hydrogen from a non–fossil fuel source. However the only prospect is to electrolyze hydrogen from water using nuclear power. If we had such a surplus of nuclear power electricity and hydrogen, we would use it directly for power, not for inefficient biomass conversion. This litany is the inescapable catch-22 of biofuels.

Converting natural gas hydrocarbons into ammonia fertilizer and then into the carbohydrates of plant biomass is a sequence of transformations that irreversibly consumes some usable energy in each step. That loss of energy can be justified if the crop being grown is food and is of greater need than the energy used to grow it. However, completing the circle by converting that plant's carbohydrate biomass back into hydrocarbons for fuel makes the whole process a futile analog of the perpetual motion machine. Improvements in technology can reduce the amount of energy lost in each conversion but cannot eliminate it. Any wood, grass, peat, bagasse, coal, natural gas, or oil will deliver much more benefit to civilization if used directly and efficiently as fuel by a consumer whose needs are compatible with its limitations, rather than by using its energy to make biofuels. As long as the preponderance of ammonia and free hydrogen and organic compounds used in agriculture are derived from petroleum and natural gas, cultivating biofuels will defy all logic. Biofuels can never be cheaper than nor replace fossil fuels while fossil fuels comprise the bulk of the energy invested to make them.

Imagine if the US military developed a weapon that could threaten millions around the world with hunger, accelerate global warming, incite widespread instability and revolution, provide our competitors and enemies with cheaper energy, and reduce America's economy to a permanent state of recession. What would be the sense and the morality of employing such a weapon? We are already building that weapon—it is our biofuels program. For the sake of our national energy strategy and global security, we must face the sober facts and reject biofuels while advocating an overall national energy strategy compatible with the laws of chemistry, physics, biology, and economics. This revised strategy must acknowledge several key aspects:

- Liquid hydrocarbons are unmatched as transportation fuel. Using hydrocarbons to process biomass into transportation fuel is detrimental to civilization's energy balance and must be avoided.
- Renewable fuels must be truly renewable in all their ingredients, and all biofuels under consideration today fail in one or more categories of water footprint, soil nutrient depletion, eutrophication, lifecycle GHG, air pollution, and overall energy balance.
- Not even today's best liquid biofuels have any prospect of simultaneously attaining the 6:1 threshold EROI necessary to support a healthy modern civilization while also achieving the massive yields per acre necessary to supplant any significant fraction of the national energy supply. Boosting yields using fossil fuel for ammonia fertilizer, pesticide and herbicide feedstock, farm equipment fuel, transportation fuel, processing plant energy, distillation energy, enzyme feedstock, or hydrotreatment hydrogen lowers EROI and undermines every clean and green energy objective.
- Government energy policies that restrict domestic development of a nation's highest EROI energy sources and fuels—such as hydropower, coal, natural gas, and petroleum—are tantamount to caps on thermodynamic efficiency, economic health, and international competitiveness. Conversely, the nations that pursue the highest EROI energy will have the greatest potential to grow their econo-

mies and have every prospect of advantage over countries limited to lower EROI sources. The US government should end subsidies and market-distorting policies that encourage low-EROI energy sources over high-EROI sources.

- Petroleum and natural gas are true primary energy sources and fuel modern agriculture. To conserve petroleum as a limited resource, it is best used directly as fuel. Use of fossil fuel energy to accelerate food crop growth may be justifiable, but its use to accelerate energy crop growth is ludicrous on its face, as the result is less overall efficiency of energy and greater net consumption of petroleum. Government policy should restrict the use of artificial ammonia-based fertilizers to food crops only.

- The price of oil, like that of any other global free-market commodity, is volatile and subject to war, politics, and speculation. However, biofuels are subject to both oil and agricultural market forces and are at the mercy of weather as well. Biofuel prices have proven as volatile as oil prices and are likely to be more so once subsidies end. In addition, it is logically indefensible to buy a $30.00 per gallon fuel over worries about the price volatility of a $3.00 per gallon fuel.

- The technologies most in need of Manhattan Project–level attention by our global security strategists and national scientific laboratories are water production and food agriculture to support the nine billion people of 2050. The government should cease funding biofuel refinery construction and instead offer incentives for enhanced food production and water desalination efficiencies.

- The best use of agricultural land and water is to produce sufficient food for the United States and a surplus for the rest of the world. This has been before and can once again be a major contribution to security and stability in the world.

- Biomass is an inefficient middleman between solar energy and fuel. A better approach is to bypass the creation of biomass completely and directly synthesize liquid fuel from sunlight. The US government should cease funding biofuel research and instead offer prizes for milestones in direct fuel photosynthesis, which is a much more worthy line of research.[100]

- The only sensible use of biomass as fuel is to harvest unfertilized biomass from unmanaged land and consume it as is (e.g., firewood), without wasteful attempts to transform it into liquid fuel.
- The best-case power density predicted for any biofuel is already attained by today's PV solar panels. The US government should cease subsidizing biofuels and instead reward improved PV solar panel performance.
- Mandating the use of higher-EROI fossil fuels to make lower-EROI biofuels requires the overall consumption of more energy to deliver the same usable power output. Current US biofuels policy is accelerating rather than decreasing the use of fossil fuels and also increasing lifecycle ecological damage and GHG emissions due to destructive global land-use change and harmful agrichemical side effects. This is the exact opposite of "clean and green." The government should set policies that favor and optimize the use of hydrocarbons for fuel and carbohydrates for food and not confuse or undermine the efficiency of either by conflating them.
- CO_2 is not the only GHG. Agriculture is the leading producer of nitrous oxide (N_2O) and a major producer of methane (CH_4), which together comprise more than 26 percent of current total atmospheric GHG effects.[101] The US government should apply any caps or levy any taxes equitably across all greenhouse gases in proportion to their global warming potentials. Any per-ton penalties imposed on CO_2 should be levied against CH_4 at 69 times the rate and against N_2O at 298 times the rate to reflect relative per-ton global warming potentials.[102]
- The US military and federal government need to rationally and legally define *renewable*, *sustainable*, and *green* and enforce empirical standards for meeting these criteria based upon rigorous lifecycle analyses. Section 526 of the Energy Independence and Security Act of 2007 specifies that the lifecycle GHG emissions of any alternative or synthetic fuel purchased by the US government must be less than or equal to such emissions from the equivalent conventional fuel produced from conventional petroleum sources.[103] In light of recent research, and in the interest of curbing global warming, the US government should reexamine all §526 certifications issued to date for biofuels and blends. Any that do not consider the full biofuel lifecycle comprising land-use change for fuel creation as well as combustion, or that neglect N_2O emissions, should be invalidated.

- Global air and long-haul transportation and agriculture are currently very dependent on fossil fuel energy. It is unlikely that physically superior combustion fuels or fertilizers will be found. If the world runs out of fossil fuels without an alternative source for massive amounts of energetic hydrogen and carbon, civilization also immediately runs out of transportation fuel. To the extent that fossil fuels are judged to be running out, the government should ensure there is excess electrical capacity from non–fossil fuel power plants to electrolyze sufficient quantities of hydrogen from water for transportation fuel and agricultural purposes.

We must understand that a national energy strategy is nothing less than a national survival strategy. Those who would craft such strategy or advise policymakers need to be well-grounded in chemistry, thermodynamics, biology, and economics, so they might discern the difference between promising avenues of research and perpetual motion schemes that defy physical laws and waste our nation's time and treasure. What remains is for leaders and policymakers to catch up with the science and adjust their energy and security strategies to match the objective facts. An effective energy strategy for the United States must be informed by history and science and must exploit rather than defy the laws of nature to increase energy independence and global stability.

Notes

[1] 10 USC §2924—"Definitions" contains definitions of *energy security*, *operational energy*, and *renewable energy sources*, among others, as specified in the National Defense Authorization Act of 2012, http://www.law.cornell.edu/uscode/text/10/2924?quicktabs_8=1#quicktabs-8.

[2] "How Much Petroleum Does the United States Import and from Where?" *Energy Information Administration*, 16 July 2012, http://www.eia.gov/tools/faqs/faq.cfm?id=727&t=6.

[3] See James T. Bartis and Lawrence Van Bibber, *Alternative Fuels for Military Applications* (Santa Monica, CA: RAND, 2011), http://www.rand.org/pubs/monographs/MG969.html; and Dina Fine Maron, "Biofuels of No Benefit to Military—RAND," *New York Times*, 25 January 2011.

[4] See James T. Bartis, *Promoting International Energy Security* (Santa Monica: RAND, 2012), http://www.rand.org/pubs/technical_reports/TR1144z1.html; and National Research Council (NRC), *Renewable Fuel Standard: Potential Economic and Environmental Effects of U.S. Biofuel Policy* (Washington: National Academies Press, 2011).

[5] *Bioenergy—Chances and Limits* (Halle, GE: Nationale Akademie der Wissenschaften—Leopoldina, 2012), http://www.leopoldina.org/en/publications/detailview/?publication[publication]=433.

[6] NRC Committee on the Sustainable Development of Algal Biofuels, *Sustainable Development of Algal Biofuels in the United States* (Washington: National Academies Press, 2012).

7. Organisms that have the hydrogenase uptake enzyme (HUP+), such as soil and legume root bacteria, can capture and oxidize H_2 into $2H^+ + 2e^-$ and directly harvest that energy. See Z. Dong and D. B. Layzell, "H_2 Oxidation, O_2 Uptake and CO_2 Fixation in Hydrogen Treated Soils," *Plant and Soil* 229, no. 1 (2001): 1–12, http://www.springerlink.com/content/qp73k5770103075r/abstract/.

8. A liter of gasoline contains 116 grams of hydrogen compared to 71 grams per liter in pure liquid hydrogen.

9. Cultivated crops respond with dramatically increased yields to energy supplied by hydrogen as pure H_2 gas or as any form of the ammonia molecule including anhydrous ammonia (NH_3), the ammonium ion (NH_4^+), and urea ($(NH_2)_2CO$). In each of these molecules, the hydrogen atoms are also the energy carriers and greatly outnumber the nitrogen. Studies have shown that fertilizing with pure hydrogen gas (H_2) without adding nitrogen can greatly boost soil bacteria activity and biomass synthesis. See Dong and Layzell, "H_2 Oxidation, O_2 Uptake and CO_2 Fixation in Hydrogen Treated Soils"; and Dong et al., "Hydrogen Fertilization of Soils—Is This a Benefit of Legumes in Rotation?" *Plant, Cell and Environment* 26, no. 11 (November 2003): 1875–79. http://doi.wiley.com/10.1046/j.1365-3040.2003.01103.x. Applying ammonia fertilizer to crops that are robust nitrogen fixers such as soy still results in substantial gains. See Richard B. Ferguson et al., "Fertilizer Recommendations for Soybean," University of Nebraska Institute of Agriculture and Natural Resources, August 2006, http://www.ianrpubs.unl.edu/live/g859/build/g859.pdf. For details of how hydrogen gas and ammoniac compounds serve as fuel to plants and bacteria, see Susanne Stein et al., "Microbial Activity and Bacterial Composition of H_2-treated Soils with Net CO_2 Fixation," *Soil Biology and Biochemistry* 37, no. 10 (October 2005): 1938–45; D. C. Ducat et al., "Rewiring Hydrogenase-Dependent Redox Circuits in Cyanobacteria," *Proceedings of the National Academy of Sciences* 108, no. 10 (8 March 2011): 3941–46, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3053959/; and F. B. Simpson and R. H. Burris, "A Nitrogen Pressure of 50 Atmospheres Does Not Prevent Evolution of Hydrogen by Nitrogenase," *Science* 224, no. 4653 (8 June 1984): 1095–97, http://www.sciencemag.org/cgi/doi/10.1126/science.6585956. Once ammonia becomes available in the soil or plant roots, whether fixed by bacteria or humans, it reacts with water and oxygen and decomposes into hydrogen ions, hydrogen gas, and nitrate ions in a process known as "nitrification." These subcomponents serve as energy packages and building blocks supporting the myriad additional reactions and processes of biosynthesis. Partial oxidation of ammonia produces nitrous oxide (a GHG) and hydrogen gas: $2NH_3 + O_2 \rightarrow N_2O + H_2O + 2H_2$. Full decomposition of ammonia in water solution with oxygen produces hydrogen ions and nitrate ions and completes nitrification: $NH_3 + H_2O + 2O_2 \rightarrow 2H^+ + NO_3^- + OH^- + H_2O$.

10. Hydrogen-free sodium nitrate ($NaNO_3$) fertilizer comprised only 0.046 percent of commercial nitrogen fertilizer use in 2010. Virtually 100 percent of the 20 million tons of "nitrogen" fertilizer used annually in the United States is ammonia-based and made with hydrogen from natural gas. See "Fertilizer Use and Price," USDA Economic Research Service, 4 May 2012, http://www.ers.usda.gov/data-products/fertilizer-use-and-price.aspx.

11. Symbiotic rhizobial root bacteria get sugar from the host plant and use some of that energy and hydrogen to create NH_3 and H_2 gas and release these to the plant and into the soil. Soil bacteria metabolize the soil ammonia and H_2 and use that energy to break down soil minerals and materials such as chitin and lignin in humus into reduced carbon and mineral nutrients usable by the plant. For various aspects of the energy relationship between plants, bacteria, and ammonia, see P. Mylona, K. Pawlowski, and T. Bisseling, "Symbiotic Nitrogen Fixation," *Plant Cell*, no. 7 (July 1995): 869–85, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC160880/; Rifat Hayat et al., "Soil Beneficial Bacteria and Their Role in Plant Growth Promotion: a Review," *Annals of Microbiology* 60, no. 4 (28 August 2010): 579–98, http://rd.springer.com/article/10.1007/s13213-010-0117-1; Guido Sanguinetti et al., "MMG: a Probabilistic Tool to Identify Submodules of Metabolic Pathways,"

Bioinformatics 24, no. 8 (21 February 2008): 1078–84, http://bioinformatics.oxfordjournals.org/cgi/doi/10.1093/bioinformatics/btn066; and V. N. Matiru, and F. D. Dakora, "Potential Use of Rhizobial Bacteria as Promoters of Plant Growth for Increased Yield in Landraces of African Cereal Crops," *African Journal of Biotechnology* 3, no. 1 (2004): 1–7, http://www.ajol.info/index.php/ajb/article/view/14908.

12. Ernst Worrell et al., *Energy Use and Energy Intensity of the US Chemical Industry*, Lawrence Berkeley National Laboratory, April 2000.

13. A. M. Blackmer et al., "Nitrogen Fertilizer Recommendations for Corn in Iowa," Iowa Cooperative Extension Service, May 1997, http://www.extension.iastate.edu/Publications/PM1714.pdf.

14. Lance Gibson and Garren Benson, "Origin, History and Uses of Corn," Iowa State University Department of Agronomy, revised January 2002, http://www.agron.iastate.edu/courses/agron212/readings/corn_history.htm.

15. W. M. Stewart et al., "The Contribution of Commercial Fertilizer Nutrients to Food Production," *Agronomy Journal* 97, no. 1 (2005): 1, https://www.agronomy.org/publications/aj/abstracts/97/1/0001.

16. The widely accepted value for *biomass accumulation efficiency*, which is the fraction of total incident solar energy converted into biomass by photosynthesis, is 0.1 percent for most terrestrial plants. Plants use a much higher fraction of the sun's energy, but most of it goes into overhead costs such as evaporating water from the leaves to perform the work of drawing up nutrients from the ground against the force of gravity. Efficiencies as high as 4 percent under special circumstances have been reported, and it may be possible to boost this to 8 percent with human reengineering of the enzymes and mechanics. However, the highest efficiencies are achieved at very low light fluxes. Photosynthesis is saturated in capacity between 20 percent and 50 percent of maximum solar irradiance, and plants suffer radiation damage at these higher levels. Gains in net biomass accumulation remain elusive. See X. G. Zhu, S. P. Long, and D. R. Ort, "What Is the Maximum Efficiency with which Photosynthesis Can Convert Solar Energy into Biomass?" *Current Opinion in Biotechnology* 19, no. 2 (April 2008): 153–59, http://linkinghub.elsevier.com/retrieve/pii/S0958166908000165; Robert E. Blankenship et al., "Comparing Photosynthetic and Photovoltaic Efficiencies and Recognizing the Potential for Improvement," *Science* 332, no. 6031 (12 May 2011): 805–9; Harmut Michel, "The Nonsense of Biofuels," *Angewandte Chemie International Edition* 51, no. 11 (12 March 2012): 2516–18, http://doi.wiley.com/10.1002/anie.201200218; and Food and Agriculture Organization of the United Nations, *Renewable Biological Systems for Alternative Sustainable Energy Production*, chap. 1: "Biological Energy Production," September 2012, http://www.fao.org/docrep/w7241e/w7241e05.htm#1.2.1. For aquatic photosynthesis, see Kristina Weyer et al., "Theoretical Maximum Algal Oil Production," *Bioenergy Research* 3, no. 2 (8 October 2009): 204–13, http://www.springerlink.com/index/10.1007/s12155-009-9046-x.

17. The National Renewable Energy Laboratory (NREL) reports that solar radiation across the spectrum delivers energy to the cloudless southwestern US desert at a rate of 7.25 kWh/m^2-day = 302 W/m^2. At the observed biomass accumulation efficiency of 0.1 percent, this equates to 0.3 W/m^2 put into plant biomass, of which only a fraction can be eventually recovered as liquid fuel. See "Concentrating Solar Resource: Direct Normal," NREL, February 2009, http://www.nrel.gov/gis/images/map_csp_us_10km_annual_feb2009.jpg.

18. Solar photovoltaic (PV) AC power density of 6.0 W/m^2 is the current real-world, best-case, annualized value for large solar farm sites in southern US latitudes. This value is based on empirical analysis of nearly five years of actual performance of the Nellis AFB solar power plant (completed December 2007, $100 million cost, 72,416 panels on 140 acres, 14MW$_{pv}$ nameplate capacity, single-axis tracking array, 19 percent land coverage density, 24.5 percent capacity factor, producing 30 GWh/yr.). See "Nellis AFB Solar Power System,"

http://www.nellis.af.mil/shared/media/document/AFD-080117-043.pdf; and "Nellis Air Force Base," *Sunpower Performance Monitoring*, http://commercial.sunpowermonitor.com/Commercial/kiosk.aspx?id=1dd14d57-7840-4b2d-af0a-0fe0fdd5c872.

19. Other formulations of energy balance ratios include energy return on energy investment (EROEI), energy cost of energy (ECE), energy intensity ratio (EIR), and energy return on investment (EROI). EROI is the most commonly used in the literature, but there is some debate over what boundaries to apply to the formula. What is offered here is the simplest version of the concept.

20. S. A. L. M. Kooijman, *Dynamic Energy and Mass Budgets in Biological Systems* (Cambridge UK: Cambridge University Press, 2000).

21. This tipping point is also correlated with greater than 10 percent GDP expenditures on energy. See C. W. King, "Energy Intensity Ratios as Net Energy Measures of United States Energy Production and Expenditures," *Environmental Research Letters* 5, no. 4 (October 2010): 044006.

22. Charles A. S. Hall et al., "What is the Minimum EROI that a Sustainable Society Must Have?" *Energies* 2, no. 1 (January 2009): 25–47.

23. David J. Murphy and C. A. S. Hall, "Year in Review—EROI or Energy Return on (Energy) Invested," *Annals of the New York Academy of Sciences* 1185, no. 1 (January 2010): 102–18.

24. X-axis energy contributions are EIA data for 2010 reported in "Estimated U.S. Energy Use in 2010: ~98.0 Quads," Lawrence Livermore National Laboratory, 2011, https://flowcharts.llnl.gov/content/energy/energy_archive/energy_flow_2010/LLNLUSEnergy2010.png. Y-axis EROI values are depicted as ellipses to capture the range of values reported in different studies and for different sites. These values derived from the author's synthesis of published literature review including the following documents: DoE, "Fact Sheet: Energy Efficiency of Strategic Unconventional Resources," http://fossil.energy.gov/programs/reserves/npr/Energy_Efficiency_Fact_Sheet.pdf; "EROI Update: Preliminary Results Using Toe-to-Heel Air Injection," *Oil Drum*, http://www.theoildrum.com/node/5183/486247; Megan C. Guilford et al., "A New Long Term Assessment of Energy Return on Investment (EROI) for U.S. Oil and Gas Discovery and Production," *Sustainability* 3, no. 10 (October 2011): 1866–87, http://www.mdpi.com//2071-1050/3/10/1866/; Nate Hagens, "Proper Calculation of Brazilian Sugarcane EROI," *Oil Drum*, 24 March 2009; C. A. S. Hall, "Wave & Geothermal," *Oil Drum*, 14 May 2008; Hall, "Why EROI Matters," *Oil Drum*, 1 April 2008; Hall, "Provisional Results," *Oil Drum*, 8 April 2008; Hall, "Unconventional Oil: Tar Sands and Shale Oil," *Oil Drum*, 15 April 2008; Hall, "Nuclear Power," *Oil Drum*, 22 April 2008; Hall, "Solar, Wind and Hydro," *Oil Drum*, 29 April 2008; Hall et al., "What Is the Minimum EROI that a Sustainable Society Must Have?"; Hall et al. "Seeking to Understand the Reasons for Different Energy Return on Investment (EROI) Estimates for Biofuels," *Sustainability* 3, no. 12 (13 December 2011): 2413–32; Hill et al., "Environmental, Economic, and Energetic Costs and Benefits of Biodiesel and Ethanol Biofuels," *Proceedings of the National Academy of Sciences* 103, no. 30 (2006): 11206; King, "Energy Intensity Ratios as Net Energy Measures of United States Energy Production and Expenditures"; King and Hall, "Relating Financial and Energy Return on Investment," *Sustainability* 3, no. 10 (11 October 2011): 1810–32; David J. Murphy, "The Energy Return on Investment Threshold," *Oil Drum*, 25 November 2011; Murphy et al., "New Perspectives on the Energy Return on (Energy) Investment (EROI) of Corn Ethanol," *Environment, Development and Sustainability* 13, no. 1 (11 July 2010): 179–202; Murphy et al., "Order from Chaos: A Preliminary Protocol for Determining the EROI of Fuels," *Sustainability* 3, no. 10 (17 October 2011): 1888–1907; Tad W. Patzek, "A First-Law Thermodynamic Analysis of the Corn-Ethanol Cycle," *Natural Resources Research* 15, no. 4 (22 February 2007): 255–70; Bruce Pile, "The Alternative Energy No One Is Thinking About," *Seeking Alpha*; David Pimentel and Tad Patzek, "Ethanol Production: Energy and Economic Issues Related to U.S. and Brazilian Sugarcane," *Natural*

Resources Research 16, no. 3 (21 August 2007): 235–42; and Hosein Shapouri et al., "Estimating the Net Energy Balance of Corn Ethanol," *Agricultural Economic Report* 721 (July 1995).

25. Corn ethanol EROI values in the literature range from 0.7–1.7:1 with a median value of 1.2:1. Many metastudies have compared and contrasted multiple EROI approaches and papers. This author judges the most thorough and authoritative individual study to be Hill et al., "Environmental, Economic, and Energetic Costs and Benefits of Biodiesel and Ethanol Biofuels." This study is one of several to promulgate a value of 1.25:1 and to find that any positive energy balance was entirely dependent upon giving energy credit for co-products. The most thorough and authoritative recent metastudy surveying multiple individual corn ethanol lifecycle analyses was judged to be Murphy et al., "New Perspectives on the Energy Return on (Energy) Investment (EROI) of Corn Ethanol." This study is actually less favorable and finds a neutral 1:1 EROI. Two USDA-funded studies have found values of 1.24:1 in 1995 and 1.34:1 in 2002. Shapouri et al., "Estimating the Net Energy Balance of Corn Ethanol"; and Shapouri et al., *The Energy Balance of Corn Ethanol: An Update* (Washington: USDA, July 2002).

26. The pure corn ethanol EROI can be estimated by dividing the petroleum-corn ethanol hybrid EROI of 1.25:1 by the pure petroleum EROI of 8:1 (discussed later under "opportunity cost") to yield 0.156:1 ~ 1:6.

27. Tad Patzek, "A Probabilistic Analysis of the Switchgrass Ethanol Cycle," *Sustainability* 2, no. 10 (30 September 2010): 3158–94, http://www.mdpi.com/2071-1050/2/10/3158/.

28. M. R. Schmer et al., "Net Energy of Cellulosic Ethanol from Switchgrass," *Proceedings of the National Academy of Sciences* 105, no. 2 (15 January 2008): 464–69.

29. National Academy of Sciences, *Renewable Fuel Standard.*

30. The cellulosic ethanol sector was recently rocked by the demise of Range Fuels, the signature creation of vocal biofuels proponent Vinod Khosla and recipient of the first USDA biofuels loan guarantee of $64 million in 2010. This failure eclipsed the 2009 fraud scandal and collapse of Cello, which was the Solyndra of cellulosic ethanol.

31. Randy Schnepf and Brent D. Yacobucci, *Renewable Fuel Standard (RFS): Overview and Issues* (Washington: Congressional Research Service [CRS], 14 October 2010), http://digital.library.unt.edu/ark:/67531/metadc31329/m1/1/high_res_d/R40155_2010Oct14.pdf.

32. See "2012 RFS2 Data," Environmental Protection Agency, 19 July 2012, http://www.epa.gov/otaq/fuels/rfsdata/2012emts.htm; "Producing Sustainable Fuel Ethanol Today," Blue Sugars Corporation, http://bluesugars.com/technology-production.htm; Meghan Sapp, "Petrobras, KL Energy Extend Cellulosic Ethanol Development Agreement," *Biofuels Digest*, 26 June 2012, http://www.biofuelsdigest.com/bdigest/2012/06/26/petrobras-kl-energy-extend-cellulosic-ethanol-development-agreement/; and *Federal Register* 77 no. 5 (9 January 2012), http://www.gpo.gov/fdsys/pkg/FR-2012-01-09/html/2011-33451.htm.

33. Matthew Wald, "Companies Face Fines for Not Using Unavailable Biofuel," *New York Times*, 9 January 2012.

34. For Gevo, see Kevin Bullis, "To Survive, Some Biofuels Companies Give Up on Biofuels," *MIT Technology Review*, 21 December 2011, http://www.technologyreview.com/energy/39371/. For Amyris, see Sophie Vorrath, "Biofuels: Have the Republicans Gutted Green Fuel?" *Renew Economy*, 17 May 2012, http://reneweconomy.com.au/2012/biofuels-have-the-republicans-gutted-green-fuel-62642. For Cellana, see Jim Lane, "Shell Exits Algae as It Commences a 'Year of Choices,'" *Renewable Energy World*, 31 January 2011, http://www.renewableenergyworld.com/rea/news/article/2011/01/shell-exits-algae-as-it-commences-year-of-choices.

35. Jim Lane, "The October Surprise: BP Cancels Plans for US Cellulosic Ethanol Plant," *Renewable Energy World*, 26 October 2012, http://www.renewableenergyworld.com/rea/news/article/2012/10/the-october-surprise-bp-cancels-plans-for-us-cellulosic-ethanol-plant.

As of this writing, ZeaChem Inc., founded in 2002 and recipient of $297.5 million in grants and loan guarantees from the DoE and USDA, is operating its 250,000 gal/year biorefinery in Oregon as a demonstration facility, which means the product is not commercially competitive. Logen of Canada is still operating its 1,200 gal/day cellulosic ethanol facility in demonstration mode with total historic production since 2004 averaging less than 200 gal/day. KiOR is starting up its new 10 million gal/year biorefinery in Mississippi that investors and the EPA have been promised will deliver commercial sales and profits from competitively priced gasoline and diesel made from wood. INEOS Bio is also in the process of commissioning an 8 million gal/year commercial cellulosic ethanol plant in Florida. Already expectations for these massive capital investments are being deflated with revised names such as "commercial demonstration" or "second generation demonstration" plant floating around and profitability target dates shifting years into the future. If these huge facilities remain "demonstration plants," it will mean that, once again, the promises have not been kept. Even if they somehow achieve marginal profitability under a regime of biofuel subsidies and mixing mandates and carbon taxes, they will still face an insurmountable capacity problem because of abysmal power density.

[36] See Jim Lane, "Coskata Switches Focus from Biomass to Natural Gas; To Raise $100M in Natgas-Oriented Private Placement," *Biofuels Digest*, 20 July 2012, http://www.biofuelsdigest.com/bdigest/2012/07/20/coskata-switches-from-biomass-to-natural-gas-to-raise-100m-in-natgas-oriented-private-placement/; and Kevin Bullis, "Biofuels Companies Drop Biomass and Turn to Natural Gas," *MIT Technology Review*, 30 October 2012, http://www.technologyreview.com/news/506561/biofuels-companies-drop-biomass-and-turn-to-natural-gas/.

[37] Alan Shaw, former CEO of Codexis, stated that "carbohydrates are not a substitute for oil. I was wrong in that, and I admit it. [They] will never replace oil because the economics don't work. You can't take carbohydrates and convert them into hydrocarbons economically. . . . It's a death blow that that maximum yield is about 30 percent." Quoted in Bullis, "Biofuels Companies Drop Biomass."

[38] *Hydrotreatment* is most often used as a collective term for a set of processes necessary to refine or upgrade biofuels into true hydrocarbons that are "drop-in" compatible substitutes for conventional hydrocarbon applications. These steps include hydrogenation, deoxygenation, cracking, isomeration, fractionation, and using additives as necessary to adjust energy density, cetane, octane, volatility, cold flow properties, and lubricity. See Carlo Munoz, Jon Van Gerpen, and Brian He, *Production of Renewable Diesel Fuel*, National Institute for Advanced Transportation Technology, University of Idaho, June 2012, http://ntl.bts.gov/lib/46000/46200/46277/KLK766_N12-08.pdf.

[39] Hill et al., "Environmental, Economic, and Energetic Costs and Benefits of Biodiesel and Ethanol Biofuels."

[40] An EROI of 1:1 (300 GJ input vs. 317 GJ output) was reported if sun-dried product algal biomass was burned whole in a furnace extracting a thermodynamically perfect 100 percent of the HHV with no attempt to convert to a liquid fuel. See Andres F. Clarens et al., "Environmental Life Cycle Comparison of Algae to Other Bioenergy Feedstocks," *Environmental Science & Technology* 44, no. 5 (March 2010): 1813–19. A study that considered the costly biomass-to-liquid fuel conversion step found that the input energy required just to circulate the water in the cultivation ponds/tanks exceeded the biodiesel fuel energy output by a factor of seven. See Cynthia F. Murphy and David T. Allen, "Energy-Water Nexus for Mass Cultivation of Algae," *Environmental Science & Technology* 45, no. 13 (July 2011): 5861–68.

[41] NRC, *Sustainable Development of Algal Biofuels in the United States*.

[42] Photosynthetic stoichiometry for typical microalgae: 99.5 CO_2 + 75.5 H_2O + 7.5 $CO(NH_2)_2$ + ½ P_2O_5 (+ sunlight) –>[C_{107} H_{181} O_{45} N_{15} P] + 119.75 O_2 [carbon dioxide + water +

urea + phosphate (+ sunlight) –> microalgae + oxygen]. In this case, one-sixth of the hydrogen (30 of 181 atoms) in the microalgae is from urea, not water. Most algae are grown heterotrophically with some hydrogen and carbon energy being provided in ammoniacal or saccharine form. Autotrophic algae growth requires only CO_2, water, phosphate, micronutrients, and sunlight but delivers diminished yields. See E. D. Frank et al., *Life-Cycle Analysis of Algal Lipid Fuels with the GREET Model* (Oak Ridge, TN: DoE, August 2011), http://greet.es.anl.gov/publication-algal_lipid_fuels.

[43] Robert Rapier, "Visit and Conversation with Executives at Solazyme," *Consumer Energy Report*, 23 October 2011, http://www.consumerenergyreport.com/2011/10/23/visit-and-conversation-with-executives-at-solazyme/.

[44] Frank et al., *Life-Cycle Analysis*. Total energy to produce one functional unit of algae biodiesel of 2,589,441 BTU vs. 219,183 BTU to make one functional unit of conventional low-sulfur diesel = 11.8:1 ratio. Well-to-pump fossil fuel energy costs of 548,329 BTU vs. 215,388 BTU yield a ratio of 2.6:1.

[45] Murphy et al., "New Perspectives on the Energy Return on (Energy) Investment (EROI) of Corn Ethanol."

[46] The 8:1 petroleum fuel EROI is chosen as a conservative value from historical fluctuations within the range of 8:1 to 24:1 since 1920, per Guilford et al., "New Long Term Assessment."

[47] The term *barrel of energy* is used here to represent a generic unit of energy for relative comparison purposes. The term is more specifically defined as the energy in a barrel of crude oil and has a value of 6.1306 GJ = 1.7029 MWh = 5.8106 MBTU. A barrel of crude oil has virtually the same energy content as a barrel of diesel fuel.

[48] The fraction of crude oil that yields fuels vice feedstocks is based on "What a Barrel of Crude Oil Makes," *Texas Oil & Gas Association*, http://www.txoga.org/articles/308/1/WHAT-A-BARREL-OF-CRUDE-OIL-MAKES. CO_2 from fuel creation: 1 bbl x 42 gal/bbl of diesel @ 23.66 lb CO_2/gal for diesel combustion = 944 lb. The CO_2 from fuel combustion (all products): 11 bbl of crude x 42 gal/bbl x 22.99 lb CO_2/gal for crude combustion = 10,621 lb. Total CO_2: 944 lb + 10,621 lb = 11,565 lb (counting all carbon on the page = worst case). Input H_2O = 9 bbl x 42 gal/bbl x 6.6 gal/gal = 2,495 gal. The water footprint of petroleum covers all extraction and refining processes including water injection into older oil fields for secondary recovery. Maximum value of 6.6 gallons water per gallon of gasoline is used to make the calculation as conservative as possible and is based on May Wu and Yiwen Chiu, *Consumptive Water Use in the Production of Ethanol and Petroleum Gasoline—2011 Update* (2008; Oak Ridge, TN: DoE, July 2011).

[49] Ksenia Galouchko, "Ethanol Follows Gasoline Higher after Iran Blocks Base Access," *Bloomberg*, 22 February 2012, http://www.bloomberg.com/news/2012-02-22/ethanol-follows-gasoline-higher-after-iran-blocks-base-access.html.

[50] Fig. 3 depicts the same net energy output as fig. 2 (i.e., 8 bbl diesel equivalent). Each barrel of diesel equivalent energy input yields energy parity in 1.625 bbl of ethanol plus a 0.25 bbl diesel equivalent net energy profit in co-product DDGS. Ethanol has 0.615 times the volumetric energy density of diesel; therefore, it takes 52 bbl of ethanol to equal the energy in 32 bbl of diesel. Values of 478 gal/acre ethanol yield and 5 lb/gal of ethanol in DDGS yield are per 2008 survey of 90 dry-mill ethanol refineries as reported in Steffen Mueller, "News from Corn Ethanol: Energy Use, Co-Products, and Land Use," presentation at Near-Term Opportunities for Bio-refineries Symposium, Champaign, IL, 11–12 October 2010, http://bioenergy.illinois.edu/news/biorefinery/pp_mueller.pdf. Acreage of cornfield required : 52 bbl x 42 gal/bbl = 2,184 gal ÷ 478 gal/acre = 4.57 acre. DDGS co-product: 5 lb/gal x 2,184 gal = 10,920 lb CO_2 from fuel creation: 32 bbl x 42 gal/bbl x 23.66 lb CO_2/gal diesel = 31,799 lb. No CO_2 is charged for ethanol or DDGS consumption. Conservative calculation of CO_2-equivalent N_2O emissions (CO_2e) from corn fertilization: 2 percent of 150 lb/acre NH_3 x 4.6 acre = 13.8 lb NH_3 x 82.35 percent N mass fraction of NH_3 = 11.36 lb N ÷ 63.64 percent

N mass fraction of N_2O = 17.86 lb N_2O x 298 multiplier for CO_2 warming potential equivalence = 5,321 lb CO_2e. Total CO_2e emissions: 31,799 lb CO_2 + 5,321 lb CO_2e = 37,120 lb CO_2e. H_2O for ethanol: 52 bbl x 42 gal/bbl x 1,220 gal/gal = 2.66M gal. (US average corn ethanol water footprint is 1,220 gal/gal, per Winnie Gerbens-Leenes et al., "The Water Footprint of Bioenergy," *Proceedings of the National Academy of Sciences* 106, no. 25 [3 June 2009]: 10219–23, http://www.pnas.org/cgi/doi/10.1073/pnas.0812619106). H_2O for diesel: 32 bbl x 42 gal/bbl x 6.6 gal /gal = 8,870 gal. Total H_20 = 2.66M + .009M = 2.67M gal (gasoline water footprint is 6.6 gal /gal, per Wu and Yiwen, *Consumptive Water Use*).

51. Hall et al., "Seeking to Understand the Reasons for Different Energy Return on Investment (EROI) Estimates for Biofuels."

52. *Annual Energy Review 2011* (Washington: Energy Information Agency, September 2012), http://www.eia.gov/totalenergy/data/annual/pdf/aer.pdf.

53. E. C. Sherrard and F. W. Kressman, "Review of Processes in the United States Prior to World War II," *Industrial & Engineering Chemistry* 37, no. 1 (January 1945): 5–8, http://pubs.acs.org/toc/iechad/37/1.

54. The threshold test for any candidate for primary energy source or fuel is demonstrating the ability to bootstrap itself up in scale and energy productivity without outside assistance with an EROI greater than 6:1. To be commercially competitive it must match or exceed the current national average (approximately 12:1 for the United States). A true twenty-first-century fuel must deliver enough energy profit to build up its own production and distribution infrastructure just as coal and oil did in the previous two centuries. Such a test quickly reveals that the quality of energy measured in such things as EROI, energy density, power density, and *dispatchability* (controllability of energy delivery location, time, and rate) matter just as much as total power output. Until this level of performance is achieved, the energy candidate is a research and development experiment that cannot survive without subsidy. Conversely, any energy candidate that is receiving a net subsidy is by definition not an energy source.

55. For the firmly established correlation between EROI and price, see C. W. King and C. A. S. Hall, "Relating Financial and Energy Return on Investment," *Sustainability* 3, no. 10 (October 2011): 1810–32; and Murphy et al., "New Perspectives on the Energy Return on (Energy) Investment (EROI) of Corn Ethanol."

56. An alternative source of hydrogen is electrolysis from water. This could only be done with massive new sources of electrical power. If such power were available, we would use the resulting hydrogen directly as fuel and not bother with the less-efficient process of growing biomass for conversion into biofuels.

57. *Energy for the Warfighter: Operational Energy Strategy* (Washington: DoD, May 2011), http://energy.defense.gov/Operational_Energy_Strategy.pdf.

58. David Miller, "Biofuels Conference: Secretary of the Navy Says Military Can Lead the Way in Alternative Energy," *Dispatch* (Starkville, MS), 7 October 2011, http://www.cdispatch.com/news/article.asp?aid=13418.

59. $26.75 per gallon for Dynamic Fuels biofuel x 42 gal/bbl = $1,123.50 per barrel. Highest price paid was $4,454.55 per gallon = $187,089.00 per barrel. See fig. 5 for details.

60. Contract quantity and price data are from official government websites in 2012 and tabulated by contract number in fig. 4. Sources include General Services Administration's "Federal Procurement Data System—Next Generation" search page, https://www.fpds.gov/fpdsng_cms/; *FedBizOpps* search page, https://www.fbo.gov/; "Bulk Petroleum Contract Awards," Defense Logistics Agency: Energy, http://www.energy.dla.mil/bulk_petroleum/Pages/Contract_Awards.aspx; and Defense Logistics Agency: Energy, *Fact Book: Fiscal Year 2011*, http://www.energy.dla.mil/energy_enterprise/Documents/Fact percent20Book percent20FY2011 percent20Rev.pdf.

61. Ray Mabus, Steven Chu, and Thomas J. Vilsack, "Memorandum of Understanding between the Department of the Navy and the Department of Energy and the Department of Agriculture," June 2011, http://www.rurdev.usda.gov/SupportDocuments/DPASignedMOUEnergyNavyUSDA.pdf.

62. Neelesh Nerurkar, *US Oil Imports: Context and Considerations* (Washington: CRS, April 2011).

63. See "Direct Federal Financial Interventions and Subsidies in Energy in Fiscal Year 2010," Energy Information Agency, July 2011, http://www.eia.gov/analysis/requests/subsidy/; and *Annual Energy Review 2011*. Subsidy amounts in table ES2 from the first reference are divided by 2010 data for US energy production for the respective forms of energy in the second reference.

64. DoE, "Energy.gov/List of Awardees," December 2011, http://energy.gov/sites/prod/files/recoveryactfunding.xls.

65. "AAA's Daily Fuel Gauge Report," American Automobile Association, 19 July 2012, http://fuelgaugereport.opisnet.com/index.asp.

66. A gallon of ethanol contains only two-thirds the energy of a gallon of gasoline; if priced at energy parity, it would be two-thirds the price. The 2010 average retail gasoline price (minus 18.4 cent/gal federal excise tax) = $2.58/gal x 2/3 = $1.72/gal (what ethanol should have cost). The 2010 average retail E85 price = $2.40/gal (what retail ethanol did cost to a close approximation). How much consumers overpaid at pump = $2.40/gal – $1.72/gal = $0.68/gal x 12 billion gallons blended in 2010 = $8.1 billion. For prices and tax credits see table 17-1 and footnotes in Office of Management and Budget, *Budget of the U.S. Government: Analytical Perspective Fiscal Year 2012* (Washington: OMB, 2011); and table A12 of "Annual Energy Outlook 2012," Energy Information Agency, June 2012, http://www.eia.gov/forecasts/aeo/pdf/0383(2012).pdf.

67. Steve Hargreaves, "Gasoline: The New Big U.S. Export," *CNN Money*, 5 December 2011, http://money.cnn.com/2011/12/05/news/economy/gasoline_export/index.htm.

68. The 2009 tax data is presented by the EIA as it was the most recent available. That was a particularly bad year for IRS revenue from oil company taxes because of the economic crash; 2010 data is likely much higher. Oil companies paid $13.7 billion in corporate taxes, and consumers paid $42.4 billion in excise taxes, for a total of $56.1 billion in federal government revenues, per "EIA Financial Reporting System Survey, Form EIA-28 Schedule 5112, Analysis of Income Taxes," *Energy Information Agency*, 2009, ftp://ftp.eia.doe.gov/pub/energy.overview/frs/s5112.xls. Dividing $56.1 billion by the 6.23 billion barrels of oil and gas produced domestically in 2010 yields $9.01 per barrel. Federal excise taxes paid by consumers at the pump were 18.4 cents per gallon for gasoline and 24.4 cents per gallon for diesel.

69. "Market Cap Stock Rankings for Major Integrated Oil & Gas Industry," *YCharts*, 7 January 2013, http://ycharts.com/rankings/industries/Major%20Integrated%20Oil%20&%20Gas/market_cap.

70. See note 18 for solar power density derivation. Wind power density of 1.13 W/m^2 based on recent NREL data reporting 2.9 W/m^2 peak and 39 percent capacity factor as averaged across 2000–2009 US installations with nameplate capacity >20MW. See Paul Denholm et al., *Land-Use Requirements of Modern Wind Power Plants in the United States*, NREL, August 2009, www.nrel.gov/docs/fy09osti/45834.pdf. Corn ethanol power density of 0.315 W/m^2 based on 500 gal/acre-year, @ 76,321 BTU/gal LHV. Soy biodiesel power density of 0.069 W/m^2 based on 70 gal/acre-year @ 119,545 BTU/gal LHV. Average US crude oil well in 2011 produced 10.6 bbl/day @ 129,667 BTU/gal on a two-acre parcel of land, which equates to ~90 W/m^2. See *Annual Energy Review 2011*.

71. Patzek, "Probabilistic Analysis of the Switchgrass Ethanol Cycle."

72. John Jeavons, *How to Grow More Vegetables: And Fruits, Nuts, Berries, Grains and Other Crops Than You Ever Thought Possible on Less Land Than You Can Imagine*, 6th ed. (Berkeley, CA: Ten Speed Press, 2004).

73. DoE NREL research has calculated the best case for algae yields from pure solar energy without fossil fuel or sugar energy augmentation to be 6,500 gal/acre-yr biodiesel = 17.8 gal/acre-day = 6.42 W/m^2 LHV. Sapphire Energy projects it will achieve 14 gal/acre-day of algae biodiesel from 300 acres by 2014. See "In Race to Algae Fuel, Sapphire Scores Point for Open Ponds," *Sapphire Energy*, 6 September 2012, http://www.sapphireenergy.com/news-article/1135734-in-race-to-algae-fuel-sapphire. Algenol, using cyanobacteria animal algae instead of microphyte plant algae, and producing ethanol instead of lipids, recently announced it achieved 21.9 gal/acre-day of ethanol. This is equivalent to 5.6 W/m^2 and still below today's PV solar. See Paul Woods, "About Algenol," Algenol Biofuels, 27 September 2012, http://www.algenolbiofuels.com/.

74. See Robert Perlack et al., *Biomass as Feedstock for a Bioenergy and Bioproducts Industry: The Technical Feasibility of a Billion-Ton Annual Supply* (Oak Ridge, TN: DoE, 2005), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA436753; and Perlack and B. J. Stokes (leads), *U.S. Billion-Ton Update: Biomass Supply for a Bioenergy and Bioproducts Industry* (Oak Ridge: DoE, 2011), http://www1.eere.energy.gov/biomass/pdfs/billion_ton_update.pdf.

75. Blue Sugars Corporation, http://bluesugars.com/index.htm.

76. Klaus Deininger et al., *Rising Global Interest in Farmland* (Washington: World Bank, 2011).

77. Raphael Slade et al., *Energy from Biomass: The Size of the Global Resource* (London: UK Energy Research Centre, 2011).

78. Govinda Timilsina et al., *The Impacts of Biofuel Targets on Land-Use Change and Food Supply*, Iowa State University working paper, December 2010, http://www.econ.iastate.edu/sites/default/files/publications/papers/p12206-2010-12-15.pdf.

79. *The State of Food Insecurity in the World* (Rome: Food and Agriculture Organization of the United Nations, 2011), http://www.fao.org/docrep/014/i2330e/i2330e.pdf.

80. Timilsina et al., *Biofuels*.

81. *Price Volatility in Food and Agricultural Markets: Policy Responses* (Paris: Organisation for Economic Co-operation and Development, 2011).

82. Lester R. Brown, "The New Geopolitics of Food," *Foreign Policy*, May 2011, http://www.foreignpolicy.com/articles/2011/04/25/the_new_geopolitics_of_food.

83. Melissa C. Lott, "The U.S. Now Uses More Corn for Fuel than for Feed," *Scientific American*, 7 October 2011, http://blogs.scientificamerican.com/plugged-in/2011/10/07/the-u-s-now-uses-more-corn-for-fuel-than-for-feed/.

84. David Pimentel et al., "Report of the Gasohol Study Group," Energy Research Advisory Board, 29 April 1980.

85. Simon Eggleston et al., eds., *2006 IPCC Guidelines for National Greenhouse Gas Inventories*, 5 vols. (Hayama, Japan: Institute for Global Environmental Strategies, 2006); and Timothy Searchinger et al., "Fixing a Critical Climate Accounting Error," *Science* 326, no. 5952 (23 October 2009): 527–28. http://www.sciencemag.org/content/326/5952/527.

86. For examples of recent studies finding that biofuels increase GHG and environmentally damaging emissions, see William K. Jaeger and Thorsten M. Egelkraut, "Biofuel Economics in a Setting of Multiple Objectives and Unintended Consequences," *Renewable and Sustainable Energy Reviews* 15, no. 9 (December 2011): 4320–33, http://www.deepdyve.com/lp/elsevier/biofuel-economics-in-a-setting-of-multiple-objectives-and-unintended-8FJ7IumYTW; Yi Yang et al., "Replacing Gasoline with Corn Ethanol Results in Significant Environmental Problem-Shifting," *Environmental Science & Technology* 46, no. 7 (5 March 2012): 3671–78, http://pubs.acs.org/doi/abs/10.1021/es203641p; Keith Smith and Timothy Searchinger, "Crop-based Biofuels

and Associated Environmental Concerns," *GCB Bioenergy*, 7 June 2012; Thomas Walker et al., *Biomass Sustainability and Carbon Policy Study* (Brunswick, ME: Manomet Center for Conservation Sciences, June 2010), http://www.manomet.org/sites/manomet.org/files/Manomet_Biomass_Report_Full_LoRez.pdf; Jörn Scharlemann and William Laurance, "How Green Are Biofuels?" *Science* 319, no. 5859 (4 January 2008): 43–44; DoE, "Ethanol Benefits and Considerations," *Alternative Fuels Data Center*, 28 January 2011, http://www.afdc.energy.gov/fuels/ethanol_benefits.html; and Hill et al., "Environmental, Economic, and Energetic Costs and Benefits of Biodiesel and Ethanol Biofuels."

87. For the negative air quality effects of ethanol as a gasoline additive, see article and supporting references within Pamela Franklin et al., "Clearing the Air: Using Scientific Information to Regulate Reformulated Fuels," *Environmental Science & Technology* 34, no. 18 (4 August 2000): 3857–63, http://dx.doi.org/10.1021/es0010103. For the increased environmental hazard of ethanol-blended fuel spills, see American Institute of Physics, "Mixing Processes Could Increase the Impact of Biofuel Spills on Aquatic Environments," *Phys.Org*, 16 November 2012, http://phys.org/news/2012-11-impact-biofuel-aquatic-environments.html.

88. Jonathan Lewis, *Leaping before They Looked: Lessons from Europe's Experience with the 2003 Biofuels Directive* (Boston: Clean Air Task Force, October 2007).

89. New record highs of 1.65 trillion barrels of proved reserves (1.9 percent annual increase) and 83.56 million bbl/day of production (1.3 percent annual increase) were set in 2011. Reserves have been growing faster than consumption since 1980. See *BP Statistical Review of World Energy June 2012*, British Petroleum, http://www.bp.com/liveassets/bp_internet/globalbp/globalbp_uk_english/reports_and_publications/statistical_energy_review_2011/STAGING/local_assets/pdf/statistical_review_of_world_energy_full_report_2012.pdf.

90. Thomas Homer-Dixon, *The Upside of Down: Catastrophe, Creativity and the Renewal of Civilization* (London: Island Press, 2006).

91. Tom Gleeson et al., "Water Balance of Global Aquifers Revealed by Groundwater Footprint," *Nature* 488, no. 7410 (9 August 2012): 197–200, http://www.engr.scu.edu/~emaurer/classes/ceng139_groundwater/handouts/gleeson_groundwater_footprint_nature_2012.pdf.

92. See Lisa Henthorne, "The Current State of Desalination," November 2009; and "Water and Oil and Gas," *Desalination* 48, no. 39 (8 October 2012), http://www.desalination.com/wdr/48/39/and-oil-and-gas.

93. Tim Padgett, "The Postquake Water Crisis: Getting Seawater to the Haitians," *Time*, 18 January 2010, http://www.time.com/time/specials/packages/article/0,28804,1953379_1953494_1954584,00.html.

94. "Desalination Industry Enjoys Growth Spurt as Water Scarcity Starts to Bite," *AMEinfo*, 30 September 2012, http://www.ameinfo.com/desalination-industry-enjoys-growth-spurt-water-313351.

95. Al Shoaiba and two-thirds of Saudi desalination plants are multistage flash distillation technology, which require about 186 MJ energy input per cubic meter of water output. See Neil M. Wade, "Distillation Plant Development and Cost Update," *Desalination* 136, no. 1–3 (1 May 2001): 3–12, http://www.desline.com/articoli/4051.pdf.

96. Wu and Chiu, *Consumptive Water Use in the Production of Ethanol and Petroleum Gasoline*. Values adjusted by a two-thirds multiplier to correct for the lower energy density of ethanol vs. gasoline.

97. Gerbens-Leenes et al., "Water Footprint of Bioenergy."

98. Wade, "Distillation Plant Development and Cost Update."

99. Barack Obama, *Executive Order 13603—National Defense Resources Preparedness*, 16 March 2012, http://www.whitehouse.gov/the-press-office/2012/03/16/executive-order-national-defense-resources-preparedness.

100. For two examples of ongoing research to photosynthesize fuel by directly recycling CO_2 and H_2O without making biomass, see Bill Scanlon, "Sun Shines on Old Idea to Make Hydrogen," *Renewable Energy World*, 5 November 2012; and "Sunshine to Petrol," Sandia National Labs, 9 November 2012, http://energy.sandia.gov/?page_id=776.

101. T. J. Blasing, "Recent Greenhouse Gas Concentrations," Carbon Dioxide Information Analysis Center, February 2012, http://cdiac.ornl.gov/pns/current_ghg.html.

102. N_2O and CO_2 have the same molecular mass of 44 Dalton, and their per-ton global warming contributions are in the direct ratio of the global warming potentials of their molecules (i.e., 298:1). CH_4 has a molecular mass of 16 Dalton and thus there are 44/16 more molecules per ton, each with a 25:1 increase in global warming potential, for a total increase in per-ton global warming potential of 69:1.

103. Energy Independence and Security Act of 2007, §526:

> No Federal agency shall enter into a contract for procurement of an alternative or synthetic fuel, including a fuel produced from nonconventional petroleum sources, for any mobility related use, other than for research or testing, unless the contract specifies that the lifecycle greenhouse gas emissions associated with the production and combustion of the fuel supplied under the contract must, on an ongoing basis, be less than or equal to such emissions from the equivalent conventional fuel produced from conventional petroleum sources. . . .
>
> No later than Oct. 1, 2015, and for each year thereafter, each Federal agency shall achieve ≥ 20 percent reduction in annual petroleum consumption and a 10 percent increase in annual alternative fuel consumption, relative to FY2005 baseline.

Summer 2013

Assessing the US "Pivot" to Asia

There has been much commentary since President Obama's tour of the Asia-Pacific region in November 2011 of a US "return," strategic "pivot," or "rebalancing" to Asia.[1] Much of this commentary comes from Asian and European commentators—Asians have been generally welcoming, while many Europeans express fears that the new strategic emphasis will downgrade the traditional importance of transatlantic ties. Despite widespread endorsement of the strategic shift within Asia, China has been notably critical of the new policy—as virtually all Chinese strategists and pundits see the initiative as thinly veiled "containment" of China. While there has been much commentary abroad, there has been surprisingly less in US media, academic, think-tank, or government circles. Much of the domestic commentary has been critical of the use of the term *pivot* for signaling a downgrading of other regions (notably Southwest Asia, the Middle East, and Europe) in US strategic priorities—and this criticism put the Obama administration on the defensive. The administration tried to recast the new initiative as a rebalancing without "abandoning" long-standing commitments elsewhere in the world. This essay goes beyond this reactive commentary, taking stock of Washington's new strategic initiative by viewing it historically, describing its different components, and assessing the positive possibilities and potential pitfalls.

Is the Policy Really New?

The new Asia pivot is both new and not new. That is, the Asia-Pacific region has long been a high priority for the United States, but not always the *highest* priority.

On the one hand, with the new so-called pivot, the United States *has* embarked on a qualitatively new strategic prioritization by emphasizing and increasing resources devoted to diplomacy, commerce, and security in the Asia-Pacific region. The Obama administration is the first administration ever to explicitly elevate Asia to the primary global regional strategic priority. This *is new* for the United States, which has long prioritized its transatlantic ties, the Middle East, or previously, Latin

America. Even at the height of the Vietnam War and the Cold War containment of China during the Kennedy and Johnson administrations, Washington still maintained its overall priority on the western front—the Cold War confrontation in Europe versus the Soviet Union.[2] Since 2001, the main strategic orientation during the "war(s) on terrorism" has been Southwest Asia. The Middle East has also been a long-standing strategic priority for the United States.

On the other hand, it is important to note that what we are witnessing is a *relative* shift, not a fundamental one. This is because of the well-established involvement of the United States in Asia that dates back many decades, indeed centuries. The United States has been a Pacific power since the turn of the last century—in the wake of the Spanish-American War of 1898 and Secretary of State John Hay's "Open Door Notes" of 1899–1900. Even more than a century before, with the sailing of the clipper ship *Empress of China* in 1784 from New York to Guangzhou, China, the United States established itself as a major commercial actor in the region. Thereafter, during the nineteenth century, a US diplomatic, cultural, and religious (missionary) presence was established in East Asia. This, in turn, triggered growing Asian immigration to the United States.

Since then, the United States has long been an Asia-Pacific nation by virtue of geography, ethnicity, commerce, culture, diplomacy, and security engagements. Its post–Korean War involvement in the Asia-Pacific region has been both deep and sustained. It is anchored on five enduring bilateral alliances, a series of strong strategic partnerships, intensive bilateral and multilateral diplomacy, deep cultural ties, enormous "soft power," and a growing Asian-American population. Thus, if viewed historically, the pivot is not so new—as US ties to, and roots in, the region run deep. Consider some of these elements in a more contemporary context.

Economic Interests

Asia is the United States' most important economic partner and has been for more than three decades. The region surpassed Europe as our leading trade partner in 1977. Today the United States has more than twice as much trade with Asia as with Europe. In 2012, US trade with Asia totaled a stunning $14.2 trillion.[3] Since 2000, Asia has become our largest source of imports and second largest export market (outside

North America). By 2010, Asia accounted for 32.2 percent of US total merchandise trade worldwide. US exports to Asia totaled $457.2 billion in 2012. Today, the United States trades more with South Korea than with Germany, more with Singapore than with France, and more with Japan than with the United Kingdom, Germany, and France combined. China and Japan are the second and third largest trade partners for the United States. Asia is also our most important export market—nine of the United States' top 20 national export markets are now in Asia, and approximately one-third of all US overseas sales go to Asia. Growth in exports to China has been the fastest worldwide for the past five years. If East Asia continues to post only 5.5 percent growth in Gross Domestic Product (GDP), US exports to Asia are estimated to contribute 5 percent to US GDP. According to US government statistics, this translates into 4.6 million jobs domestically per annum.

The flipside of this, of course, is the huge trade *deficits* the United States accumulates with the region—particularly with China ($282 billion in 2011 alone). Overall, the United States imported $966.4 billion from Asia in 2012, leaving a whopping $509.2 billion trade deficit.[4]

US economic and commercial ties to the Asia-Pacific region are growing deeper by the day. Bilateral free trade areas (FTA) and the prospect of the multinational Trans-Pacific Partnership (TPP) will bind the United States even more deeply with partner economies in the region (currently, 11 nations are negotiating to bring the TPP into force).

Cultural Interests

We should also note the significant cultural impact across Asia. US culture—films, sports, authors, musicians, fashion, dance, innovation, and so forth—has long attracted Asian interest. One recent indication of US impact in Asia is the 2008 Chicago Council on Global Affairs unprecedented survey of "soft power in Asia."[5] The council developed a complex set of 70+ metrics to measure a soft power index in five categories. Many interesting findings emerged from this survey—conducted in the United States, South Korea, Japan, China, Indonesia, and Vietnam—but one of the most important concerned the overall strength of US soft power in the region (see following table).

Relative soft power in Asia (2008)

Survey Countries	United States soft power	China soft power	Japan soft power	South Korea soft power
United States	—	.47	.67	.49
China	.71	—	.62	.65
Japan	.69	.51	—	.56
South Korea	.72	.55	.65	—
Indonesia	.72	.70	.72	.63
Vietnam	.76	.74	.79	.73

Reprinted from Chicago Council on Global Affairs, ***Soft Power in Asia: Results of a 2008 Multinational Survey of Public Opinion.***

Of course, a long-standing and key element of US cultural engagement with Asia has been higher education, with US efforts spanning a century to build modern universities, medical, and other professional schools. Even more important, particularly in the post–World War II era, has been US university training of generations of Asians in a wide variety of fields, many of whom have become private and public sector leaders in their native countries. In the 2011–12 academic year, 489,970 Asian students were enrolled in US universities. The People's Republic of China led the way with 194,029, followed by 100,270 Indian students and 72,295 South Koreans.[6] US educators also fan out across Asia, teaching in a wide range of Asian universities and vocational schools. The Fulbright Program remains the flagship sponsor, sending US professors and students to Asia and bringing Asians to the United States to teach and study.[7]

One can offer many other examples of US cultural and intellectual engagement with Asia (not the least of which is film, literature, arts, and sports). But this is not to say all has been positive, as a distinct paternalism and cultural arrogance has sometimes been apparent on the part of Americans in Asia. On the whole, the United States is deeply and positively culturally engaged in Asia.

Diplomacy

Generally speaking, despite the importance of Asia to the United States, our diplomatic attention to the region has often been highly episodic, sometimes neglectful, and not always deeply engaged—particularly in Southeast Asia. US presidents have been infrequent visitors to Asia, while cabinet secretaries have been slightly more engaged but not as regularly with their counterparts as they could or should be. Before President Obama took office, Association of Southeast Asian Nations (ASEAN) leaders and publics complained about the relative lack of interest from Washington. But the Obama administration has made this a high priority and thus alleviated some of the sense of neglect. The administration has tried hard to reverse this perception. Secretary of State Hillary Clinton was, by far, the best traveled ever in the region, having visited virtually every country across the vast Asia-Pacific. Significantly, Secretary Clinton took her first trip abroad to Asia and returned more than a dozen times in four years. This included resuming regular and symbolically important attendance by the secretary of state at the ASEAN Regional Forum Annual Meeting.

President Obama himself has made Asia *the top* US foreign policy priority. As he said in his speech unveiling the pivot to the Australian Parliament on 17 November 2011, "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." President Obama has visited the region at least annually since taking office. This includes the first-ever attendance by a US president at the East Asian Summit and the ASEAN leaders meeting, hosting the 17th Asia-Pacific Economic Cooperation leaders meeting, and paying individual visits to Japan, South Korea, China, Australia, Indonesia, Singapore, and India. At a more local level, US embassies and diplomats throughout the region are—after a long dormancy—beginning to display a new proactivity, even if the embassies themselves remain fortresses.

Secretary Clinton described this new diplomatic engagement as "forward deployed diplomacy." In a key *Foreign Policy* magazine article, she outlined six elements of this regional diplomacy:

- strengthening bilateral security alliances;
- deepening working relationships with emerging powers, including China;
- engaging regional multilateral institutions;
- expanding trade and investment;
- forging a broad-based military presence; and
- advancing democracy and human rights.[8]

We have seen the Obama administration work to strengthen bilateral relations with just about every country in the region since entering office. Nations long neglected by Washington—like New Zealand, Indonesia, the Philippines, and small Pacific island states—have received high-ranking US official visits. Perhaps the most noteworthy is Burma (Myanmar), where the administration has fundamentally shifted from a policy of isolation to engagement.

Regional powers India and China have also received sustained US diplomatic attention. There is literally no country in the world with which the US government and society is more deeply engaged than the People's Republic of China. Reflecting this, the United States and China maintain more than 60 annual official dialogue mechanisms, while the US Embassy in Beijing now has the largest staff in the world—1,400. Building comprehensive and deep relations with India has also become a significant priority for the United States. President Obama has described the US relationship with India as a "defining partnership of the 21st century." Washington and New Delhi are now engaged in deepening and expanding a variety of bilateral, regional, and global interactions.

At the same time, an intensification of US engagement in multilateral diplomacy throughout the Asia-Pacific region is also apparent. By signing and acceding to the Treaty of Amity and Cooperation, the United States is now a full participant in the East Asian Summit, and we have witnessed a new surge of US participation in the "spaghetti bowl" of regional intergovernmental and Track II organizations. Previously, Washington was frequently (and appropriately) criticized for "not showing up" at regional multilateral and "minilateral" forums—but the Obama administration has tried to reverse this perception.

While the new thrust of US diplomacy in the region is to be welcomed, it cannot be taken for granted. It requires constant attention, diplomats knowledgeable of regional and national dynamics, and sustained allocation of resources. It also requires subtlety—something at which US diplomacy has not always excelled. Because Northeast Asia, Southeast Asia, South Asia, Central Asia, and Austral-Asia all have very different dynamics, ethnicities, subregional institutions, traditions, and relations with each other, different parts of the region require nuanced and differentiated policies.

One of the big stories of recent years in Asian international relations is the increasing *integration* across and among these five subregions. They used to act quite autonomously, but no longer. Today, they are increasingly tied together via an intricate web of interstate and substate relations.[9] Despite these increasing intraregional interactions, Asia remains remarkably diverse in all respects—politically, economically, religiously, ethnically, culturally, and militarily. To be effective in the years ahead, US diplomacy must both grasp the integrative forces—and become part of them—as well as appreciate and respect intraregional differences.

Security Engagement

Finally, let us consider the security dimension of US engagement with the region. It may seem obvious or even trite, but maintaining regional security and stability is absolutely fundamental to advancing the totality of US interests in the region—economic, cultural, and diplomatic—as well as advancing the broader public goods of regional interactions. As Joseph Nye astutely observed, the US contribution to regional security is the "oxygen" that permits the region to "breathe" and thrive. Without it, quite simply, the Asia-Pacific would very likely not have developed so dramatically over the past quarter century.

Providing security and stability has at least four dimensions:

1. preventing the rise of a regional hegemon hostile to US interests;
2. preventing major power rivalry and polarization of the region;
3. preventing internal political-socioeconomic crises from spilling outside national borders, thus causing destabilizing effects in the region; and
4. enabling working relationships with others to jointly manage an increasing range of transnational nontraditional security challenges.

In each of these areas, the United States maintains a "hub-and-spoke" regional security architecture that includes at least five levels of security:

1. A unilateral, forward-deployed military presence including approximately 325,000 military and civilian personnel in the Pacific theater. The Pacific Fleet alone includes six aircraft carrier battle groups (CVBG), approximately 180 ships and submarines, 1,500 aircraft, and 100,000 personnel. The US military stations 16,000 personnel at sea, 40,000 in Japan, 28,500 in South Korea, 500 (rotationally) in the Philippines, 4,500 in Guam (to grow to 9,000), and 250 Marines in Australia (to grow to 2,500). US forces are forward deployed in

Hawaii, Guam, the Mariana Islands, Japan, South Korea, Australia, and Kyrgyzstan. Former Secretary of Defense Leon Panetta stated the United States will now keep 60 percent of its naval assets in Asia.

2. Five long-standing bilateral alliances with Japan, the Republic of Korea, the Philippines, Thailand, and Australia.
3. Nonallied but strong "security partnerships" with Singapore, New Zealand,[10] and India (and increasingly with Malaysia, Mongolia, and Vietnam).
4. Participation in a wide range of multilateral security arrangements, multinational exercises, intelligence sharing, and professional military education (such as IMET and the Asia-Pacific Center for Security Studies).
5. Bilateral security and military exchanges with countries that are neither allies nor strategic partners, such as the People's Republic of China.

Through these means, the United States contributes to a robust set of security engagements throughout the region. Moreover, the US Pacific Command (PACOM) maintains a strong forward presence and wide range of interregional cooperative programs it calls "presence with a purpose."[11] Its five specific missions are somewhat duplicative of those above and include (1) strengthening advancing alliances and partnerships, (2) maturing the US-China military relationship, (3) developing the US-India strategic partnership, (4) remaining prepared to respond to a Korean Peninsula contingency, and (5) countering transnational threats.

Meeting these challenges and fulfilling these missions will require resources and sustained effort. Although we can expect US defense spending to contract over the coming years, President Obama himself has made it clear that cuts will not come from the Asia-Pacific theatre, pointing out in his address to the Australian Parliament:

> So, here is what this region should know. As we end today's wars, I have directed my national security team to make our presence and mission in the Asia-Pacific a top priority. As a result, reductions in U.S. defense spending will not—I repeat, will not—come at the expense of the Asia-Pacific. My guidance is clear.[12]

Thus, we see a clear continued US commitment to undergird the security architecture in the region. However, it is important to emphasize that this robust and multifaceted set of security commitments should not be viewed in isolation. They are important, but they are only part of the more comprehensive economic, cultural, and diplomatic engagement the United States has with Asia.

Concluding Perspectives

The pivot—or rebalancing—is *not* a new policy; it is a deepening and broadening of previous commitments. Part of this broadening includes a geographic expansion of sorts—by including India and the Indian Ocean in the broader Asia initiative. Thus, it is not just an East Asia initiative: US-India relations are growing very robustly and positively even though the five bilateral alliances remain the bedrock of US relations in the region. Engagement of China also continues as a central element in US strategy and diplomacy.

Despite the continuation and deepening of these previous commitments, the new pivot policy nonetheless *does* illustrate a new level of commitment—and it also indicates a new level of strategy. The resources devoted to the Asia-Pacific are being increased—both absolutely and relatively vis-à-vis other regions of the world, with Southeast Asia and the South Pacific receiving new attention. It is also very important to recognize that the new pivot policy is *not* being unilaterally thrust upon Asian nations by the United States—quite the contrary. Although the Obama administration began planning the reorientation as soon as it entered office in 2009, with an eye toward winding down the wars in Iraq and Afghanistan, it was the 2009–10 "year of assertiveness" by China that triggered many Asian states to grow sharply concerned about Beijing and therefore ask Washington to increase its presence and attention to the region. Thus, to the extent China is an element of focus in the pivot strategy (and it is), Beijing's own assertive behavior is the cause.

The new strategic reorientation to the Asia-Pacific should work well as long as the United States does several things:

- Allocates sustained resources necessary to the effort;
- Maintains sustained diplomatic attention to the effort;
- Balances bilateral ties with multilateral ones;
- Does not premise the policy on countering China (although, to be sure, "balancing" China—which is different from "containing" China) and continues to engage the PRC in a comprehensive fashion.

> No Asian nation wishes to be drawn into an anti-China coalition or be put in the position of "choosing" between Washington and Beijing. The pivot must, therefore, be an inclusive effort that tries to involve and integrate China into the regional order. Any US regional policy premised *against* China will fail.

As long as the United States takes care of these points, it should achieve a successful strategy which will work not only to its own benefit, but also the broad stability, security, and prosperity of the Asia-Pacific region.

David Shambaugh
Professor of Political Science and International Affairs
George Washington University
Nonresident Senior Fellow Center for Northeast Asian Policy Studies
The Brookings Institution

Notes

[1] All three of these terms have been used to describe the new (re)prioritization in US foreign and national security policy.

[2] See Tsuyoshi Hasegawa, ed., *The Cold War in East Asia, 1945–1991* (Stanford, CA: Stanford University Press, 2011).

[3] "2012: U.S. Trade in Goods with Asia," http://www.census.gov/foreign-trade/balance/c0016.html.

[4] Ibid.

[5] Chicago Council on Global Affairs, *Soft Power in Asia: Results of a 2008 Multinational Survey of Public Opinion*, http://www.thechicagocouncil.org/UserFiles/File/POS_Topline%20Reports/Asia%20Soft%20Power%202008/Chicago%20Council%20Soft%20Power%20Report-%20Final%206-11-08.pdf.

[6] Institute for International Education, *Open Doors 2011–2012*, http://www.iie.org/Research-and-Publications/Open-Doors/Data/Fact-Sheets-by-Region/2012.

[7] The author spent the 2009–10 academic year as a Senior Fulbright Research Scholar in China.

[8] Hillary Rodham Clinton, "America's Pacific Century," *Foreign Policy*, 11 October 2011.

[9] See David Shambaugh, "International Relations in Asia: The Two-Level Game," in *International Relations of Asia*, ed. Shambaugh and Michael Yahuda (Lanham, MD: Rowman & Littlefield Publishers, 2008).

[10] Technically New Zealand and the United States remain members of ANZUS, but the military component of this alliance has been attenuated since 1976.

[11] See http://www.pacom.mil/about-uspacom/presence-with-a-purpose/index.shtml.

[12] The White House, "Remarks by President Obama to the Australian Parliament," 17 November 2011.

Summer 2013

US Grand Strategy, the Rise of China, and US National Security Strategy for East Asia

Robert S. Ross

In the twenty-first century, the foremost US national security interest remains what it has been since 1776—to ensure a balance of power in its two transoceanic flanking regions that keeps them internally divided. US security has continually depended on this balance of power to prevent European and East Asian powers from considering expansion into the Western Hemisphere. Whereas, in the early years of the republic, the United States could count on power balancing among European and East Asian great powers, since World War II, it has had to participate directly in balance-of-power politics in both regions. During the Cold War, it faced challenges in Europe and East Asia that required simultaneous strategic engagement in both regions.

The current balance-of-power challenge for the United States is in East Asia. Unless balanced by the United States, China's rise could yield regional hegemony. None of its Asian neighbors has the resources necessary to balance China's rise. Japan's decline has been precipitous, and China's other neighbors are too small to present a challenge. A balance of power in East Asia will require direct US strategic involvement to maintain a divided region.

During the first term of the Obama administration, the United States undertook a strategic initiative to strengthen its presence in East Asia. Often called the US "pivot" toward East Asia, this policy has been characterized by development of enhanced strategic cooperation with a wide

Robert S. Ross is a professor of political science at Boston College, an associate at Harvard University's Fairbank Center for Chinese Studies, and senior advisor to the Massachusetts Institute of Technology security studies program. His research focuses on Chinese security policy and East Asian security, including China's use of force and the role of nationalism in its defense policy. His recent publications include *Chinese Security Policy* (Routledge, 2009) and *Twenty-First Century Seapower: Cooperation and Conflict at Sea* (Routledge, 2012).

range of East Asia countries, including traditional allies and new security partners. In many ways the pivot to East Asia has redefined US policy there, with potential implications for great-power relations and regional stability.

The first part of this article examines the underlying and fundamental national security interests that have informed US grand strategy since the nation's founding and its implications for US national security interests in East Asia, both in the past and in the twenty-first century. The second part considers the long-term implications of the rise of China and post–Cold War objectives and policies that have sustained the regional balance of power. The third part looks at the Obama administration's pivot to East Asia and its implications for US-China cooperation and for US national security interests. The article concludes by examining implications of the pivot strategy for balancing the rise of China and the long-term prospects for US security and regional stability.

US Grand Strategy since 1776

Fundamentally, US national security interest in East Asia is no different than in Europe. Both regions are contiguous to the oceans that border US coastal regions—Europe across the Atlantic Ocean and East Asia across the Pacific. Because these two major regions flank the North American coasts, US security policy since its founding has depended on balance-of-power politics in these regions and the strategic imperative of a divided Europe and a divided East Asia, lest a regional hegemon develop the capability and the ambition to reach across the oceans and challenge US security.

President George Washington first explained this national security interest in his 1796 Farewell Address. His admonishment to avoid "interweaving our destiny with that of any part of Europe" and its "frequent controversies" did not imply that the United States should not involve itself in the international politics of Europe. On the contrary, he merely warned the United States from engaging in "permanent alliances" and "artificial ties," for such entanglement would constrain its flexibility to maneuver among the contending European states to maximize its security. Flexibility and detachment from European interests would enable the United States to "safely trust to temporary alliances for extraordinary emergencies."[1]

Washington learned the value of "temporary alliances" during his leadership of the war for independence against Great Britain, when the Anglo-French rivalry and corresponding French assistance to US forces were critical to the military successes of the former colonies. This was especially so during the pivotal Battle of Yorktown. Not only did France contribute approximately 40 percent of the troops and much of the heavy armaments deployed in the siege of Yorktown, but it also used its navy to block the British navy from supplying critical reinforcements and aid for its troops, thus contributing to the surrender by Lt Gen Lord Cornwallis in October 1781. The Battle of Yorktown was the last major battle of the war and ultimately persuaded the British to negotiate independence.[2]

The importance of a transoceanic divided flank to the new republic was evident throughout the Napoleonic Wars of the late eighteenth and early nineteenth century. Although the terms of the peace agreement of 1786 called for Great Britain to withdraw its forces from US territory, it continued to deploy them at posts along the Canadian border. Only in 1794, when faced with Napoleon's growing continental coalition, did Great Britain finally agree to the terms of Jay's Treaty, which required it to withdraw its forces from the frontier posts.[3] Spain agreed to US navigation rights on the Mississippi River and settled the US-Spanish boundary dispute (Pinckney's Treaty, 1796) because it feared British retribution after Madrid defected from the Anglo-Spanish alliance and signed a peace agreement with Napoleon.[4] President Thomas Jefferson's opportunity to purchase the French territory of Louisiana in 1803 resulted from the heavy cost of Napoleon's continental ambitions and his need to replenish France's treasury to finance continuation of the war.[5] The United States also benefitted from Anglo-French rivalry during the War of 1812. The young US Navy fared poorly, including in the Battle of New Orleans. Nonetheless, Napoleon's escape from exile on Elba in March 1815 forced Britain to accept a peace favorable to the United States so it could redeploy its forces against a resurgent French army and defeat Napoleon's forces on 18 June 1815 at Waterloo.[6]

The United States continued to benefit from European rivalries through the nineteenth century. Following a series of Southern military victories during the US Civil War, Napoleon III gave serious consideration to intervening on behalf of the Confederacy to alleviate the French shortage of cotton. But in 1862, he told Confederate diplomats that he was too preoccupied with conflicts in Italy and Greece to risk war with the United States. Moreover, he was concerned that if Great Britain did not also intervene in the US Civil War, it would aim to entangle France and thus destroy French commerce.[7] Shortly thereafter, Russian rivalry following the Crimean War and preoccupation with its European security conflicts contributed to its eagerness to sell Alaska to the United States in 1867.[8]

US interests also benefitted from a divided East Asia in the late nineteenth century. In the Spanish-American War of 1898, no European power was willing to support Spain for fear it would undermine security vis-à-vis the other powers. Great Britain played a leading role in blocking European support for Spain, but Germany, France, and Russia were all reluctant to jeopardize their interests in Europe and Asia by assisting Spain.[9] The resulting isolation enabled the United States to defeat the Spanish navy not only in Cuba, but also in the Philippines, where it secured the islands as a colony and established a strategic presence in East Asia. Subsequently, US security benefitted in the early twentieth century from the multiple European countries vying for influence throughout East Asia, including Great Britain, France, Russia, and Germany, as well as Japan. The McKinley administration's "Open Door" policy regarding trade with China was premised on the unwillingness of the many great powers, especially Great Britain, to allow any single power to dominate the Chinese market.[10]

On the other hand, danger clearly emerged for the United States in the absence of balance-of-power politics in its East Asia flanking region following the 1939 battle at Nomonhon and the subsequent 1941 Soviet-Japanese Neutrality Pact. The Soviet Union's preoccupation with German ambitions and its corresponding vulnerability in East Asia led Joseph Stalin to secure the eastern borders by conceding Japan's superiority in Northeast Asia. The resulting absence of a great power that could balance against Japanese regional power encouraged Tokyo to extend its military occupation to all of East Asia and ultimately to send its navy across the Pacific Ocean to launch its preemptive attack on US forces at Pearl Harbor.[11]

The strategic lesson of World War II for the United States was that it could no longer rely on balance-of-power politics to maintain its security by dividing its flanking regions. Instead, it would have to directly involve itself in European and East Asian politics to maintain the balance of power and US national security. It fought World War II to resist

German dominance of Europe.[12] In East Asia it acquiesced to Japanese expansion until Japan moved from occupying simply the Korean Peninsula and China to seeking dominance throughout maritime East Asia, as well.[13] US resistance to German and Japanese expansion thus prevented the emergence of a regional hegemon across its coastal flanks.

In the aftermath of World War II, US policymakers sought the same grand strategy objectives—a balance of power that assured divided regions opposite the eastern and western US coasts. It thus balanced Soviet and Chinese power in Europe and East Asia. For US planners, the lesson of World War II was that the United States could no longer "free-ride" on other powers to assure its security. Rather, it had to assume that responsibility by participating in the balance of power in Europe and East Asia.[14]

US Grand Strategy and the Rise of China

The rise of China poses a challenge to US security in East Asia because, unless balanced, China could achieve regional hegemony. This could occur regardless of Chinese intentions and policies. Given the historical pattern of great-power politics, once China possesses the capabilities to challenge the regional order, it will presumably seek a dominant strategic position throughout East Asia. This has been the European experience, repeated many times over the past 500 years and often characterized by war. It has also been the experience in the Western Hemisphere since 1823, when the United States proclaimed its regional ambitions in the Monroe Doctrine. And it has been the recent experience in South Asia, where only Pakistan's possession of nuclear weapons has prevented India from achieving dominance throughout the subcontinent. Great powers in search of security seek a region-wide sphere of influence. Should China have similar aspirations, it would be neither good nor bad nor reflect hostility toward the United States; it would simply reflect great-power politics. On the other hand, even should China not have aspirations for regional leadership, it will emerge as the regional hegemon unless its rise is balanced by another great power. Local powers, responding to China's growing advantage in the balance of capabilities in the region, will gravitate toward it rather than risk its hostility. In the absence of balancing, the rise of China will challenge a cornerstone of US security—a divided flank across the Pacific Ocean.

The United States requires sufficient military and political presence in East Asia to balance the rise of China and to deter it from using force to achieve regional hegemony, should it become frustrated at the pace of change. US strength will also reassure local powers that their security does not require accommodation to China's rise.[15]

The optimal US grand strategy for East Asia will secure balance-of-power objectives at the least possible cost to US blood, treasure, and honor. To do otherwise would divert scarce strategic resources from capabilities and missions that would better serve US security elsewhere and would undermine achievement of critical nonstrategic objectives, including economic development and social welfare. Balancing China's rise at the least possible cost will require continual modernization of US capabilities while managing US-China relations to avoid unnecessary yet costly conflict. The former is a military challenge; the latter is a political challenge.

US Military Presence in East Asia and Balancing China's Rise

The United States requires sufficient military capability in East Asia to deter China from using force to realize its strategic ambitions and to reassure US security partners that they can rely on the United States to provide for their security against a rising China. This is how to maintain the balance of power in East Asia.

China's long-term strategy to challenge US military presence focuses on access-denial capabilities. Rather than fund a large power-projection and sea-control naval capability dependent on large and numerous surface ships, it has developed low-cost, secure platforms that may challenge the ability of the United States to protect its war-fighting ships, especially aircraft carriers. Chinese efforts primarily focus on the use of relatively quiet and increasingly numerous diesel submarines.[16] By 2000, China's submarine force had awakened concern in the US Navy over the wartime survivability of its surface fleet, especially its carriers. More recently, Chinese research and testing of an antiship ballistic missile system and antiship cruise missiles deployed on submarines and surface ships suggest China may eventually pose an even greater challenge to the US fleet.[17] Should China's People's Liberation Army (PLA) develop an effective intelligence, surveillance, and reconnaissance (ISR) targeting capability to inflict critical attacks on US naval assets, it may be able to deter US intervention in its hostilities with local states or create region-wide doubts that the United States has the resolve to defend their security at the risk of war.[18] If China believes it can deter US intervention, it may be encouraged to use force against US allies.

Over the past 15 years, the United States has responded to Chinese military modernization with an ongoing effort to sustain a military presence in East Asia for power projection. Following the 1996 confrontation in the Taiwan Strait, the Clinton administration initiated the US strategic transition toward East Asia with the first redeployment from Europe to Guam of a *Los Angeles*–class submarine. Since then, the United States has deployed nearly every type of air and naval weapon system to East Asia, including its most modern ones as they come into operation. The US Navy plans to deploy six *Los Angeles*–class submarines to East Asia. It has also deployed the *Virginia*-class submarine and a converted *Ohio*-class SSGN (nuclear-powered, guided-missile-equipped submarine) to East Asia, and it has home-ported an additional aircraft carrier at San Diego for western Pacific operations. As early as 2006, the Department of Defense (DoD) *Quadrennial Defense Review* called for the US Navy to deploy 60 percent of its submarine force and six of its 11 aircraft carriers to the Pacific theater.[19] In addition to its forces based in Japan, the US Air Force has deployed F-15s, F-16s, the B-1 and B-2 bombers, and the F-22 Raptor, its most-advanced aircraft, to Guam. It has also based air-refueling aircraft on Guam and stockpiled air-launched cruise missiles there.[20]

The United States has also strengthened its forward presence in East Asia through cooperation with its regional security partners. Despite domestic political complications in Japan over Marine Corps Air Station Futenma in Okinawa, cooperation has continued to expand between the US and Japanese militaries, including exercises focused on defending Japanese-controlled islands claimed by China. The 1999 completion of the deep-draft-vessel pier at Singapore's Changi port facility provided the US Navy with a modern and comprehensive aircraft carrier facility in the South China Sea. In 2005, Singapore and the United States signed the Strategic Framework Agreement, consolidating defense and security ties and enabling greater cooperation in joint naval exercises.[21] During the George H. W. Bush administration, the United States developed greater defense cooperation with the Philippines. It expanded access for

US naval ships to Philippine waters, and between 2001 and 2005, annual US military assistance to the Philippines increased from $1.9 million to approximately $126 million, making it the largest recipient of US military assistance in East Asia.[22] The US Navy also expanded its access to Malaysia's Port Klang in the Strait of Malacca.[23] More recently, during the Obama administration, the United States further expanded US-Philippine cooperation with increased arms sales, including coastal patrol ships and the expansion of US-Philippine naval exercises, while reaching agreement for US Navy access to its former base at Subic Bay.[24] The administration has also developed improved defense cooperation with Indonesia and New Zealand and reached agreement with Australia for stationing US Marines on its military training base in Darwin.

Ongoing modernization of US defense capability has been especially important for balancing the rise of China. The development of ISR-based weapon systems, including remotely piloted aircraft (RPA) and unmanned underwater vehicles (UUV), is an effective response to China's development of antiship missile capability. These systems will reduce the vulnerability of US regional power-projection operations while contributing to its antisubmarine warfare capability vis-à-vis China's growing and advanced submarine fleet.[25] The deployment of advanced armaments in underwater platforms, including Tomahawk cruise missiles on *Ohio*-class submarines, is a similarly effective response to Chinese military modernization.

US defense modernization has sustained the ability to deter Chinese use of force to challenge the regional order. Although the PLA dominates China's land borders, its navy remains grossly inferior to the US Navy.[26] It continues to depend on small coastal administration and coast guard ships for its maritime activities in disputed waters in the South China Sea, and its antipiracy activities in the Gulf of Aden consist of unsophisticated operations conducted by very few ships. China's surface ship capability remains weak; its new aircraft carrier is undersized, lacks aircraft, and is highly vulnerable to US forces. It is primarily a prestige ship rather than a warfighting ship.[27] China has just begun construction of its next-generation guided-missile destroyer. Both the quantity and quality of these ships will be vastly inferior to US Aegis-equipped destroyers. The DoD reported that in 2011 less than 30 percent of PLA surface forces, air forces, and air defense forces were "modern" and that only 55 percent of its submarine fleet was modern.[28] The recent eagerness of US regional strategic partners to consolidate defense cooperation with the United States reflects its continued dominance vis-à-vis China and confidence that it can provide for their security despite Chinese opposition.

The challenge for the United States in balancing China's military modernization is developing an effective response to its missile program and thus neutralizing a developing access-denial capability. The growing accuracy of China's land-based medium-range missiles increasingly challenges the long-term efficacy of US aircraft carriers.[29] US development of SSGNs, RPAs, and UUVs is an effective response to this problem. Nonetheless, continued US commitment to the aircraft carrier imposes high financial costs on its defense budget that may undermine its long-term ability to contend with Chinese defense modernization, thus undermining US security in East Asia. Although the carrier is an effective platform for maintaining a maritime "presence" in East Asia, evaluation of its financial value ultimately rests on its war-fighting capability compared to the cost and effectiveness of other platforms. Given the carrier's expense and its growing vulnerability to land-based and sea-based missiles, it may become a long-term liability rather than in asset in the effort to balance China's rise. This is especially true given the relative cost advantage of the offense versus the defense in the missile-carrier balance.

Given the growing constraints on the US defense budget, the significant domestic social welfare demands, and the likelihood of slow economic growth, continued funding of aircraft carriers may challenge the US ability to balance China's rise.[30] It will limit funding for more-capable and cost-effective platforms, including submarines, RPAs, and UUVs deployed on smaller, less vulnerable, and less costly surface ships and/or submarines. Moreover, China is better able than the United States to contend in a cost-based arms race; its annual defense budget increases will continue to be greater than annual US increases.

US Strategic Partnerships in East Asia and US-China Relations

As a geographically external power, the United States must determine with which East Asian countries it must develop strategic partnerships to enable it to deploy and operate forward-based forces and maintain the regional balance of power. This determination must reflect the geopolitical significance of the regional real estate rather than historical relationships or ideological affinity. It will thus necessarily reflect the unique geopolitical characteristics of East Asia.

Large insular countries encircle mainland East Asia from the northeast to the western reaches of the South China Sea. Together Japan, the Philippines, Indonesia, Singapore, and Malaysia possess considerable assets, including energy resources, well-situated and modern port facilities, large land masses to enable critical deployments, and sophisticated infrastructures that can support maritime operations. Further offshore from the mainland, Australia and New Zealand offer substantial and secure rear-basing facilities. This geopolitical environment enables the United States to maintain a large and defensible regional presence that can dominate maritime East Asia and thus contend with a mainland great power.

The geopolitical contrast between Europe and East Asia is instructive.[31] Following World War II, the United States determined that a significant military presence in Europe was necessary to balance the power of the Soviet Union. Great Britain did not offer sufficient land mass or the geopolitical location necessary to maintain adequate forward-deployed maritime presence to control Europe's western coastal waters should a continental hegemon emerge. On the other hand, in early 1950—as the Truman administration returned US forces to the European mainland and funded the economic recovery of Western Europe to maintain a divided continent—after the Chinese Communist Party defeated Chiang Kai-shek's Republic of China government, Secretary of State Dean Acheson declared that the United States did not have a significant national security interest in a strategic presence on mainland East Asia. His definition of the US Pacific "defense perimeter" excluded the Korean Peninsula, Taiwan, and mainland Southeast Asia, including Indochina, Burma, and Thailand. According to Acheson, the US defense perimeter only encompassed the region's insular countries, particularly Japan and the Philippines, and by extension, the South China Sea countries.[32] US military leaders concurred with Acheson's assessment, and between late 1949 and early 1950 they argued that US national security did not require a strategic presence on the Korean Peninsula or on Taiwan.[33]

Eventually the United States developed strategic alliances with South Korea, Taiwan, South Vietnam, and Thailand, but these alliances did not reflect the intrinsic importance of their geopolitical location to US security interests in a divided region. Rather, the United States intervened in Korea to establish its determination to contain Soviet-led communist military expansionism, wherever and whenever it occurred. It fought the Korean War to defend US credibility, not to defend strategic territory critical to its security.[34] Once North Korean communist forces invaded South Korea and the United States perceived China as a hostile and expansionist country, previously secondary interests assumed greater military importance. In the aftermath of the Korean War, the United States signed alliances with South Korea, Taiwan, and Thailand and extended an alliance commitment to South Vietnam. These developments tied the US reputation for resolve to defend its offshore allies, including Japan, to the defense of its mainland allies and thus drew it into wars and multiple crises, despite the secondary importance of these countries to US interest in a divided East Asia.[35]

The US post–Vietnam War retrenchment from the East Asian mainland underscores its secondary importance to US security. The greatest "tragedy" of the US involvement in Vietnam is that after 10 years of war and significant losses of American blood, treasure, and honor, the withdrawal from Indochina and the loss of military bases in Thailand had an imperceptible impact on US security. The defense relationship with Taiwan has been equally peripheral to US security. A military presence on Taiwan in the 1960s supported US operations in Vietnam. Thus, in early 1972, President Richard Nixon could easily concede to Beijing that once the Vietnam War was over, the United States would withdraw all of its military forces from Taiwan.[36] In the twenty-first century, the United States has not resisted Taiwan's political accommodation to the PRC's growing coercive capabilities and its economic absorption into the PRC economy. On the contrary, the George W. Bush administration supported Taiwan's effort to expand economic and political cooperation with the PRC.[37] The Obama administration has continued this policy. Because the PRC has relied on its growing economic and military capabilities to compel peaceful accommodation with Taiwan, it has not challenged US credibility or the US defense commitment to its maritime security partners. This has allowed the United States to disengage from the mainland China–Taiwan conflict without any measurable effect on US security.

Also during the Bush administration, the United States began to disengage from the Korean Peninsula. By 2008, as South Korea expanded political and economic cooperation with China and increasingly relied on it to manage the North Korean threat, the United States reduced its forces in South Korea by 40 percent, ended its military deployments between Seoul and the demilitarized zone, committed to relinquishing operational control (OPCON) over the South Korean military by 2012, and significantly reduced the size and frequency of US–South Korean joint exercises. As with its disengagement from the Taiwan issue, the United States could acquiesce to peaceful South Korean accommodation of the rise of China without any evident concern for its credibility to defend its alliance commitments or for the effect on US security.

The Obama Administration and US Strategy for East Asia

The Obama administration's pivot toward East Asia reflects a significant departure from prior US efforts to balance the rise of China. Whereas prior administrations focused on strengthening security cooperation with the region's offshore states, this administration has expanded relations with mainland states on the Chinese periphery—in Indochina and on the Korean peninsula. Not only are these initiatives unnecessary to sustain the traditional US effort to maintain a divided East Asia, but they also impose potentially costly relationships on the United States that ultimately cannot contribute to balancing the rise of China.

After the US withdrawal from Indochina in 1975, successive administrations avoided security cooperation with Vietnam, despite Hanoi's apparent interest in developing relations since 1991, and US administrations all but ignored Cambodia. This changed in 2010, when, for the first time since the end of the Vietnam War, the United States pursued a strategic presence in Indochina. That year, Secretary of Defense Robert Gates visited Hanoi, and Secretary of State Hillary Clinton visited the city twice. She expressed US interest in developing a "strategic partnership" with Vietnam.[38] Additionally, the United States carried out joint naval exercises with Vietnam in 2010, 2011, and 2012. In June 2012, Secretary of Defense Leon Panetta visited Cam Ranh Bay, where the US Navy was based during the Vietnam War, and announced that "access for United States naval ships into this facility is a key component of this relationship [with Vietnam] and we see a tremendous potential here for the future." During the visit a senior defense department official observed that "we are making significant progress in our military relationship with

Vietnam." The United States and Vietnam have also signed a memorandum of understanding regarding civil nuclear cooperation.[39]

The United States has also strengthened security cooperation with Cambodia. Visiting Phnom Penh in 2010, Secretary Clinton encouraged Cambodian leaders to exercise greater independence from Chinese political influence. Cambodia then joined for the first time the annual US-led Cooperation Afloat Readiness and Training (CARAT) regional naval exercises, and US Marines based in Okinawa conducted interoperability exercises and maritime exercises with the Cambodian military.[40]

The Obama administration has also reversed Bush administration policy toward South Korea. Following the 2010 North Korean sinking of the South Korean naval ship *Choenan*, the administration reasserted US strategic presence on the Korean Peninsula. It deferred relinquishing wartime OPCON of South Korean forces from 2012 to 2015 despite South Korea's significant conventional military superiority vis-à-vis North Korea and its increasing ability to contend with North Korean forces unassisted. Since the summer of 2010, the scale and number of US–South Korean joint military exercises has significantly expanded, with their largest ever that year, and the United States has increased its troop presence in South Korea. The two nations have reached four new defense agreements: the South Korea–US Integrated Defense Dialogue, the first joint South Korea–US Counter-Provocation Plan, the Extended Deterrence Policy Committee, and an agreement on military space cooperation.[41] In 2012, the Pentagon developed plans to upgrade its capabilities in South Korea, and the US Navy led the first US–Japanese–South Korean joint naval exercise, which took place in the Yellow Sea and included a US aircraft carrier. It was the largest one-day, live-fire military exercise since the Korean War.[42]

These initiatives in Indochina and South Korea cannot enhance US security. Because both regions are on China's immediate periphery, US naval power cannot effectively challenge Chinese coercive power. The coercive capability of China's contiguous ground force capability (with support from its economic power) cannot be adequately mitigated by US offshore presence. Even as a primitive fighting force in 1950, the PLA held the US military to a draw in Korea. During the Cold War, the PLA contributed to the defeat of France, the United States, and the Soviet Union in Indochina. Today, PLA ground forces are far more capable than its neighbors along the entire Chinese periphery and the US military.[43]

From 2008 to 2012, South Korea's conservative leadership eagerly sought improved defense cooperation with the United States. But during the 2012 South Korean presidential campaign, both candidates promised to improve relations with North Korea and to restore greater balance in relations between China and the United States. In January 2013, President Park Geun-hye sent her first presidential envoy to Beijing. Chinese capabilities are far greater in Indochina today than in 1979, when the PLA suffered massive losses in its border war with Vietnam. In the twenty-first century, Chinese leverage vis-à-vis Vietnam will undermine US efforts to expand US-Vietnam defense cooperation. Unless South Korea and the Indochina countries are willing to once again host significant US ground-force deployments and extensive basing facilities—therefore once again incurring Chinese hostility—they will ultimately succumb to the rise of China by distancing themselves from the United States, thus accommodating China's national security interest in border regions secure from US strategic presence. Moreover, because China possesses superior leverage on its periphery vis-à-vis the United States, US challenges to Chinese security along its borders cannot induce cooperation with US interests.

Not only are recent US initiatives on mainland East Asia neither necessary nor effective, but they will ultimately be costly to US interests because they will destabilize US-China cooperation. Chinese leaders view US policy toward Indochina and South Korea as an effort to reestablish a strategic presence on China's periphery.[44] They view this as a challenge to Chinese national security.

Since 2010, China has significantly strengthened economic and political relations with the North Korean leadership, undermining US sanctions. It continues to provide North Korea with significant oil shipments and free food aid, which increased substantially in 2011. Chinese investment in North Korean mining, infrastructure, and manufacturing and its import of North Korean mineral resources have also significantly increased since 2009. It has also expressed little interest in cooperating with the United States in pressuring North Korea to participate in the Six-Party Talks.[45] That structure is now irrelevant to Northeast Asian security, and the United States has had to negotiate bilaterally with Pyongyang. Washington negotiated the short-lived 29 February 2012 agreement with North Korea outside of the Six-Party Talks venue. Since then, it has continued to negotiate bilaterally with North Korea. Meanwhile, North Korea continues to expand its nuclear weapons capability.

China has used coercive diplomacy to pressure local powers to rethink their cooperation with US strategic advancement on its periphery, contributing to instability in the South China Sea. Sino-Vietnamese tension over disputed waters escalated in spring 2010, with many Chinese advocating use of force against the Vietnamese navy.[46] China's prolonged maritime confrontation with the Philippines in 2012 over fishing near Scarborough Shoal, which included the presence of combat-ready Chinese naval patrols in disputed waters, similarly reflects Beijing's eroding tolerance for small-power cooperation with the United States. Before 2011, China had not detained any Philippine ships operating in disputed waters nor sent government ships within disputed waters surrounding the Spratly Islands, but since 2012, PRC ships have been operating within 12 miles of Philippine-claimed islands. While Chinese oil companies had not previously operated in disputed areas of the South China Sea, in 2012 Beijing announced that its companies would commence oil exploration there.[47] Since US intervention in the territorial dispute, there has also been greater tension within the Association of Southeast Asian Nations (ASEAN). Whereas the Obama administration has tried to promote ASEAN unity on the South China Sea territorial conflicts and had hoped to work with the ASEAN to promote US presence in Southeast Asia, China has relied on its partners within the ASEAN to resist US policy. The ASEAN is more divided today than at any time since its formation.

There is also reduced Chinese cooperation with the United States on global issues. In the 1990s, Beijing cooperated with the United States on humanitarian intervention, Indonesia, and, as recently as 2011, in Libya. It also cooperated with both US military operations against Iraq, but more recently, it has resisted cooperation over the violence in Syria. It has blocked US initiatives in the United Nations, merely informed the United States of its initiatives toward the Syrian government, and contributed to Russia's efforts to support the Syrian leadership. Regarding proliferation of nuclear weapons, China now undermines US efforts to curtail Iran's nuclear program. Whereas from 2006 to 2010 China voted for five UN Security Council resolutions imposing sanctions on Iran, in 2012 it opposed US efforts to tighten those sanctions, compelling the

United States to impose sanctions outside the UN framework. Following agreements by the United States, European countries, and Japan to sanction Iranian oil exports, China reached agreement with Tehran to purchase Iranian oil.[48] In South Asia, China has not assisted US efforts to enhance Pakistan's cooperation with the war in Afghanistan, and it has not restrained Pakistan's nuclear and missile programs.

Ongoing US strategic cooperation with the mainland states on China's periphery will not contribute to US security, but it will elicit increased Chinese suspicion of US intentions and greater Chinese resistance to US interests in East Asia and elsewhere. It will also lead to a deterioration of US-China relations, contributing to more destabilizing Chinese behavior in the South China Sea, higher Chinese defense spending, and diminished PRC cooperation on bilateral issues, including economic conflicts and military-to-military cooperation. And it will contribute to greater regional tensions and a greater likelihood of US-China conflict over insignificant maritime territorial disputes.

Conclusion

Since 1776, US grand strategy has sought a balance of power in its transoceanic flanking regions. When multiple great powers contended in Europe and East Asia, the Western Hemisphere was secure from the presence of extraregional powers, and the United States was secure from challenges from rival great powers that might threaten its survival. Only when a great power threatened to achieve hegemony in Europe and/or East Asia was the United States gravely threatened, as from Japan and Germany during World War II. Since World War II, the United States has assumed the responsibility from the regional great powers for the balance of power in the transoceanic regions, thus preventing flanking powers from threatening its homeland. During the Cold War, it kept Europe and East Asia divided, and in the twenty-first century it maintains the balance of power in East Asia.

In 1943, Walter Lippmann wrote that "foreign policy consists in bringing into balance, with a comfortable surplus of power in reserve, the nation's commitments and the nation's power."[49] An effective great-power national security strategy requires awareness of the "Lippmann gap," and failure to maintain such a balance results in a costly squandering of resources. At times the United States has fallen victim to the Lippmann gap, such as when it waged a costly and protracted war in

Indochina while simultaneously contending with Chinese power in East Asia and Soviet power in Europe. US leaders erroneously believed that the United States possessed important security interests in Indochina.

In the twenty-first century, the United States has responsibility for maintaining the balance of power in East Asia. The cost of contemporary US policy in East Asia does not remotely approach the cost of the Lippmann gap during the Vietnam War era. Nonetheless, the US defense budget will face increasing difficulties contending with China's rise should it continue to fund twentieth-century capabilities, including aircraft carriers, even as it transitions to ISR-based twenty-first-century platforms.

Whereas post–Cold War US administrations refrained from asserting US power on mainland East Asia, the Obama administration has reversed course and is expanding US strategic presence on China's mainland periphery. The United States lacks the capabilities to sustain this effort. China's strategic advantage on mainland East Asia is greater today than at any time since 1949. It now possesses the capability to coerce its neighbors to accommodate its security. China's economic resources are also greater than ever and are increasing. On the other hand, the United States is developing an expanded presence on mainland East Asia just as constrained financial resources challenge the US military's ability to sustain its current level of spending. Moreover, the cost of US policy on mainland East Asia will grow as its challenge to Chinese national security will elicit ever greater Chinese challenges and contribute to heightened and costly tension in US-China relations.

Since the end of the Cold War, US national security policy has enabled the United States both to contend with the rise of China to sustain a divided East Asia and to manage US-China relations to contain the cost of US policy. The United States consolidated its strategic relationships with its maritime security partners and benefitted from regional stability and US-China cooperation on a wide range of regional and global issues. Moreover, this policy elicited at most minimal controversy in the United States. There were few voices calling for a more proactive US policy toward mainland East Asia. The challenge for the United States is to recognize the essential requirements for a national security strategy that secures US interests in a divided region and to avoid the temptation to adopt policies that unnecessarily raise the cost of US national security. SSQ

Notes

[1] "Transcript of President George Washington's Farewell Address," 19 September 1796, http://www.ourdocuments.gov/doc.php?doc=15&page=transcript.

[2] Samuel Flagg Bemis, *A Diplomatic History of the United States* (New York: Henry Holt, 1936), 31, 50.

[3] Samuel Flagg Bemis, *Jay's Treaty: A Study in Commerce and Diplomacy*, rev. ed. (New Haven, CT: Yale University Press, 1962), 311–15.

[4] Samuel Flagg Bemis, *Pinckney's Treaty: America's Advantage from Europe's Distress, 1783–1800* (New Haven: Yale University Press, 1926).

[5] Bemis, *Diplomatic History of the United States*, chap. 8.

[6] Ibid., chap. 10.

[7] Frank Lawrence Owsley Sr., rev. by Harriet Chappell Owsley, *King Cotton Diplomacy: Foreign Relations of the Confederate States of America* (Tuscaloosa: University of Alabama Press, 1959), 333–34.

[8] Ibid., 397–99.

[9] Ernest R. May, *Imperial Democracy: The Emergence of America as a Great Power* (New York: Harper, 1961), chap. 15; Howard K. Beale, *Theodore Roosevelt and the Rise of America to World Power* (New York: Collier, 1956), 93–96; John A. A. Grenville and George Berkely Young, *Politics, Strategy and American Diplomacy: Studies in Foreign Policy, 1873–1917* (New Haven: Yale University Press, 1966), 249–50, 260–61; Samuel Flagg Bemis, *The Latin American Policy of the United States* (New York: Harcourt Brace, 1943), 135–37.

[10] Richard W. Leopold, *The Growth of American Foreign Policy: A History* (New York: Alfred A. Knopf, 1962), chap. 17.

[11] Boris Savinsky, trans. Geoffrey Jukes, *The Japanese-Soviet Neutrality Pact: A Diplomatic History, 1941–1945* (New York: RoutledgeCurzon, 2004), 57–59; Waldo Heinrichs, *Threshold of War: Franklin D. Roosevelt and American Entry into World War II* (New York: Oxford University Press, 1988), 51–52; and James W. Morley, ed., *The Fateful Choice: Japan's Advance into Southeast Asia 1939–1941* (New York: Columbia University Press, 1980).

[12] See Nicholas Spykman, *America's Strategy in World Politics: The United States and the Balance of Power* (New York: Harcourt Brace, 1942), 367–72, chaps. 14–15; and Spykman, *The Geography of the Peace* (New Haven: Yale University Press, 1944), chap. 5.

[13] A. Whitney Griswold, *The Far Eastern Policy of the United States* (New Haven: Yale University Press, 1938); Dorothy Borg, *The United States and the Far Eastern Crisis of 1933–1938* (Cambridge, MA: Harvard University Press, 1964); Christopher Thorne, *The Limits of Foreign Policy: The West, The League of Nations and the Far Eastern Crisis of 1931–1933* (New York: G. Putnam, 1973); Akira Iriye, *Across the Pacific: An Inner History of American-East Asian Relations* (New York: Harcourt, Brace & World, 1967), 201–4, 216–20; and Michael A. Barnhart, *Japan Prepares for Total War: The Search for Economic Security, 1919–1941* (Ithaca, NY: Cornell University Press, 1987), chap. 12.

[14] See Frederic S. Dunn et al., "A Security Policy for the United States," 8 March 1945, classified as a confidential document of the Joint Chiefs of Staff, cited in Melvyn Leffler, *A Preponderance of Power: National Security, the Truman Administration, and the Cold War* (Palo Alto, CA: Stanford University Press, 1992), 10–14. On the European balance, see ibid.; and John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy during the Cold War* (New York: Oxford University Press, 1982), 25–31.

[15] For a comprehensive discussion of US interests in Asia, see Robert J. Art, "The United States and the Rise of China: Implications for the Long Haul," *Political Science Quarterly* 125, no. 3 (Fall 2010).

[16] On China's submarine force, see Lyle Goldstein and William Murray, "Undersea Dragons: China's Maturing Submarine Force," *International Security* 28, no. 4 (Spring 2004); and William S. Murray, "An Overview of the PLAN Submarine Force," in *China's Future Nuclear Submarine Force*, ed. Andrew S. Erickson, Lyle Goldstein, and William Murray (Annapolis: Naval institute Press, 2007).

[17] Eric Hagt and Matthew Durnin, "China's Antiship Ballistic Missile: Developments and Missing Links," *Naval War College Review* 62, no. 4 (Autumn 2009); and Andrew S. Erickson and David D. Yang, "Using the Land to Control the Sea?: Chinese Analysts Consider the Antiship Ballistic Missile," ibid. On the development of the antiship cruise missile, see William S. Murray, "Underwater TELS: PLAN Submarine Transformation," in *China's Strategy for the Near Seas*, ed. Andrew S. Erickson (Annapolis: Naval Institute Press, 2012).

[18] On the targeting issues for the ASBM, see Owen R. Cote Jr., "Assessing the Undersea Balance," SSP working paper WP11-1, Massachusetts Institute of Technology, 12–14, http://web.mit.edu/ssp/publications/working_papers/Undersea%20Balance%20WP11-1.pdf.

[19] *Quadrennial Defense Review Report* (Washington: DoD, 2006).

[20] For a discussion of US deployments on Guam, see Shirley A. Kan, *Guam: U.S. Defense Deployments*, Congressional Research Service (CRS) report RS22570 (Washington: CRS, October 2012), http://www.fas.org/sgp/crs/row/RS22570.pdf.

[21] Anthony L. Smith, *Singapore and the United States 2004–2005: Steadfast Friends* (Honolulu: Asia-Pacific Center for Security Studies, 2005), 4–5; and Jim Garamone, "Singapore, U.S. Reaffirm, Strengthen Relationship," *American Forces Press Service*, 12 July 2005, http://www.defenselink.mil/news/Jul2005/20050712_2040.html.

[22] "RP Now Biggest Recipient of US Military Aid in East Asia," *Manila Standard*, 6 March 2004.

[23] Ian Storey, *Malaysia and the United States 2004–2005: The Best of Times?* (Honolulu: Asia-Pacific Center for Security Studies, 2005), 5; and *Malaysiakini*, 5 June 2006, FBIS document no. 200606051477.1_c1bf005f528d30b4.

[24] On the Navy's access to Subic Bay, see *Manila Standard*, 7 June 2012, 1, 2, http://www.scribd.com/doc/96160598/Manila-Standard-Today-June-7-2012-Issue. On US arms sales to the Philippines, see "U.S. Triples Military Aid to Philippines in 2012," *Reuters*, 3 May 2012, http://www.reuters.com/article/2012/05/03/us-philippines-usa-idUSBRE8420IU20120503.

[25] On US development of UUVs, see Department of the Navy, *The Navy Unmanned Undersea Vehicle (UUV) Master Plan* (Washington: DoD, 2004), http://www.navy.mil/navydata/technology/uuvmp.pdf.

[26] On China's maritime power projection capability, see Mark Cozad, "China's Regional Power Projection: Prospects for Future Missions in the South and East China Seas," in *Beyond the Strait: PLA Missions Other Than Taiwan*, ed. Roy D. Kamphausen, David Lai, and Andrew Scobell (Carlisle, PA: Strategic Studies Institute, US Army War College 2009).

[27] On China's aircraft carrier program, see Robert S. Ross, "China's Naval Nationalism: Sources, Prospects, and the U.S. Response," *International Security* 34, no. 2 (Fall 2009).

[28] *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2011* (Washington: DoD, 2011), 43.

[29] See Robert C. Rubel, "The Future of Aircraft Carriers," *Naval War College Review* 64, no. 4 (Autumn 2011).

30. Ronald O'Rourke, *Navy Ford (CVN-78) Class Aircraft Carrier Program: Background and Issues for Congress*, CRS report no. RS20643 (Washington: CRS, 29 June 2012).

31. For an extended discussion of this issue, see Robert S. Ross, "The Geography of the Peace: Great Power Stability in Twenty-First Century East Asia," *International Security* 23, no. 4 (Spring 1999).

32. See Dean Acheson, *Crisis in Asia: An Examination of U.S. Policy* (Washington: Department of State, 23 January 1950), 111–18.

33. "Memorandum of Conversation, by the Secretary of State," 5 January 1950, US Department of State, *Foreign Relations of the United States (FRUS), 1950*, vol. 6 (Washington: Government Printing Office [GPO], 1976), 260–61; and "Memorandum of Conversation, by the Secretary of State," 29 December 1949, *FRUS, 1949*, vol. 9 (Washington: GPO, 1974), 467.

34. On the US decision to enter the Korean War, see William Whitney Stueck Jr., *The Road to Confrontation: American Policy toward China and Korea, 1947–1950* (Chapel Hill: University of North Carolina Press, 1981); and Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton, NJ: Princeton University Press, 1992).

35. On the importance of a reputation for resolve and credibility to US involvement in the Vietnam War and in the multiple Taiwan Strait crises, see Robert D. Schulzinger, *A Time for War: The United States and Vietnam, 1941–1975* (New York: Oxford University Press, 1997), 110–11, 133, 166; and Leslie H. Gelb and Richard K. Betts, *The Irony of Vietnam: The System Worked* (Washington: Brookings Institution, 1979), 184–87, 197–200. On the policy shift toward Taiwan following the onset of the Korean War and the ensuing development of a commitment, see Robert Accinelli, *Crisis and Commitment: United States Policy toward Taiwan, 1950–1955* (Chapel Hill: University of North Carolina Press, 1996), 7–17, 24–27, 158–62; and Nancy Tucker, *Taiwan, Hong Kong, and the United States, 1945–1992* (New York: Twaynes, 1994), 40–43, 50–51.

36. See the text of the February 1972 US-China Shanghai Communiqué at *FRUS, 1969–1976*, vol. 17, China, 1969–1972, Document 203, http://history.state.gov/historicaldocuments/frus1969-76v17/d203.

37. Robert S. Ross, "Taiwan's Fading Independence Movement," *Foreign Affairs* 85, no. 1 (March/April 2006).

38. See Secretary of State Clinton's 30 October 2010 remarks in Hanoi at http://www.state.gov/secretary/rm/2010/10/150189.htm.

39. See Secretary Panetta's 3 June 2012 media availability in Hanoi at http://www.defense.gov/transcripts/transcript.aspx?transcriptid=505; and Jim Garamone, "Panetta to Visit American Ship in Vietnam's Cam Ranh Bay," *American Forces Press Service*, http://www.defense.gov/news/newsarticle.aspx?id=116596. On civil nuclear cooperation, see the Department of State announcement at http://www.state.gov/r/pa/prs/ps/2010/03/139255.htm.

40. John Pomfret, "Clinton Urges Cambodia to Strike a Balance with China," *Washington Post*, 1 November 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/11/01/AR2010110101460.html; and Mike Morley, "U.S., Cambodian Navies Participate in Final CARAT 2010 Exercise," *America's Navy*, http://www.navy.mil/submit/display.asp?story_id=56819.

41. On the OPCON transfer, see Kim Deok-hyun, "Delay of Wartime Command Transfer to Bolster Security on Korean Peninsula, *Yonhap*, 26 June 2010, in OSC doc. no. KPP20100626971072. On the military agreements, see the text of the Joint Communiqué of the 42nd ROK-US Security Consultative Meeting, 28 October 2010, http://www.defense.gov/news/d20101008usrok.pdf; and "S. Korea, U.S. Pact To Boost Joint Space Cooperation," *Defense News*, 24 October 2012, http://www.defensenews.com/article/20121024/DEFREG02/310240012

/S-Korea-U-S-Pact-Boost-Joint-Space-Cooperation. For a record of US–South Korean exercises in 2010, see *Xinhua*, 23 December 2010, in OSC doc. no. CPP20101223968128.

42. Choi He-suk, "U.S. Forces Korea Bolsters Ground Units Ahead of Wartime Control Transfer," *Korea Herald*, 19 June 2012; "United States, Republic of Korea and Japanese Naval Exercises Announced," DoD news release no. 490-12, 13 June 2012, http://www.defense.gov/releases/release.aspx?releaseid=15367; Mure Dickie, Song Jung-a, and Kathrin Hille, "US, Japan Begin Naval Drills Near China," *Financial Times*, 21 June 2012, http://www.ft.com/intl/cms/s/0/64acf730-bb9b-11e1-90e4-00144feabdc0.html#axzz22mDcpERo; and Jon Rabiroff, "Allies Wage Largest Live-Fire Drill Since Korean War," *Stars and Stripes*, 22 June 2012, http://www.stripes.com/news/allies-wage-largest-live-fire-drill-since-korean-war-1.181046.

43. On the improvement in China's ground force capabilities, see Susan M. Puska, "Rough but Ready Force Projection: An Assessment of Recent PLA Training," in *China's Growing Military Power: Perspectives on Security, Ballistic Missiles, and Conventional Capabilities*, ed. Andrew J. Scobel and Larry M. Wortzel (Carlisle, PA: Strategic Studies Institute, Army War College, 2002), 223, 244–45.

44. See, for example, Wang Jisi, "Zhong Mei Zhongda Zhanlue Jiaoliang yi Bimian" (It will be difficult to avoid a major strategic test of strength in US-China relations), *Guoji Xianqu Daobao*, 9 August 2010, http://news.xinhuanet.com/herald/2010-08/09/content_13988055.htm; Wang, "Zhong Mei Guanxi Xin Qushi ji qi dui Dongbei Ya Anquan de Yingxiang" (The recent trend in China-US relations and its implications for Northeast Asian security)," *Guoji Zhengzhi Yanjiu* (*International Politics Quarterly*) no. 1, 2011; and Zhu Feng, "Zhong Mei Hui Jinru Diyuan Zhengzhi Duikang Ma (Will China and the United States face geopolitical confrontation?), *Huanqiu Shibao*, 14 January 2012, http://opinion.huanqiu.com/roll/2012-01/2352598.html.

45. On China's Recent North Korea Policy, see Peter M. Beck, "North Korea in 2011: The Next Kim Takes the Helm," *Asian Survey* 52, no. 1 (January 2012). On economic relations, see "Scale of Yearly Chinese Unconditional Aid to N. Korea Unveiled, *Dong-a Ilbo*, 25 June 2012, http://english.donga.com/srv/service.php3?biid=2012062508548; "N. Korea, China Agree to Jointly Develop Three Mines in North, *Yonhap*, 9 August 2012, http://english.yonhapnews.co.kr/northkorea/2012/08/09/98/0401000000AEN20120809004600315F.HTML; and Xiaoyi Shao and Nick Edwards, "China Signals Strong Support for Decaying North Korea Economy," *Chicago Tribune*, 14 August 2012, http://www.chicagotribune.com/news/sns-rt-us-korea-north-chinabre87c0yg-20120813,0,3130799.story.

46. Chinese military officers and civilian foreign policy analysts, interviews by author, June 2010 within China.

47. "SE Asia Meeting in Disarray over Dispute with China," *Reuters*, 13 July 2012, http://www.reuters.com/article/2012/07/13/us-asean-summit-idUSBRE86C0BD20120713; and "CNOOC says S. China Sea Blocks Tender Well," *Reuters*, 17 July 2012, http://in.reuters.com/article/2012/07/17/china-cnooc-scs-idINL4E8IH1RD20120717.

48. Mark Landler, "China Is Excluded from Waivers for Oil Trade with Iran," *New York Times*, 11 June 2012; and Judy Hua and Fayen Wong, "China Iran Oil Imports Recover, Recoup Earlier Fall," *Reuters*, 21 June 2012, http://www.reuters.com/article/2012/06/21/us-china-oil-iran-idUSBRE85K0L020120621.

49. Walter Lippmann, *U.S. Foreign Policy: Shield of the Republic* (Boston: Little, Brown, 1943), 34–36. For a discussion of the "Lippmann gap" and its relevance to US foreign policy in the 1960s and 1970s, see Samuel Huntington, "Coping with the Lippmann Gap," *Foreign Affairs* 66, no. 3, (Winter 1987/1988).

Spring 2014

War on Our Doorstep

Not a Mere Crime Problem

James P. Farwell
Darby Arakelian

The television show *Miami Vice* regaled viewers with stories of undercover agents as they battled to keep Colombians and their Miami cohorts from smuggling cocaine and other illegal drugs into this country. In real life, US authorities did even better. They proved so effective that the Colombia cartels decided to shift operations west and outsourced drug trafficking to Mexican gangs. Instead of cash, they paid the traffickers in-kind, offering 30–50 percent of the drugs to sell on their own, and the gangs graduated from transport to distribution. Drug trafficking through Mexico had long been a problem, but this change triggered a great rise.[1]

While Western media focus heavily on the civilian deaths in Syria, they often overlook our own backyard, where Mexican drug violence has claimed 110,000 lives.[2] Former president Felipe Calderon pronounced that "the most lethal war is the one being fought by criminal gangs among themselves."[3] That statement reflects only one element in the story, because cartel violence greatly affects the United States.[4] As cartels battle for turf among one another, the threat transcends borders and raises *hemispheric security* issues that embrace the United States, Canada, Mexico, and their neighbors in Central and South America. Mexican security forces have made cross-border incursions into this country, hundreds of US Customers and Border Patrol (CBP) agents have been

Dr. James P. Farwell is a national security expert who has advised the US Special Operations Command. He holds a JD in law from Tulane University and a DCLS in comparative law from the University of Cambridge. He is the author of *Persuasion and Power: The Art of Strategic Communication* (Georgetown University Press, 2012).

Darby Arakelian is a national security expert and former CIA officer. She holds a BA in political science, Russian, and economics from the University of Denver and an MA is in security policy studies from the George Washington University. Ms. Arakelian specializes in terrorism and counterterrorism communications strategy and analysis, cyber warfare, and automated media monitoring and analysis.

attacked,[5] and even US Soldiers have been suborned into acting as hitmen south of the border.[6] The cartels are also increasingly active in US cities.

Although Calderon's team boasts that it captured 25 of its 37 most wanted criminals,[7] no one suggests the flow of drugs has been stopped. In this high-stakes struggle, while Mexico may not be a failed state, the war is eroding its credibility and ability to govern. It is also affecting security in the region. In Guatemala, cartels reportedly control 40–60 percent of the entire country.[8] The Mexican Sinoloa cartel has formed links with Mara Salvatrucha (MS-13), a gang started in Los Angeles by Salvadoran immigrants.[9] Mexican cartels are also linked to murders in Argentina and Peru.[10]

While the United States wants to stop trafficking and eliminate kingpins, Mexicans want to stop kidnapping and violence. This has left both Mexico and the United States without a cohesive strategy for combating the cartels—a totally unacceptable situation. Most observers, including the Mexican government, believe this to be a law enforcement problem. We challenge whether that approach is most effective and argue that conventional definitions for characterizing this struggle do not apply to this emerging, unprecedented conflict. The required debate over how to protect vital US security interests has barely commenced. What legal authorities govern US action? What roles should our military or law enforcement play? Do we rely upon conventional definitions of high-intensity crime, terrorism, or insurgency to dictate solutions? What are the tradeoffs for using the military or law enforcement to battle the cartels? The threat to US national security interests calls for a different approach. A combination of law enforcement, social reform, covert intelligence, military special operations, and, as appropriate, selective military action by Mexico with indirect mission assistance from the US military offers a plausible path to success.

Characterizing the Conflict to Determine Strategy

How the war is characterized matters as to what body of law governs it—the law regulating law enforcement or the law of armed conflict?[11] The answer affects tactics and the nature of forces employed. For example, while police can use deadly force against suspects who pose a threat of serious physical harm, the principle of military necessity authorizes a military to take all necessary measures not prohibited by international law to defeat an enemy.[12] The US and Mexican militaries have a role in low-intensity conflict, fighting an insurgency, or combating terrorism, especially if those terrorist groups support al-Qaeda.[13] Scholars like Paul Rexton Kan argue that while drug cartels share certain organizational and operational characteristics of terrorist organizations,[14] the Mexican drug war is not an insurgency because cartels lack a political agenda. Kan's key argument rests upon the widely—and mistakenly—held view that terrorists seek political goals while criminals are motivated by greed.[15] Writing in *Small Wars Journal*, Brad Freden acknowledges that elements of counterinsurgency (COIN) operations are useful in fighting the cartels but argues that "the violence, drug trafficking, and lawlessness that we see in northern Mexico does *not* constitute an insurgency. Drug cartels have no ideology beyond profit, no aspirations other than to be left alone, and no popular support beyond that which can be purchased with money or intimidation" (emphasis in original).[16] University of Maryland scholar Shibley Telhami also views terrorists as linked to political goals and defines them as those who deliberately target civilians for such ends.[17]

Those who oppose characterizing the Mexican drug wars as an insurgency argue that cartels have not "captured" the state to implement a social or political agenda and are not seeking to overthrow the government and replace it with their own, but focus on shoving the state aside in their pursuit of profits. This thinking, ably argued by Kan, is that "no insurgent or terrorist group . . . has been dismantled by rolling up its financial networks," a statement that would come as news to the US Treasury and other agencies engaged in counterterrorism financing.[18] The pivot of the argument is that cartels do not seek to "substitute their ideology for the existing one or to achieve any other political goal that is routinely associated with armed groups who instigate social upheaval."[19]

So, should fighting the drug cartels be limited to law enforcement and political measures that effect a social reform agenda or is this a form of counterinsurgency for which properly trained military geared to special missions should play a key role? Most voices strongly oppose using the military to combat drug trafficking. At its core, their argument rests most importantly on three confluent propositions.

- The Mexican drug war is not an insurgency, terrorism, or low-intensity conflict (LIC), but at most, a "mosaic cartel war" that requires social reform and law enforcement.[20]

- The military is not well suited for waging this war. Rice University scholar Tony Payan asserts that Mexico's military strategy has produced as many as 100,000 deaths and "let loose on the civilian population the military and, increasingly, a militarized federal police."[21]
- Institutional reforms to clean up Mexico's criminal justice system could provide meaningful social reform plus a better, cohesive collaboration with the United States.

Mexico's drug war presents a different kind of warfare, with different players and political dynamics, for which success requires achieving parallel political and security goals. Characterizing the war turns on whether the drug cartels—sometimes called drug trafficking organizations (DTO) or transnational criminal organizations (TCO)—have a political ideology and seek political power. Both factors apply to the cartels. They espouse an ideology rooted in surprisingly specific stories, narratives, themes, and messages that go well beyond what other groups who are widely accepted as political, such as al-Qaeda, Italy's Red Brigades, Sendero Luminoso (Shining Path) in Peru, Colombia's FARC (Revolutionary Armed Forces of Colombia) and National Liberation Army (Ejército de Liberación Nacional, ELN), or Paraguay's Ejército del Pueblo Paraguayo (EPP) espouse. Those groups embrace the rhetoric of ideology but offer little content to define one. They all seek political power, either to overthrow the existing regime or, as in Mexico, to paralyze and remove the government as a threat to their operations. And they are all criminal.

Even then, the argument that the cartels do not present an insurgency because greed or profit, not a "political" agenda, motivates them is flawed. There is no accepted definition for what constitutes a political agenda. Yale political scientist Harold Lasswell probably came as close as anyone to how politicians view politics: "Politics is who gets what, when, and how."[22] Whether parties seek money legally or illegally may affect their status as criminals or law-abiding citizens, but they may easily qualify as criminals and political actors. Most politicians would scoff at the idea that parties whose agenda in the political process is to seek money are not political. Crime and politics are not mutually exclusive.

Cartel Ideology

The notion of what constitutes an ideology lends itself to different expressions. In politics, almost any approach constitutes a belief system, although not all belief systems are ideologies.[23] Broadly, ideology consists of a collection of ideas that define goals, expectations, and actions and express a cohesive basis for thought and behavior. Ideologies exert influence over the beliefs and values that people share, how they see themselves, and how they perceive the world and their place in it. Ideology guides action and influences how people relate to one another. It defines hopes, dreams, and aspirations.

A striking quality about organizations labeled "terrorist" is their substantive lack of ideology. Harvard scholar Louise Richardson has pointed out that terrorist movements do not describe meaningfully the new world they intend to create.[24] All terrorist movements, she observes, "have two kinds of goals: short-term organizational objectives and long-term political objectives requiring significant political change."[25] She points out that their political causes have been about changing the status quo, not offering an alternative vision for the future.

Colombian FARC leader Paul Reyes admitted he could not define a ruling program. Tamil Tigers leader Velupillai Prabhakran's description of the future was pabulum about a socialist state. Chechen Shamil Basayev said he stood for "power to the people," whatever that meant. Shining Path's Abimael Guzmán brushed off questions about his vision for the future, admitting that "we have not studied this question sufficiently."[26] Colombia's FARC and ELN and Peru's Shining Path all morphed into criminal entities that finance themselves from drug trafficking, but all claim to fight for a political ideology. Except for regime change, it is hard to discern much content to their views. They do not discuss the exact form of government, health care, education, jobs, or items that define what real political parties or actors offer.[27] Al-Qaeda is no different. Richardson observes that in defining his vision, Osama bin Laden was "extremely vague."[28] French scholar Olivier Roy eviscerated bin Laden for his empty rhetoric.[29]

By contrast, the Mexican drug cartels are remarkably concrete in spinning a story, narrative, theme, and message that hold particular meaning for their targeted audiences. Greed may drive cartels, but what has made them effective is their ability to recruit and mobilize younger, alienated Mexicans through messaging what the cartels offer that the state does not: social mobility, hope, opportunity, and prosperity. The Mexican drug cartels net a 6,000-percent profit from trafficker to user; counting from the purchase price paid to growers, the business yields an eye-popping 150,000-percent profit.[30] In such a lucrative market, cartels easily find a rich source of recruits among impoverished Mexicans, particularly in Juarez assembly plants established in the wake of NAFTA that pay $200–300 a month. The cartels reportedly can pay teenagers $5,000 for a single act of violence.[31]

Cartels articulate a story defining themselves as rooted in the romantic nineteenth-century image of a bandito preying upon the rich and a national history in which wealthy Mexicans and foreign investors have controlled much of the economy, leaving most Mexicans impoverished.[32] Cartel ballads and music videos stem directly from the Mexican folk tradition of romanticizing revolutionary heroes and legend, except that today's songs glorify drug lords.[33]

The songs (*narco-corridos*), videos, social media, signs, and banners (*narcomantas*) present a populist patina that celebrates the humble origins of cartel leaders and their exploits. Ricardo Ainslie points out that this strategic communication has shifted the terrain "for a political left long accustomed to an adversary defined as the nation's elites and long accustomed to viewing itself as a movement that defended the downtrodden."[34]

The narratives help define a specific culture that appeals to teenagers and younger people who the cartels vigorously recruit. It is manifest in the attire: garish cowboy hats, ostrich-skin boots, flashy sneakers, brightly colored baseball hats, tight dresses, gaudy jewelry, lavish homes, fast cars, alcohol, and a glamorous life that offers the best food, beautiful women, and action. The cartels provide a way of life that offers a macho identity and pride for which recruits have no other means of access.[35]

Writing in *Milenio*, Tijuana writer Heriberto Yépez accurately observed that the cartels have evolved from being an economy to an ideology that saturates society. The term *narco* becomes conflated in "drug trafficker" (*el narco)* and "drug life" (*lo narco)*. Yépez argues that *narco* used to be an adjective that described one aspect of Mexican culture. Now it *is* culture: "narco and culture are synonyms."[36] The cartels offer meaning and concrete opportunities that directly influence norms, values, beliefs, attitudes, opinion, and behavior.

The messaging is directed as well to the military. Los Zetas recruits by exploiting the fact that the minimum wage in Mexico is five dollars a day, unfolding banners—*narcomantas*—asking, "Why be poor? Come work for us."[37] One Zetas banner hanging over a major thoroughfare declared: "Operative Group 'the Zetas' wants you soldier or ex-soldier. We offer a good salary, food and benefits for your family. Don't suffer any more mistreatment and don't go hungry." Members of at least one cartel, La Familia Michoacana, now succeeded by the Knights Templar (Caballeros Templarios), view themselves as resistance fighters against crime. They developed expertise in soft power to gain popular credibility.[38] They espouse an odd form of Christianity and run drug rehab clinics. The cartel offers jobs and organizes popular protests against the government.[39] Of course there is a darker side. The cartels employ directed violence to secure loyalty, extract revenge, send messages, claim turf, and fill power vacuums.[40] In short, the cartels *do* espouse a political philosophy that meets the hopes and aspirations, as well as playing on the fears, of their targeted audiences.

Seizing Political Power

The cartels also aggressively seek political power. They have succeeded so well that Calderon acknowledged, "This criminal behavior [by cartels] . . . has become a challenge to the state, an attempt to replace the state."[41] They have created an atmosphere of fear and intimidation that impairs the government's ability to operate in any normal fashion in providing security or ensuring the welfare of the people. Tactics of intimidation have choked off press freedom.[42] They have "superseded or seriously weakened" the government in a growing number of Mexican states, even in places becoming a "parallel government."[43] Reportedly, the cartels spend a *billion dollars annually* to bribe police.[44] They have assassinated political candidates and high-ranking military and law enforcement officials. They engage in campaigns to subvert the Mexican government at all levels.[45] Their extortion has obstructed commerce.[46]

Los Zetas stands out for why normal law enforcement will not defeat cartels, and drawing lessons, other cartels have stepped up their own capabilities. Recruiting from Mexico's special operations forces and arming itself with AK-47s, IEDs, RPGs, and 50-caliber machine guns, Los Zetas has trained in small-squad infantry tactics, uses social media adroitly, operates with sophisticated intelligence capabilities, and could easily become an overt insurgency. It will be difficult for a regular police force to tackle this type of militia.[47] While we disagree with how Paul Kan characterizes the drug war, we agree with a lot of his ideas on how to address it. His point that any strategy must take on the Zetas first is prescient. Among all the cartels, this one offers the greatest threat of evolving overtly into an antigovernment insurgency movement.[48] But one should never underestimate the lethality of the others.

Although concerned about the effect of labeling the Mexican drug war an insurgency, Christopher Ljungquist summed up the point that the cartels are political by stating that "the Mexican state is fighting powerful and atypical insurgencies, armed with virtually unlimited access to firearms, including anti-aircraft batteries, and funded by an expert trade in illegal narcotics worth billions of dollars."[49] Former secretary of state Hillary Clinton is among those who concur that Mexico faces an insurgency, having declared that the cartels "are showing more and more indices of insurgencies."[50]

While not writing about Mexico per se, Bard O'Neil and David Kilcullen seem to agree that a confrontation qualifies as insurgency only where it is politically motivated and constitutes a political uprising.[51] The Mexican drug war meets that definition. It is a war tailored for a *new form* of counterinsurgency defined as "an armed struggle for support of the population" that requires a holistic approach and unity of effort to achieve security, drug eradication, social reform, judicial reform, crackdowns on corruption, multinational partnerships with neighbors who the drug war affects directly and indirectly, and special-mission military efforts against heavily armed and trained cartels. It is an iterative, unique approach.[52]

Not all criminal activity qualifies as insurgency.[53] But the Mexican drug war is a low-intensity conflict, and the cartels do qualify as insurgents, hostile combatants, and terrorists. The fact is the lines between crime, terrorism, and insurgency are becoming increasingly blurred. Indeed the US Drug Enforcement Administration (DEA) reports that designated foreign terrorist organizations (FTO) involved in the global drug trade have jumped from 14 groups in 2003 to 18 in 2008.[54] Therefore, it is imperative the United States, whose vital security interests are linked with Mexico as well as the rest of the hemisphere in managing and prevailing in this conflict, recognize what is happening in Mexico and deal with it realistically.

A Different Approach

We start with two realities. First, Mexico's priorities are to stop violence and kidnapping, while the United States is focused on eliminating kingpins and stopping the flow of drugs.[55] Until the early 1990s, the drug business in Mexico was relatively peaceful. US citizens suffered, but the situation worked well for Mexicans.[56] Second, neither side has a strategy for managing or prevailing in this war—a problem complicated by extreme Mexican sensitivity that the United States will intrude upon its sovereignty. Success requires resolving these challenges. While there are no quick fixes, these actions merit consideration:

- Approach the situation as a low-intensity conflict against insurgents who are both criminals and terrorists—and treat them as terrorists. Make no settlement with the cartels. They are in the business in which they want to be. The cartels are an evil, and evil cannot be defeated. It must be eradicated.

- Seize and restrict access to cartel finances. This is pivotal since their wealth gives them exceptional power that must be broken. One challenge the United States confronts is the refusal of the Treasury Department to deal with the reality of the drug war—or counterterrorism—as requiring a combination of law enforcement and special operations. The *Washington Post* reports a proposal by the White House to target cartel assets was declined by Treasury. That mistake must be rectified.[57] Mexico could deplete cartel bank accounts and seize assets. The United States could provide intelligence and technical support to help locate such assets then defer to Mexico for action. If the United States seized such assets, it should share them with Mexico as an incentive to encourage Mexican cooperation. A key element of this approach lies in disrupting the relationships cartels have with international terror networks.

- Work with the Mexican government to develop a special-mission military force that will avoid human rights violations and work well with civilian authority but that has the expertise and military capability to take on and defeat heavily armed adversaries like Los Zetas. President Nieto is backing away from his suggestion of creating a national gendarmerie. Whatever the force is called, Mexico needs an effective, well-trained special-mission force. Critics worry the cartels will try to subvert and corrupt such a force. Be assured they will make that effort. But Mexico and the United States must work cooperatively to ensure an effective force is recruited, trained, and retained. Though not an easy task, it should not deter us.

- The United States must persuade Nieto of the value of US assistance, particularly intelligence, surveillance, and reconnaissance. The *Washington Post* reported last April that former president Calderon had granted US spy planes access to Mexican airspace to gather intelligence. US drones supported CBP patrols, and cyber technology was employed to combat trafficking. The *Post* reported the United States was also helping target and vet potential intelligence assets.[58] In Iraq, Gen Stanley McChrystal forged a task force that accounted for between 11,000 and 13,000 members of al-Qaeda. Their British counterparts accounted for another 3,500.[59] That was achieved through a fusion team that identified key terrorist leaders and middle-echelon loyalists and eliminated them. US-Mexican fusion centers were established, the *Post* reported, in Mexico City and Monterrey, as well as in regional headquarters. Apparently more limited than McChrystal's task force, this was still a step in the right direction.[60] Nieto may eschew such help, but we must persuade him to reverse course and make clear that vital US interests are at stake—and we will act accordingly.

- Except for its marines, who have proven relatively effective, Mexico's military should be employed with restraint. Those who argue that most military personnel are not trained for law enforcement have a valid point. Mexico's experience in using its military has produced mixed results, while alienating many Mexicans. The US Marines should continue and step up efforts to work with Mexico's marines through indirect mission assistance in training and equipping.

- Mexican leadership must persuade its population, especially its elites (who arguably have too often helped, not fought, the cartels),[61] middle class, unions, and civil society organizations to support the fight against the cartels—stop kidnapping, extortion, robbery, human trafficking, arms smuggling, and drug trafficking. Calderon failed to lay a solid political foundation for waging the war. Success requires persuading Mexicans their own lives depend on defeating the cartels.[62] The challenge is difficult, but Nieto must avoid repeating Calderon's mistakes.

- Work with Mexico to develop a joint strategy and support it with the necessary resources. Violence does not affect the entire country. One-third of Mexican states have violence levels similar to the

United States. A strategy should focuses on the most violent areas; the capital, Mexico City, and the financial center, Monterrey; and tourist areas which contribute heavily to the nation's economy, such as Acapulco, Leon, San Miguel, Cuernavaca, Guadalajara, and Toluca.

- Revamp the Merida Initiative.[63] Too much money went to US contractors and too little to Mexicans who could make a difference. Mexico lacks the resources needed to properly implement the institutional and social reforms needed to win this war. This is a long-term challenge, but success requires achieving social justice in Mexico. We can do more to help and we must.
- Forge border management solutions with realistic division of responsibility between the United States and Mexico.
- Abrogate the Brownsville Agreement, which former attorney general Janet Reno entered into in 1998. This agreement lacked foresight in that it compelled the United States to notify the Mexican government of undercover operations in Mexico. That agreement handicapped our law enforcement agencies on any number of fronts without Mexican compromise.
- A hemispheric approach must be reviewed by looking beyond Mexico to our regional neighbors. The drug war threatens Canada as well as Central and South America. Coordinate with Canadian SOF in providing training to Central and South American militaries for counternarcotics and to the military in Guatemala, El Salvador, Honduras, and other Latin allies through SOF assistance to help them develop special-mission capabilities for defeating drug traffickers.

The United States must move beyond defeatist rhetoric suggesting the drug war can only be managed, not won. It can and must be won. But that requires viewing it realistically and taking significant action against the cartels to help Mexico gain control of the strategic situation. While general-purpose military forces are unsuited for winning this conflict, special-mission units are essential to defeat heavily armed, often well-trained cartel forces whose capabilities can overwhelm any normal law enforcement capability. Mexico lies on our doorstep, and much of what affects its vital interests is entwined with vital US interests. Recognizing that reality is the beginning, and it is time to get moving.

Notes

[1] Blog del Narco, *Dying for the Truth: Undercover inside the Mexican Drug War* (Unknown site: Blog del Narco, 2012). The blog is written anonymously by Mexican journalists who conceal their identity to protect against drug cartel violence. The book documents the violence in 2010. Nobody is certain since so few homicides are reported—just 5 percent. The rest is guesswork. During Calderon's presidency, 60,000 deaths are estimated, but another 25,000 persons went missing (not all due to crime). Clare R. Seelke and Kristin Finklea, *U.S.-Mexican Security Cooperation: The Mérida Initiative and Beyond* (Washington: Congressional Research Service [CRS], 12 June 2013), 3, www.fas.org/sgp/crs/row/R41349.pdf; and "Mexican Military Takes Over Drug-Ridden Port," *AFP*, 4 November 2013, http://www.news24.com/World/News/Mexican-military-takes-over-drug-ridden-port-20131105-3.

[2] William C. Martin, "Cartels, Corruption, Carnage and Cooperation," in *A War That Can't Be Won*, ed. Tony Payan, Kathleen Staudt, and Z. A. Kruszewski (Tucson: University of Arizona Press, 2013), Kindle Loc. 1166/7339.

[3] Marcos Pablo Moloeznik, "President Felipe Calderon's Strategy to Combat Organized Crime," in *A War That Can't Be Won*, Kindle Loc. 1728/7339.

[4] David A. Shirk, "The Drug War in Mexico: Confronting a Shared Threat," Council on Foreign Relations Special Report no. 60, March 2011, Kindle Loc. 74/933.

[5] Paul R. Kan, *Cartels at War* (Washington: Potomac Books, 2012), 74.

[6] Michael Kelly, "Mexican Cartels Are Recruiting US Soldiers as Hitmen, And the Pay Is Good," *Business Insider*, 5 August 2013, http://www.businessinsider.com/cartels-are-recruiting-us-soldiers-as-hitmen-2013-8.

[7] "Mexico's Drug Lords: Kingpin Bowling," *Economist,* 20 October 2012.

[8] "Drug Traffickers Have Stranglehold on Guatemala Says Top Prosecutor," *El País*, 23 February 2011; and Hal Brands, *Crime, Violence and the Crisis in Guatemala* (Carlisle Barracks, PA: Strategic Studies Institute, 2010), 2.

[9] Adam Elkus, "Gangs, Terrorists and Trade," *Foreign Policy in Focus*, 12 April 2007. Salvadoran gangs in Los Angeles founded MS-13.

[10] Strategic Forecasting, Inc. (Stratfor), *Mexico in Crisis: Lost Borders and the Struggle for Regional Status* (Austin, TX: Stratfor, 2009), 197.

[11] See Gregory E. Maggs, "Assessing the Legality of Counterterrorism Measures without Characterizing Them as Law Enforcement or Military Action," 80 Temp. L. Rev., 661 (2007), 3 (online copy), http://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1826&context=faculty_publications.

[12] See *Tennessee v. Garner*, 471 U.S. 1, 11 (1985); US Army Field Manual (FM) 27-10, *The Law of Land Warfare*, 1956, chap. 2, sec. II, para. 29, citing annex to Hague Convention no. IV, 18 October 1907, embodying the Regulations Respecting the Laws and Customs of War on Land, art. 23(c); and Maggs, "Assessing the Legality of Counterterrorism," 4. See also Jimmy Gurule and Geoffrey S. Corn, *Principles of Counter-Terrorism Law* (St. Paul: West Group, 2010), 65; Army FM 6-20-10, *Tactics, Techniques and Procedures for the Targeting Process*, 8 May 1996, chap. 2. See generally "Protocol Additional to the Geneva Conventions of August 12, 1949 and relating to the Protections of Victims of International Armed Conflicts (1977), 1125 UNTS 3 (entered into force 7 December 1978)"; and "Protocol Additional to the Geneva Conventions of August 12, 1949 and relating to the Protection of Victims of Non-International Armed Conflicts (1977), 1125 UNTS 609 (entered into force 7 December 1978)."

[13] The Authorization to Use Military Force passed by Congress on 14 September 2001, P. L. 107-40, authorizes "all necessary and appropriate force" against persons who aided

organizations involved in the 9/11 attacks "to prevent any future acts of international terrorism against the United States."

14. Kan quotes from Michael Roth and Murat Sever, "The Kurdish Workers Party (PKK) as Criminal Syndicate: Funding Terrorism through Organized Crime," *Studies in Conflict and Terrorism* 30 (October 2007): 903, to state that cartels are "(1) involved in illegal activities and frequently need the same supplies; (2) exploit excessive violence and the threat of violence; (3) commit kidnappings, assassinations and extortion; (4) act in secrecy; (5) challenge the state and the laws (unless they are state funded); (6) have back-up leaders and foot soldiers; (7) are exceedingly adaptable, open to innovations, and are flexible and (8) enact deadly consequences for former members who have quit the group."

15. Kan, *Cartels at War*, 6–13.

16. Brad Freden, "The COIN Approach to Cartels: Square Peg in a Round Hole," *Small Wars Journal*, 27 December 2011, http://smallwarsjournal.com/jrnl/art/the-coin-approach-to-mexican-drug-cartels-square-peg-in-a-round-hole. Freden concedes, however, that some COIN principles and practices can support a law enforcement strategy to weaken or destroy the cartels.

17. Shibley Telhami, *The Stakes* (Boulder, CO: Westview Press, 2002), 35. Telhami's focus is on distinguishing between hostile or enemy forces and terrorists. For example, he points out that while the United States deems Hezbollah a terrorist organization, other parties, especially in the Middle East, do not, viewing it as a political or religious movement; and ibid., 9.

18. See Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: Public Affairs, 2013).

19. Kan, *Cartels at War*, 8.

20. Ibid., 7; See also Payan, Staudt, and Kruszewiski, eds., *A War That Can't Be Won*.

21. Tony Payan, "The Many Labyrinths of Illegal Drug Policy," in *A War That Can't Be Won*, Kindle Loc. 352/7339.

22. Harold D. Lasswell, *Politics: Who Gets What, When and How* (Gloucester, MA: Peter Smith Publishing, 1990).

23. Maurice Cranston, "Ideology," *Encyclopedia Britannica*, http://www.compilerpress.ca/Competitiveness/Anno/Anno%20Cranston%20Ideology%20EB%202003.htm. The French philosopher Destutt de Tracy expounded affirmative characteristics. Karl Marx saw ideology as a set of beliefs with which people deceive themselves—a theory that expressed what they are led to think as opposed to that which is true. Ibid.

24. Louise Richardson, *What Terrorists Want* (New York: Random House, 2006), 85.

25. Ibid., 75. She discusses various motives that animate terrorist organizations, including revenge, publicity, seeking concessions, causing disorder, provoking repression, making a show of strength.

26. Ibid., 86–87.

27. W. Alex Sanchez, "The End of Ideologically Motivated Violent Movements in Latin America?" *e-International Relations*, 24 September 2012, www.e-ir.info/2012/09/24/the-end-of-ideologically-motivated-violent-movements-in-latin-america/. Sanchez also falls into the trap of conventional definitions in failing to recognize that profiting from illegal activity can qualify as both a criminal and political agenda, although one does not necessarily imply the other.

28. Richardson, *What Terrorists Want*, 86.

29. Olivier Roy, trans. Carol Volk, *The Failure of Political Islam* (Cambridge: Harvard University Press, 1994). Roy argues persuasively that political Islam has failed to define a concrete vision and, to the extent that one has been, it bears a closer resemblance to radical leftwing politics than religion.

30. Ioan Grillo, *El Narco*, (London: Bloomsbury Press, 2011), Kindle Loc. 2747/6409.

31. "Teens Lured into Mexican Drug Cartels," *Big Country* (Nexstar Broadcasting, Inc.), 19 April 2009, www.bigcountryhomepage.com/story/teens-lured-into-mexican-drug-cartels/d/story/cSPztt2XMEW2GeUVZ-XmRQ.

32. Watt and Zepeda, *Drug War in Mexico*.

33. Sylvia Longmire, *Cartel* (New York: Palgrave MacMillan, 2011), 102.

34. Ricardo C. Ainslie, *The Fight to Save Juarez* (Austin: University of Texas Press, 2013), Kindle Loc. 4206/6219.

35. Grillo, *El Narco*.

36. Quoted in Josh Kun, "Death Rattle," *American Prospect*, 5 January 2012, http://prospect.org/article/death-rattle.

37. Ashley Fantz, "The Mexico Drug War: Bodies for Billions," *CNN.com*, 20 January 2012, http://www.cnn.com/2012/01/15/world/mexico-drug-war-essay/index.html.

38. Kan, *Cartels at War*, 43–45; and Akbar Khan, "The War on Drugs: Mexican Cartels," *Generation.net*, 29 May 2013, http://the-generation.net/the-war-on-drugs-mexican-cartels/. Kan quotes one observer who calls La Familia Michoacana a "faith-based, right-wing populist socialist movement" run by a criminal organization.

39. Tim Padgett and Ioan Grillo, "Mexico's Meth Warriors," *Time*, 28 June 2010, http://content.time.com/time/magazine/article/0,9171,1997449,00.html; and William Finnegan, "Silver or Lead," *New Yorker*, 31 May 2010, www.newyorker.com/reporting/2010/05/31/100531fa_fact_finnegan?currentPage=all.

40. Kan, *Cartels at War*, chap. 2, well describes the business plan that cartels employ.

41. Payan, "Many Labyrinths of Illegal Drug Policy."

42. Blog del Narco, *Dying for the Truth*; Oscar Villalon, ed., *Blood Calls to Blood: Mexican Writers on the Drug War* (San Francisco: By Liner, 2012); Alfredo Corchado, *Midnight in Mexico: A Reporter's Journey Through a Country's Descent into Darkness* (New York: Penguin Press, 2013); Ainslie, *Fight to Save Juarez*; and Guadalupe Correa-Cabrera and Jose Nava, "Drug Wars, Social Networks and the Right to Information," in *A War That Can't Be Won*.

43. Payan, "Many Labyrinths of Illegal Drug Policy." See also Ed Vulliamy, *Amexica: War along the Borderline* (Farrar, Strauss & Giroux, 2010), 246. Shawn Teresa Flanigan has drawn interesting parallels between the Mexican drug cartels and Hamas and Hezbollah. All are tied to relatively defined geographic locations. All seek to control specific territory to maintain access to drug trade routes. All have deep, sophisticated relationships with the states within which they operate. See Flanigan, "Terrorists Next Door? A Comparison of Mexican Drug Cartels and Middle Eastern Terrorist Organizations," *Terrorism and Political Violence* 24, no. 2 (2012): 279–94.

44. Payan, "Many Labyrinths of Illegal Drug Policy."

45. Ainslie's *Fight to Save Juarez* offers a riveting account of the bloodbath that cartel violence has inflicted on that city. It is an excellent study of how Mexico's government has failed to cope. See also George W. Grayson, *Mexico: Narco-Violence and a Failed State?* (New Brunswick, NJ: Transaction Publishers, 2009). There is wide reporting on the corruption problem.

46. See Vulliamy, *Amexica*, 247. He goes into great detail about the extortion practiced among even small businesspeople.

47. George W. Grayson and Samuel Logan, *The Executioner's Men* (New Brunswick: Transaction Publishers, 2012); and Longmire*, Cartel.*

48. Kan, *Cartels at War*, 150–51.

49. Christopher S. Ljungquist, "Mexican Cartel War: Profiling an Unorthodox Insurgency," *Geopolitical Monitor*, 4 February 2013, http://www.geopoliticalmonitor.com/mexican-cartel-war-profiling-an-unorthodox-insurgency-4777.

50. "Clinton Says Mexico Drug Crime like an Insurgency," *BBC News*, 9 September 2010, http://www.bbc.co.uk/news/world-us-canada-11234058.

51. Bard O'Neil, *Insurgency and Terrorism: From Revolution to Apocalypse*, 2nd ed. (Washington: Potomac Books, 2005); and David J. Kilcullen, "Three Pillars of Counterinsurgency," remarks delivered to the US Government Counterinsurgency Conference in Washington, DC, 28 September 2006, both cited in Freden, "COIN Approach to Mexican Drug Cartels."

52. Army FM 3-24.2, *Tactics in Counterinsurgency*, April 2009, https://www.fas.org/irp/doddir/army/fm3-24-2.pdf.

53. Terrorist organizations and criminal groups may have peripheral connections (arguably, al-Qaeda). Terrorist organizations may have criminal sympathizers (arguably, Hezbollah). Criminal entrepreneurs may act as specialists or shadow facilitators for terrorist groups (arguably, Viktor Bout, Abu Ghadiyah, Monzer al-Kassar). Terrorists groups and criminals organizations may collude (arguably, the Taliban and drug traffickers). See http://fpc.state.gov/documents/organization/141615.pdf.

54. Statements by Stephen W. Casteel (DEA) and Raphael Perl (CRS), "Narco-Terrorism: International Drug Trafficking and Terrorism—A Dangerous Mix," prepared for a hearing conducted by the Senate Judiciary Committee, 20 May 2003; and Michael Braun, "Drug Trafficking and Middle Eastern Terrorist Groups: A Growing Nexus?" speech at the Washington Institute for Near East Policy, 18 July 2008. The CRS observes that the US government lacks a strategy or policy to address comprehensively the confluence of terrorism and transnational crime. John Rollins and Liana S. Wyler, *International Terrorism and Transnational Crime: Security Threats, U.S. Policy and Considerations for Congress* (Washington: CRS, 18 March 2010), 4.

55. Dana Priest, "U.S. Role at a Crossroads in Mexico's Intelligence War on the Cartels," *Washington Post*, 27 April 2013, http://www.washingtonpost.com/investigations/us-role-at-a-crossroads-in-mexicos-intelligence-war-on-the-cartels/2013/04/27/b578b3ba-a3b3-11e2-be47-b44febada3a8_story.html.

56. See Pamela F. Izaguirre, "Narco-Politics: How Mexico Got There and How It Can Get Out," *Council on Hemispheric Affairs*, 22 August 2013, www.coha.org/narco-politics-how-mexico-got-there-and-how-it-can-get-out/.

57. Priest, "U.S. Role at a Crossroads."

58. Ibid.

59. Mark Urban, *Task Force Black* (Little, Brown, & Co., 2011).

60. Priest, "U.S. Role at a Crossroads."

61. Watt and Zepeda, *Drug War in Mexico*.

62. See James P. Farwell, *Persuasion and Power: The Art of Strategic Communication* (Washington: Georgetown University Press, 2012); and Longmire, *Cartel*. Longmire presents an excellent description of those challenges and how Calderon perceived and addressed them.

63. Seelke and Finklea, *U.S.-Mexican Security Cooperation*, 3. See also Craig A. Deare, "U.S.-Mexico Defense Relations: An Incompatible Interface," Strategic Forum, Institute for National Strategic Studies, National Defense University, July 2009; and Statement of Assistant Secretary of State for International Narcotics and Law Enforcement Affairs William Brownfield, US House Committee on Foreign Affairs, Subcommittee on the Western Hemisphere, "U.S.-Mexico Security Cooperation: An Overview of the Merida Initiative 2008–Present," 113th Cong., 1st sess., *CQ Congressional Transcripts*, 23 May 2013.

Spring 2013

Why Cyber War Will Not and Should Not Have Its Grand Strategist

Martin C. Libicki

Cyber war proponents often argue the domain needs its own Billy Mitchell or Giulio Douhet—strategists with great vision who will declare to the world what great power lies therein.[1] To be sure, cyber war has no shortage of advocates. But as Colin Gray recently observed, "When historians in the future seek to identify a classic book or two on cyber power written in the 1990s and 2000s, they will be hard pressed to locate even the shortest of short-listable items. . . . Certainly they are nowhere near deserving (oxymoronic) instant classic status."[2]

But has the failure of cyber war to generate any such ideal necessarily been a bad thing? There is a case to be made that it is too early to expect such a classic. If the Owl of Minerva flies at dusk, in cyberspace the sun is just above the yardarm; the information revolution is hardly a done deal. But such a case is too easy. What if the fundamental features of cyber war were to remain essentially as they are into the indefinite future? Although highly unlikely, this is not so absurd a proposition. The late Roger Molander of RAND would frequently remind me that the questions we wrestled with in the mid 1990s are no less relevant and no better understood today than they were then.

Even assuming that the cyber domain has yet to stop evolving, it is not clear that a classic strategic treatment of cyber war is possible, or, even if it were, it would be particularly beneficial. In explaining why, this article makes three points. First, the salutary effects of such classics are limited. Second, the basic facts of cyberspace, and hence cyber war, do not suggest that it would be nearly as revolutionary as airpower has

Martin C. Libicki is the Maryellen and Dick Keyser Distinguished Visiting Professor at the US Naval Academy's Center for Cybersecurity Studies and author of *Cyberspace in Peace and War*. His research has focused on the impact of information technology on domestic and national security. Previously, he worked for RAND (where he is still adjunct), the National Defense University, and the Navy staff. He holds a master's degree and a PhD from the University of California–Berkeley.

been, or anything close. Third, more speculatively, if there were a classic on cyber war, it would likely be pernicious.

The Limited Usefulness of Classics

Clausewitz's *On War* was, is, and will continue to be perhaps *the* classic book on warfare, but it would be an exaggeration to argue that it was an "instant classic." It was published posthumously. Its influence spread slowly—within a generation in Germany and not until after 1945 in the United States. Furthermore, it really is not a book that gained its reputation by talking about land warfare as such. True, all of its chapters between the introduction and conclusion discuss that subject. But what made it a classic was its treatment of war itself—that is, the role and purpose of military force within the relations among states and the relationship between the goals of war and its reality in battle ("fog and friction").

In the naval domain the name Mahan is clearly front and center. Mahan lauded naval power as essential to the maintenance of a seafaring state, especially one that wanted to maintain a global empire—not an irrelevant consideration circa 1890 when he published *The Influence of Sea Power upon History, 1660–1783* (such historic dates suggest he was not overly impressed by technology fads). His book argued strenuously for large battle fleets, which by their very presence and concentration ("fleet in being") could dissuade other states from trying to assert sea control on their own behalf. He eschewed the *Jeune Ècole* preference for commerce raiding.

Mahan's work was enormously influential inside the United States (an inspiration for Theodore Roosevelt's Great White Fleet), and perhaps even more outside it. Kaiser Wilhelm was particularly enchanted by it, as were, to only a slightly lesser extent, Jackie Fisher and the British Royal Navy. Although the expensive Anglo-German naval rivalry cannot be entirely laid at Mahan's doorstep, his influence was not trivial, and the rivalry over battleship building hardly played a calming role in that bilateral relationship.

But as for naval strategy, Mahan's work was not particularly helpful for those who believed in his doctrine. The Kaiser's love for his fleet kept it in port for the two and a half years after the Battle of Jutland, even though Germany might have had a chance—admittedly, with a substantial amount of luck—to break the blockade on it and the Austro-Hungarian Empire. This blockade ultimately accelerated the Central Powers breaking under the stress of war before the Allies defeated them on the ground, finishing the job. Meanwhile, the naval action that nearly broke the war the other way was the success of German U-boat attacks on Britain's supply lines to North America. In retrospect, the more decisive use for naval power in World War I was closer (albeit with submarines, not surface ships) to the commerce-raiding that Mahan disdained 25 years earlier in favor of grand fleet actions. He had argued these fleet actions were the sine qua non of naval power.

All this suggests that the global enthusiasm over Mahan's writing—which *was* an instant classic—was good neither for world peace nor a productive naval strategy. Perhaps these are tough tests for any analyst to pass, but if we are to laud the writing of great strategic formulations these are not unfair evaluations.

Consider now airpower. Three individuals stand out in the development of post–World War I strategic thought: the writer Giulio Douhet and generals Billy Mitchell and Hugh Trenchard. All three argued that air forces would become an increasingly important component of modern militaries and that military strategy should, correspondingly, reflect that fact. In that insight, they were correct.

Douhet went further to emphasize the role of strategic bombardment in not only winning future wars, but also shortening them (in that respect—if World War II was any indication—he was not correct). There is an important distinction to be made between the tactical or operational use of airpower (to aid ground and naval forces) and its strategic use: to break the enemy's will to resist and destroy its ability to arm itself. In theory, air forces can do both operational and strategic missions; in practice, their resources are limited, and funds used for strategic purposes compete for resources used operationally.

This leads to the question: Was World War II's emphasis on the strategic campaign such a good idea? In the first major war in which this proposition could be truly tested, only three countries were capable of mounting a serious strategic bombing campaign—first Germany, then the United Kingdom and the United States. Germany's efforts did not seem to have accomplished much; it did not force the UK out of the war nor make much of a dent in its war production. The US and UK bombing campaigns certainly had effects, but these effects were purchased at great cost—the Eighth Air Force alone suffered more than 27,000 deaths (by comparison, the entire US Pacific campaign cost fewer than four times as many lives).

The succeeding decades saw considerable controversy over whether such bombing campaigns were worthwhile, with detractors saying they *increased* Germany's will to resist and, only toward the very end, impaired its ability to produce war materiel. A recent prominent defense of strategic bombing by Richard Overy maintains they were worthwhile,[3] not for what harm they did to the Germans, but for how much Germany spent (mostly wasted) to counter them. Even if true, that is a far cry from Douhet's rationale ("air power will demoralize foes" to "air power will cause foes to overreact in self-defense"). Admittedly, a B-29 loaded with nuclear weapons can have a considerably greater effect than a B-29 loaded with conventional weapons—a victory for airpower, but only for 15 years until missiles were invented to do the job more efficiently and reliably. Furthermore, it took until NATO's campaign in Kosovo before there was a first, albeit even then arguable, validation of Douhet's thesis.

If the strategic implications of airpower were poorly understood by virtue of their being exaggerated, the operational implications of airpower à la Billy Mitchell (and many others at the time, if not so dramatically) were on point. Airpower *would* rise in importance relative to land and sea weapons. At sea, by 1942 the carrier was universally recognized as the replacement for the battleship, although the carrier was under firm naval control. Only a half-century after World War I, success in gaining air control (the 1967 Six-Day War and Operations Desert Storm and Iraqi Freedom) predisposed and foretold success in ground combat (at least over uncluttered terrain).

The basis for Billy Mitchell's optimism was, in retrospect, clear. Every year, aircraft became faster; flew higher, farther and longer; and could carry more weight (weapons but also cargo). Antiaircraft weapons were improving but not so quickly (targeting radar and analog computing helped but only somewhat). Nor were ground or sea-based weaponry getting more impervious to bomb damage all that quickly. Technology was inexorably shifting the dominance of battle to the skies. That being so, every other decision about the conduct of battle would have to factor the shift in power relationships from ground and surface to air accordingly.

As noted, nothing boosted airpower as much as the development of atomic weapons, which seemed to have validated Douhet's thesis, at least ex post facto. The US Air Force came to absorb almost half of the nation's defense budget in the Eisenhower administration. Clearly, a single weapon capable of knocking out cities was going to have a strategic effect on both war and warfare. So, were there any classics in this new *atomic* field, and what good did they do?

The first place to look was a set of essays by Bernard Brodie for the book, *The Absolute Weapon: Atomic Power and World Order*,[4] wherein can be found his famous quote: "Thus far the chief purpose of our military establishment has been to win wars. From now on its chief purpose must be to avert them. It can have almost no other useful purpose." His essays do mention deterrence, but the thrust of his writing was not about how to use atomic forces but to drive home the point that a country under serious atomic attack (that is, thousands of atomic bombs) would be effectively destroyed regardless of how well defended it was. Indeed, his essay spends more time on how to lay out cities to maximize their survivability in an atomic war than it does contemplating what a strategy of deterrence might mean for the construction and the use of forces. So, instant classic quote but no instant classic work.

More works followed in the 1950s by Albert Wohlstetter (on the importance of a second-strike capability),[5] Tom Schelling (on strategies that "left something to chance"),[6] and Herman Kahn (on the need for escalation dominance).[7] It was undoubtedly brilliant stuff, but was it necessarily a wise way to fight—or, better yet, avoid—a nuclear war? The classic model of a nuclear confrontation featured ultra-cool decision makers rationally facing the prospect of mega deaths and maneuvering deftly to avoid that and worse. The actual conduct of a nuclear crisis (Cuba 1962) suggested something a little different: world leaders, having stared at the abyss, realized they had come far too close to a nuclear holocaust and never ever wanted to get that close again. Reactions to that near catastrophe included the hotline and the 1963 test ban treaty. Rather than each side making noises as if it would throw the steering wheel out the window (as Schelling's strategy suggested), each instituted measures to ensure and assure others that it had a much better grip. Similarly, strategic thinking, deprived of direct evidence of Soviet thought, tended to assume that the Soviet Union would approach a confrontation much as Americans would—that is, by carefully delineating (if not necessarily observing) a firebreak between conventional and nuclear operations. The opening of the Soviet archives in 1989 indicated that such delineations were not particularly important to them. Fortunately, no one ever had to go to war based on these strategic theories.

Incidentally, none of this infers that such thinkers did not educate the mind by raising key questions. Even when wrong, one cannot help but profit by working through arguments and, in some cases, asking whether their logic applies to cyberspace. Unfortunately, when such thinkers are cited as authorities—which they inevitably are—their arguments are converted into answers, at least in the minds of their adherents.

The next two domains of conflict—space and spectrum—have no comparably memorable strategic doctrines or assessments associated with them at all. This, alone, should raise the question of why cyberspace should. Once touted as the really high ground, outer space turns out to be merely a nifty place to stick information collection/transmission devices—surveillance satellites, communications relays, and timing/navigation systems (e.g., GPS)—and it is not clear that space will always remain competitive vis-à-vis networked unmanned air-breathing systems for the first two roles. Space is not a particularly good place from which to fight wars. It costs a great deal to get something into orbit, and the price per pound has not appreciably fallen since the 1970s. Space-based weapons are not only expensive but, in their current incarnation, take longer to reach their targets than do simple missiles[8]—deorbiting something actually takes some time. Space systems are also quite fragile in the sense that they can be destroyed by a very small object hitting head-on at a relative speed of 36,000 miles an hour, assuming they are both in low-earth orbit. In a contest between a ground-based missile and a satellite, the odds (these days) are on the missile. So, much to the anguish of the space community, here is a domain without a strategic concept, and, at this point, not inappropriately. It is easy, incidentally, to get lost in arcane debates over which orbit in space is truly the high ground that dominates all the other orbits in space (true aficionados wax rhapsodic about controlling the L1 point, which is roughly four times as far from the earth as the moon and sits directly between the sun and the earth).

Finally, a word is needed in defense of the radio-frequency (RF) spectrum as a domain of warfare, mostly because this domain not only lacks a strategic theory but also lacks a strong proponent for theory-building. Yet, it is a *physical* domain in which dominance, in the sense that those who can get their signal through and keep others from getting their signal through, thereby gives its possessor a signal advantage in warfare. No serious military power ignores electronic warfare, largely because radio communications allow militaries to coordinate their operations and radar allows detection and tracking of all manner of enemy assets. But the wizards in the business know the purpose of manipulating the use of a spectrum is to enable physical warfare; by itself, electronic warfare is next to worthless. Similarly, no one seriously thinks that one country can wreak persuasive or dissuasive damage on another by unleashing its electronic warriors on it, although the latter may be the source of some interesting forms of annoyance, particularly if they can interfere with all GPS applications and mobile devices.

The Significance of Warfare in Cyberspace

It should be fairly clear by now that this article will not close with a ringing call for a strategic cyberspace doctrine. As oft noted, such doctrines—even, or especially, if they meet with universal approbation—are as likely to be wrong as they are right.

To start with, cyber warfare and cyber war need to be distinguished from one another. Cyber warfare, like warfare itself, is about the conduct of war, carried out inevitably to further the performance of combat in the physical domain (it can also be considered operational or instrumental cyber war). Cyber war is undertaken to affect the will of the adversary directly (it can also be considered tantamount to strategic cyber war). A similar distinction can be made between electronic warfare and electronic war—the difference being that no one talks about electronic war as something interesting.

First we can ask whether cyber warfare can so alter warfare that warfare—how it is conducted and what one can do with it—needs to be seriously rethought. Although the ultimate answer to that question is empirical and yet to be determined, it is easy to establish that such a question cannot be answered without an important intermediate step. Cyber warfare attacks systems and digital networks. Prior to the 1960s, militaries had no digital networks to attack. A cyber attack carried out against a military today can, at worst, return it to its prenetworked condition (as long as it *has* something to revert to). To argue that cyber warfare can have a revolutionary effect on the battlefield requires establishing that digital networking is itself revolutionary. This is a step many proponents of cyber warfare neglect to take.

So how much *does* digital networking improve the workings of a military? First, one does not need digital communications to have RF communications; the latter can be carried out with analog equipment as it was prior to the 1970s, and, to some extent, still is. Second, as helpful as network-centric warfare may have been for the United States, every other military in the world is less digitized and therefore less susceptible to cyber war than the US military (notwithstanding the possibility that the digital equipment they have is more vulnerable than the equivalent in the hands of US forces).

Thus, the revolutionary impact of cyber warfare can be no greater than the revolutionary impact of digital networking, which is not, itself, a fully tested proposition. The question of how much less entails asking how effective cyber warfare can be at nullifying the advantages of digital networking. The most it can be is 100 percent, but there are many simple measures militaries can take to reduce it well below 100 percent. One is electronic isolation. If a network is disconnected from the rest of the world, it is very difficult for outsiders to penetrate it. In practice, as Buckshot Yankee and Stuxnet proved, it is not enough that a network lacks an Internet address (or a phone number). There also has to be no way for errant bytes to get into these machines via RF links that can leverage the strength of the attacker's transmitter. These are challenging problems but hardly insurmountable. For the most part, systems can be immunized against much of cyber warfare if their instructions are difficult to alter without hands-on contact. This could be because the logic is hardwired into the unit, or because the logic can only be replaced by new hardware modules, or the update has to be digitally signed by a known trustworthy source (using reliable cryptographic protocols implemented correctly). This prevents malware or malicious software with rogue instructions from being placed on the machines, which then limits a machine's actions to those prespecified in its programming. Stuxnet, (and its relatives such as Flame) as well as much of cybercrime, and the advanced persistent threat all depend on the possibility of malware (arbitrarily altered instruction sets) to work.[9]

All this suggests that the effect of cyber warfare, if properly recognized, will be far less revolutionary than the putatively revolutionary effect of digitized networking.

In fairness, consider two objections to this argument. One is that militaries cannot revert to their predigitized network state. This may be empirically true, but if true, it says either that (1) such militaries have abjured that option because they *correctly* recognize that the impact of cyber warfare is something they can manage, or (2) the revolutionary impact of cyber warfare is *incorrectly* underappreciated by militaries who consequently digitize without giving sufficient thought to what would happen if cyber warfare *were* revolutionary. If the former is true, the issue is settled. If the latter is true, then the only way cyber warfare could be revolutionary is if those victimized by it fail to see it was going to be revolutionary. This is the sort of error that is unlikely to be made more than once, if it is even made at all. Consider, by way of example, Stuxnet. If Iranians had understood what Stuxnet *could* have done to them, they would have likely taken pains to ensure that no USB device was accessible. Because it came as a surprise, Stuxnet worked. But can one assign revolutionary strategic impact to a form of warfare that requires it be systematically underestimated before it can work?

The second objection is that while cyber warfare is not much to look at now, it is only to get more important as militaries continue to digitize. This line echoes the argument that aircraft were going to get better every year; thus, what was false today may be true tomorrow. Can the same be said about cyber warfare?

At this point in the article, one distinction between cyber warfare and warfare in all other media must be made: cyber warfare (as well as cyber war) requires that the targets have made mistakes in their implementation and use of digital equipment. In theory, digital machines should only obey their given instructions in service of their owners/operators. In practice, there are variations between what a system actually does and what it is supposed to do that permits cyber warfare to work. But neither the form nor even the existence of these variations is inevitable. They are artifacts of systems programming. Such artifacts can be reduced, perhaps even effectively eradicated. As noted above, even if systems still have errors, users—especially military users—have a great number of steps they can take to reduce vulnerability to cyber warfare. Indeed, many such steps are being taken—and, doubtlessly, more would be taken if the threat from cyber attacks and the like were greater (or at least perceived to be greater) than is currently the case. This is no proof that there will be a declining threat from cyber warfare to advanced militaries (militaries that have failed to advance have little or nothing to attack in cyberspace); it may well grow. The fact that the threat from cyber warfare has to be enabled by the target's decisions weighs against the proposition that cyber warfare can be revolutionary.

Indeed, there is every indication that electronic warfare will continue to generate more consequential effects on the battlefield than cyber warfare because electronic warfare is not an artifact of the other side's poor decisions. It is an unavoidable aspect of long-distance RF communications. And, as noted, there is no classic strategic treatment of electronic warfare; nor is there indication that such effort is missed.

That leaves the question of whether strategic cyber war can be significant enough to merit some twenty-first-century version of the Douhet proposition: a form of war that can induce countries to stop fighting (or better, avoid starting fights) without having been defeated or threatened on an actual battlefield. Arguments similar to those above can be generated to suggest that such a thesis is not terribly convincing today. Most cyber attacks, once discovered, are resolved and the effects (apart from leaked information) reversed within a period ranging from hours to days. In the long run, even in the highly unlikely event that hackers will always be able to control the systems they attack, the worst that can happen would be to convince people to abandon networking and thus set economies back to where they were in 1995 (when the Internet started to spread beyond universities and defense-related sites).[10] For advanced countries, 1995 is not that much further behind than they are in 2013. Thus an economy subject to continuous, vicious, and expectedly successful attacks would not retrogress as much as a society subject to World War II–level bombing. And cyber attacks have yet to kill anyone. Granted, if societies have evolved in ways that are difficult to reverse, the effects of cyber war on such societies may be worse than if they had never adopted digitized networks in the first place. But such effects, almost by definition, can be used only once—and only if a society's leadership systematically underestimates its vulnerability to cyber war. Of course, if cyber war turns out to be weak, then perhaps they have not underestimated it at all.

Over time, the distance between 1995 and the then-current year will increase, which will, in theory, lend cyber war more leverage than it has today. Perhaps then, it will be possible to write how cyber war has changed everything we know about warfare. Or maybe not. True, just as aircraft grew monotonically more capable from their invention forward, so societies are growing increasingly digitized, with little prospect that they will move backward (unless, cyber attacks prove to be far more powerful and unavoidable than they are today). But the correlation ends there. Aircraft improvement was a contest against a fixed target (the laws of aeronautics, physics, and chemistry); cyber war is a contest against a moving target wherein offense contends with defense. It is not obvious that offense will get continually better, particularly when defense (in the form of the target's system and software) defines what the offense can do. Granted, hackers are getting better, thanks in part to markets and market-like mechanisms for sharing information about software vulnerabilities. Furthermore, new uses for digitization (e.g., networked cars) are constantly creating new vulnerabilities or new ways for vulnerabilities to do serious damage. But defense is not catatonic. If the problem with cyber attacks gets bad enough, there are more radical steps that can be taken. One example is Apple's iOS operating system, which has successfully resisted malware because it is a fairly closed system (although some countries have been rumored to have prepared and stashed away attacks on it). Another is the consensus reached by security professionals that Java (software) should be disabled on all browsers because it is becoming very difficult for its developer to stay ahead of all the vulnerabilities hackers keep discovering in it. On purely technical grounds, every successive version of Microsoft's products is more malware-resistant than its prior versions. These days operating systems are subverted by insecure applications rather than being attacked directly. So, the technology dynamic that Billy Mitchell employed—even if aircraft cannot do it today, tomorrow's eventually will—does not necessarily translate into cyberspace, even if cyber security may get worse before it gets better.

Then there is the possibility that the strategic effects of cyber war may arise from the interaction of state actors that systematically overestimate its effects (as quasi-apocalyptic statements from both US and Chinese military officials suggest is quite possible). This could lead to unfortunate dynamics, but in the longer run, the problem with such analyses is similar to those analyses that posit leaders *underestimate* the effects of cyber war and are therefore unprepared in ways that make it more dangerous. Either way, this is an attitude capable of being corrected by events, and, by its very nature, of temporary import (unless one can successfully argue that the *perception* of what cyber attacks *have done* is systematically in error, but that is a hard case to make).

Cyberspace, as it turns out, is ill-suited for grand strategic theories for other reasons. As mentioned earlier, cyberspace *is* changing very quickly in many important respects. Circa 1999, for instance, US cyber war capability, such as it was, housed itself within the US Space Command (disestablished in 2002). In an era in which mischief in cyberspace was most likely perpetrated by individual hackers who were adroit at getting into systems, maneuvering deftly while discovering how they worked, doing their job, and leaving quietly, its working ethos would have made it a natural fit for something like the US Special Operations Command. Fortunately, that never happened, because within a dozen years, it was clear that hacking was less about individual rough-and-ready hackers and more like a team-based enterprise building malware tools that took commands from afar and otherwise went about their business based on their programmed-in wits. Today, the original fit between cyber war and the space business looks better—although the fit between US Cyber Command and the National Security Agency is quite good itself.

Another difficulty in proposing a grand theory of cyber warfare is that deception lies at the essence of cyber war. Systems, although meant to be under the control of their owners/operators, are tricked into obeying the commands of others. Once the precise nature of the trick is realized, it is relatively straightforward to figure out how to foil that particular attack; this requires hackers to come up with new tricks, which they often but cannot always do. Deception, by nature, introduces its own self-defeating dynamic, because its existence depends on two sides having different notions of what something can do. Success, in certain key respects, is often inherently unpredictable. Those who wrote strategic theory for, say, airpower had the advantage of understanding the interaction between the machine and its aeronautical environment and between weapons and their targets. They could use that solid base to speculate on the relationship between the effects caused by aircraft and the goals for which countries went to war. Those who would write strategic theory for cyberspace have no such foundation. Everything appears contingent, in large part, because it is.

The Possibly Pernicious Effects of Writing a Cyber War Classic

To be fair, it is not easy to counter what some yet-to-be-written cyber war classic would say. Setting forth here the brilliant insights of such a classic would create the tome this article says cannot exist. Yet, if cyber war's forthcoming classic looks like classics in past domains, they are likely to say (1) cyber war is totally important, (2) those who wield its power should fight to win wars on their own rather than helping warriors in other domains, and (3) war fighters in those other domains should take their strategic cues from what takes place in cyberspace.

To say that war in the virtual world can match the horrors of war undergone or contemplated might seem a stretch, but anyone who ventured such an opinion would not stand alone. Joining them would be the US Defense Science Board (which imagined a cyber attack so severe as to merit a nuclear response),[11] some Chinese generals (one of whom casually opined that a cyber attack could be as damaging as a nuclear attack),[12] and even Russian president Vladimir Putin (who said that a cyber war could be worse than conventional warfare—this from the head of a country that lost 25 million in World War II).[13] There is nothing quite like a good nuclear analogy to rally those in favor of an independent cyber-war force. Yet, the mere argument that cyber war is going to be very important hardly says what to do with cyber-war capabilities, apart from keeping them well fed.

Emphasizing the strategic aspects of cyber war over its tactical (alternatively, operational or instrumental) aspects is not necessarily wrong. Because the operational uses of cyber war are neither ethically nor particularly strategically problematic[14]—in that it only substitutes nonlethal for lethal means—there is little reason *not* to use it against military targets. But military targets are generally harder targets than civilian ones. What may produce limited gains on the battlefield may produce huge payoffs off the battlefield, thereby tempting the elevation of the strategic over the operational.[15] But such elevation has consequences. It affects the allocation of resources and manpower. If talented cyber warriors convince themselves that strategic warfare offers a better shot at top command slots, they will migrate accordingly. Perhaps if cyber war *is* that important, there will be enough resources and manpower to go around—although the current difficulties in finding enough cyber-security professionals suggest that their supply is not infinite and only time will tell how elastic. However, there are certain resources where serious choices must be made: that is knowledge of vulnerabilities in software that allows cyber warriors into many of their targets. To the extent military and civilian systems rely on the same software and hardware—as they increasingly do, although there are still major differences—then a vulnerability exploited for disruptive/destructive purposes (rather than espionage) is likely to be a vulnerability that can be used only during a small time window. Its availability for strategic purposes limits its availability for military purposes. Hence, choices, notably between operational and strategic cyber war, must be made. Because systems have to be penetrated well before they are attacked, such choices may have to be made well before the character of the upcoming conflict is clear.[16]

Consider, too, that both forms of cyber war—the strategic and the operational—compete with cyber espionage when it comes to allocating vulnerabilities to exploit.[17] Those who want to reserve the exploit for cyber espionage can make two strong points. First, since penetration, in and of itself, tends to be deliberately stealthy, the vulnerability can remain hidden longer than it can once a disruptive/destructive attack takes place.[18] Second, the yield from cyber espionage can be immediate, while the yield from getting into a system that might be taken down is contingent on a war starting.

Strategic cyber war is far more problematic than its operational cousin. It raises laws-of-armed-conflict issues that operational cyber warfare does not. Similarly, it is more likely to result in escalation and in ways that make conflict resolution more difficult. By contrast, operational cyber warfare ends when kinetic warfare ends, because there is no longer any advantage in making targets more susceptible to kinetic attack when kinetic attack terminates.

If the galvanizing theory emphasizes doctrines such as preemption, further difficulties await. Although exactly how to preempt a cyber attack remains a mystery, there is very little that can be destroyed, and only a narrow class of attacks can be disrupted by actions taken outside one's network. If the doctrine is attractive enough, people will think they have found a way to do so. Unfortunately, the many ambiguities of who is doing what to whom in cyberspace suggest that understanding who is preparing to do what to whom is even harder to discern. Grave mistakes are possible—particularly if the decision to preempt attacks is delegated from the president, as many have suggested it might be.[19]

Finally, what might be those cues that warriors in today's domains should take from cyberspace according to some yet-to-be-written doctrine? Cyber war is sneaky stuff. It relies on deceiving computers, which, in turn, requires deceiving humans who manage these computers. It usually works a great deal better when it comes without warning. Insofar as its success depends on the discovery of impermanent elements in the target system, laid-in attacks have to be used quickly if they are to be used at all. Furthermore, because many of its effects are temporary, they must be exploited in a very short time (as quickly as within hours and days). In that sense, powerful cyber attacks can pull follow-up strategic or operational actions behind them, whether or not the latter are, respectively, appropriate or ready. Cyber war is also an elite activity in which numbers of hackers count for little but the skills of the best of the best count for a great deal.

Cyber operations are covered in heavy layers of secrecy. In some ways, secrecy is deserved: vulnerabilities described quickly become vulnerabilities eradicated. But in other cases, it is questionable: no country admitted to having cyber-war forces until 2012. And in other ways, particularly when disclosing information about vulnerabilities that the other side found in the systems of commercial organizations, it can get in the way. All this makes it difficult to have a serious public debate about the role of cyber war in national security. To be fair, the common difficulty of understanding cyberspace also interferes with useful public debate. Hence the question: Would it be beneficial for the mores of physical war fighting to reflect the inherent mores of war fighting in cyberspace? Perhaps not.

Conclusions

So, rather than bemoan the fact that there are no instant strategic classics on cyber war, or even well-percolated ones, perhaps we should count ourselves lucky. Many of the strategic classics from earlier domains seem to have been misleading, even harmful. War fighters that deal with the more recent media, such as outer space or the radio-frequency spectrum, seem to be doing just fine without them. And cyber war appears to have even less basis for a strategic treatment than space warfare or electronic warfare. Its efficacy—much less significance—has been postulated well before it has been proven. By its very nature, cyber war has to continually morph to retain its relevance. Furthermore, there are good reasons to believe that its contribution to warfare, while real, is likely to be modest, while its contribution to strategic war is a great deal easier to imagine than to substantiate. SSQ

Notes

[1] To those who think the argument in favor of finding a Billy Mitchell for cyberspace is a straw man, note the following requests from Frank Cilluffo, former special assistant to

the president for homeland security: "We must find the cyber equivalents of Billy Mitchell, George Patton, Curtis LeMay and Bill Donovan—leaders who understand both the tactical and strategic uses of new technologies and weapons," http://www.gwumc.edu/hspi/policy/Cilluffo_Knop.pdf); Stewart Baker, former general counsel of NSA: "As Brig Gen Billy Mitchell predicted, airpower allowed a devastating and unprecedented strike on our ships in Pearl Harbor. We responded with an outpouring of new technologies, new weapons and new strategies. Today the threat of new cyber weapons is just as real, but we have responded with an outpouring—not of technology or strategy but of law review articles, legal opinions and legal restrictions," http://www.steptoe.com/publications-8146.html; Robert Cringeley, an influential columnist in the IT trade press: "My fear is that when it comes to cyber warfare there is no Billy Mitchell today in Washington," http://www.cringely.com/2009/06/01/remember-billy-mitchell/; George Stein writing in *Air Power Journal* in 1995: "In some ways, 'info-warriors' are like Gen William ('Billy') Mitchell and the pioneer league of airmen. They see the potential. Mitchell's vision of the potential for airpower drove, at great cost to himself but great benefit to the nation, the development of a new form of warfare"; and Robert Lee writing in *Air and Space Power Journal* in 2013: "theorists and military officers, including Gen Giulio Douhet, Marshal of the Royal Air Force Hugh Trenchard, and Brig Gen William 'Billy' Mitchell, helped guide the direction of airpower. As cyberspace reaches its full potential as a domain of warfare equal to the traditional domains, we—like those leaders—must vector it properly."

[2] Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is not Falling* (Carlisle, PA: US Army War College Press, April 2013), viii, http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubid=1147.

[3] Richard Overy, *Why the Allies Won* (New York: Norton, 1997). Incidentally, his most recent book, *The Bombing War* (New York: Penguin, 2013), is far more critical of the entire air campaign.

[4] Bernard Brodie, ed., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace, and Co., 1946).

[5] Albert Wohlstetter, "The Delicate Balance of Terror," *Foreign Affairs* 37, no. 2 (January 1959): 211–34.

[6] Thomas Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960).

[7] Herman Kahn, *On Escalation* (Westport, CT: Praeger, 1965).

[8] For a good general treatment, see Robert Preston, *Space Weapons, Earth Wars* (Santa Monica, CA: RAND, 2002).

[9] This does not eliminate all sources of cyber warfare. A class of attacks known as SQL (structured query language) injection does not require malware to work, but it only works against systems that accept structured queries, which very few weapons systems do.

[10] In the short run, it is possible that an errant set of codes can break equipment, as happened to Iran's nuclear centrifuges following Stuxnet. There is considerable disagreement about whether Stuxnet can be replicated. Its revelation, incidentally, by illustrating what is theoretically possible may have made a repeat performance practically much more difficult because systems managers came to understand they expose their sensitive production and control equipment to the outside at their peril.

[11] "The cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War." Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat* (Washington: DoD, January 2013), ES-1.

[12] "The United States and China held their highest-level military talks in nearly two years on Monday, with a senior Chinese general pledging to work with the United States on cybersecurity because the consequences of a major cyberattack 'may be as serious as a nuclear bomb.'"

Jane Perlez, "U.S. and China put Focus on Cybersecurity," *New York Times*, 23 April 2013, www.nytimes.com/2013/04/23/world/asia/united-states-and-china-hold-military-talks-with-cybersecurity-a-focus.html.

13. "[Putin] warned that damage from cyberattacks could be higher than that of conventional weapons." "Putin Urges Readiness against Cyber and Outer Space Attacks," *RIA Novosti*, 5 July 2013, www.rianovosti.com/russia/20130705/182079750/Putin-Urges-Readiness-Against-Cyber-and-Outer-Space-Attacks.html.

14. "Particularly" inserted to the extent there are not fully explored stability impacts of using cyber war as the opening shot of a kinetic engagement or using any form of warfare where attribution is less than obvious.

15. In March 2013, "The chief of the military's newly created Cyber Command told Congress . . . that he is establishing 13 teams of programmers and computer experts who could carry out offensive cyberattacks on foreign nations if the United States were hit with a major attack on its own networks." Mark Mazzetti and David E. Sanger, "Security Leader Says U.S. Would Retaliate against Cyberattacks," *New York Times*, 12 March 2013, http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html. It would seem, from such comments, that these offensive teams would be oriented toward strategic rather than tactical missions.

16. That NATO actions against Gadhafi were unforeseen months before they took place was a key reason that cyber attacks were not used to take out Libyan air defenses. See Ellen Nakashima, "U.S. Cyberweapons Had Been Considered to Disrupt Gaddafi's Air Defenses," *Washington Post*, 17 October 2011, http://articles.washingtonpost.com/2011-10-17/world/35276890_1_cyberattack-air-defenses-operation-odyssey-dawn.

17. Not every exploit, however, requires a software vulnerability. Some can be penetrated and exploited by poor systems administration, notably but not exclusively, poor password management.

18. A year is roughly the time that a typical (discovered) advanced persistent threat attack lasts prior to its discovery. Mandiant, *APT 1: Exposing One of China's Cyber Espionage Units*, http://intelreport.mandiant.com/. A year is also roughly the time that a discovered vulnerability sold on the vulnerability market remains undiscovered by anyone else. Nicole Perlroth and David E. Sanger, "Nations Buying as Hackers Sell Flaws in Computer Code," *New York Times*, 14 July 2013, www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html.

19. David Sanger and Thom Shanker, "Broad Powers Seen for Obama in Cyberstrikes," *New York Times*, 3 February 2013, http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html.

Spring 2015

Busting Myths about Nuclear Deterrence

America is embarked on a quest for a world without nuclear weapons, but we live in a world not yet safe from war and threats of war. Hence, as long as nuclear weapons exist, the United States must maintain a safe, secure, and effective arsenal—both to deter potential adversaries and to assure US allies and other security partners that they can count on US security commitments. Our nuclear posture communicates to potential nuclear-armed adversaries that they cannot use nuclear threats to intimidate the United States, its allies, or partners or escalate their way out of failed conventional aggression. The United States Air Force (USAF) will continue to maintain its responsibilities as steward of two of the nation's three legs of the strategic nuclear triad and the nation's associated nuclear command, control, and communications infrastructure.

Since the Cold War, three states (India, Pakistan, and North Korea) have developed nuclear-weapon capabilities, while Iran remains on course to do so. Moreover, ongoing nuclear modernization programs in China and Russia point to the continued importance of nuclear deterrence and assurance for our allies and partners. Some countries now have military doctrines that include potential first use of nuclear weapons in a militarized crisis, and these countries regularly exercise those doctrines. These threats require the United States to seriously consider its responsibility to educate and advocate for the commitment and investment needed to sustain nuclear deterrence capabilities in a dangerous world.

The commitment must resemble Voltaire's *Candide*, dealing with the world as it is, rather than succumbing to the quest of Cervantes's *Don Quixote*, tilting fatefully at windmills. Currently, there are too many erroneous popular myths accepted uncritically by too many people about US nuclear capability. This commentary serves as a myth buster to elucidate these beliefs and confront them with the facts about America's nuclear arsenal and the purpose that arsenal serves.

Myth #1: The United States Does Not Use Nuclear Weapons

Although no nation has detonated a nuclear weapon in war since 9 August 1945, every US president since Harry Truman has used nuclear weapons to deter or compel adversaries by communicating the message that the United States is fully capable of employing nuclear weapons under circumstances determined by the National Command Authorities. US Navy ballistic missile submarines (SSBN) and USAF intercontinental ballistic missiles (ICBM) are used 24/7 to deter any nuclear-armed country with hostile intentions against the United States. Moreover, USAF nuclear-capable bombers also have been used to convey national resolve to adversaries and allies.

This was the case with Pres. Barack Obama's decision to fly B-52 and B-2 bombers over the Korean peninsula in March 2013. North Korea had just completed its third nuclear weapons test and successfully launched a space-launch vehicle that clearly showed Kim Jung Un's intent to develop ballistic missiles capable of delivering a nuclear warhead against an Asian ally and possibly US territory. When the global news media noticed a B-2 over Seoul, one international news agency did not report that the bat-winged, radar-evading aircraft had flown a regularly scheduled peacetime exercise. Instead, the outlet stated that the "United States flew two nuclear-capable stealth bombers on practice runs over South Korea . . . in a rare show of force following a series of North Korean threats that the Pentagon said have set Pyongyang on a dangerous path."[1] Chinese, North and South Korean, Russian, European, and US news outlets likewise focused almost exclusively on the nuclear capability of the bombers used in this mission.

Any nuclear-armed state contemplating aggression against the United States recognizes the overwhelming odds against its success and the jeopardy it faces for foolhardy acts. Silo-based ICBMs deployed across America's heartland, SSBNs patrolling beneath the world's oceans, and our nuclear-capable bombers are constant, tangible reminders of the price for nuclear aggression against the United States. *Myth #1 Busted—The fact is the United States uses its nuclear weapons every day.*

Myth #2: Nuclear Weapons Have Only Limited Utility for Their Cost

The USAF spends about $5 billion a year to maintain ICBMs and bombers to deter nuclear attacks against the United States, and the service is committed to a 10-year, $83.9 billion strategic modernization plan for its portion of the nation's nuclear deterrent. The Congressional Budget Office reports that the federal government will spend $355 billion over the next 10 years for all nuclear weapons investments, including those of the USAF, the Navy, the Department of Defense (DOD), and the Department of Energy.[2] These actual and projected expenditures are by no means insignificant, yet the cost of a weapon system is meaningful only in relation to the capability it provides and the broader purpose it serves. Stated differently, one must measure the merits of a weapon beyond just its monetary cost relative to the threat it confronts.

By deterring the only existential threat that can destroy the United States, nuclear weapons are a bargain. This does not diminish the warfighting capability of conventional forces, but history has shown repeatedly that conventional weapons are not an effective deterrent against major interstate war, and certainly would not be in a nuclear-armed world. In the past, civilian and military leaders often failed to anticipate the costly consequences of war. One need only consider the millions killed in the two world wars of the twentieth century to conclude that conventional forces alone do not deter national leaders determined to undertake large-scale aggression.

Yet, foreign leaders today could hardly fail to grasp the consequences of such aggression against the United States. Carl von Clausewitz observed in his classic work, *On War*, that when the potential exists for extreme violence, states should not take the first step toward war without carefully considering the last step. Because the US nuclear arsenal clarifies and sharpens nuclear-armed adversaries' thinking about war in ways other weapons cannot, those states are wary of taking the first step—because they readily grasp the image of the last step. Nuclear deterrence is thus a bargain against extreme forms of aggression. *Myth #2 Busted—Nuclear weapons are a priceless deterrent until nuclear weapons are verifiably eliminated from all countries' arsenals.*

Myth #3: Nuclear Weapons Are Going Away

Why bother spending billions of dollars to modernize US nuclear forces? Faith in the eventuality of a world devoid of nuclear weapons is the clarion call of the arms control community for radically reduced spending on nuclear weapons.[3] The hope for nuclear disarmament has inspired many US presidents, most recently President Obama, but the twenty-first century presents an incontestable reality of nuclear-armed states, most notably China and Russia.[4] The Congressional Commission on the Strategic Posture of the United States acknowledged this reality: "The conditions that might make possible the global elimination of nuclear weapons are not present today and their creation would require a fundamental transformation of the world political order."[5]

The commission observed—with specific reference to uncertainty about China and Russia—that "the U.S. nuclear posture must be designed . . . not just [for] deterrence of enemies in time of crisis and war but also assurance of our allies and dissuasion of potential adversaries. . . . The triad of strategic nuclear delivery systems should be maintained for the immediate future and this will require some difficult investment choices."[6] In 2014, nearly five years after the commission's final report was released, the commander of US Strategic Command affirmed that foreign "nuclear powers are investing in long-term and wide-ranging military modernization programs."[7] Notable among these programs are China's and Russia's growing nuclear capabilities.

China's once modest nuclear force is rapidly evolving in size and in quality. "Over the next three to five years, China's nuclear program will become more lethal and survivable with the fielding of additional road-mobile nuclear missiles; five nuclear-powered ballistic missile submarines, each carrying 12 sea-launched intercontinental-range ballistic missiles; and ICBMs armed with multiple independently targetable re-entry vehicles."[8] In late 2014 Beijing tested its first ICBM capable of carrying up to 10 warheads, a development that has been characterized as "a significant advance for China's strategic nuclear forces and part of a build-up that is likely to affect the strategic balance of forces."[9] Even the less-favored air-breathing leg of China's nuclear arsenal will benefit from the addition of the new H-6K bomber, which is equipped with long-range, nuclear-capable Changjian-10 cruise missiles, effectively increasing the aircraft's combat radius to reach Okinawa, Guam, and Hawaii from the mainland.[10] Russia also continues a robust nuclear modernization program that includes silo-based and mobile versions of the RS-24 and mobile RS-26 ICBMs, both carrying multiple independently targetable reentry vehicles; deployment of up to eight new Borei-class SSBNs, fitted with 16 launch tubes for new Bulava ICBMs (each carrying up to 10 independently targetable warheads); and development of a new long-range bomber to be outfitted with hypersonic missiles.[11] Given the reality of nuclear-armed states and nuclear-weapon aspirants, the United States must make the difficult choices to sustain our nuclear deterrent. *Myth #3 Busted—Nuclear weapons are not going away; rather nuclear states are modernizing their arsenals, while other states seek these weapons.*

Myth #4: The United States Can Deter with Submarines Alone

This myth is predicated primarily on the notion SSBN survivability is "easier to achieve" relative to fixed-site ICBMs and long-range bombers that may be vulnerable on the ground and in the air.[12] However, there are two risks with the submarine-only deterrent myth. First, while some argue the stealth of SSBNs ensures their survival for second-strike missions, the current US chief of naval operations has noted the limits of stealth-based platforms. Adm Jonathan W. Greenert has observed that the "rapid expansion of computing power also ushers in new sensors and methods that will make stealth and its advantages increasingly difficult to maintain above and below the water."[13] While adversaries probably could not achieve antisubmarine warfare (ASW) breakthroughs in the near term to threaten SSBNs, by divesting itself of the deterrent triad for a SSBN-based monad, the United States would necessarily create a high payoff incentive for adversaries to seek ASW capabilities to neutralize US ballistic missile submarines. Rather than saving defense resources by scrapping ICBM and bomber forces, a new and potentially destabilizing arms race could occur as each side postures and repostures below the world's oceans.

The second risk of a submarine-only nuclear force is that the United States would have no way to demonstrate intent to nuclear-armed regional adversaries or to allies who rely on US extended deterrence to preserve peace. Locational uncertainty is necessary for SSBNs to preserve their second-strike capability; thus, submariners are highly averse to revealing their position. This vulnerability surrenders their primary method for survivability.[14] However, being visible is exactly what is needed to demonstrate resolve—thus, the reason nuclear-capable bombers are so important. Ballistic missile submarines simply could not do what the B-2 bombers did over Korea in 2013. As the Commission on the Strategic Posture of the United States observed, "each leg of the triad has its own value."[15] The commission further pointed out that the unique and synergistic characteristics of the triad will remain "valuable as the number of operationally deployed strategic nuclear weapons" declines.[16] *Myth #4 Busted—The United States cannot safely deter nuclear aggression with an SSBN-based monad alone.*

Myth #5: The USAF Is Stuck in a Cold War Mind-Set

Although the United States took an intellectual holiday from thinking about nuclear deterrence following the Cold War, the USAF has undertaken a fundamental transformation of its approach to thinking about nuclear weapons in the twenty-first century.[17] Secretary of the Air Force Deborah James has noted the diminished understanding of deterrence across the nuclear enterprise and within the USAF, even among senior leaders, and she has made a forceful call for USAF professionals to reestablish their intellectual leadership on deterrence. In addition to dozens of immediate actions under its Force Improvement Programs, the USAF is undertaking longer-range reform of its doctrine, professional military education (PME) for all Airmen, and continuing education of its nuclear professionals.

Established by the Nuclear Oversight Board, a governing body of USAF senior executives chaired by the secretary and chief of staff, the Air Force Nuclear Enterprise Flight Plan guides these initiatives. This publicly available document articulates the USAF's foundational understanding of the nature of deterrence and the role of Airmen in providing the nation with nuclear deterrence capabilities.[18]

The USAF Chief of Staff, Gen Mark Welsh, has instituted a quarterly deterrence seminar for Air Staff principals. He leads this tabletop exercise, employing staff and outside expertise to consider various plausible near-future scenarios and debating contending solutions. USAF senior executives take this seriously, and their debates are frank, open, and sometimes contentious.

The curriculum of all USAF PME institutions is under vigorous review; new content and courses on twenty-first century nuclear deterrence are being introduced at every level. The Air Force Academy will soon offer several new courses supporting a new nuclear weapons and strategy minor for undergraduates. For all general officers and senior executives (even the chief of chaplains) there is now a senior leader course, "Nuclear 400," that engages participants in problem-solving case studies of real-world deterrence operations and nuclear enterprise management challenges. Nuclear professionals are required to complete weeklong continuing education courses to refresh and renew their expertise.

The Air Force LeMay Doctrine Center is bringing together nuclear deterrence professionals from all across the USAF to make a fundamental transformation of the nuclear deterrence operations annex to Air Force doctrine and to revise the treatment of deterrence across all elements of Air Force basic doctrine. In November 2014 the Air Force Studies Board of the National Academies concluded a two-year effort to develop a comprehensive plan for developing new methods, approaches, and tools for analyzing twenty-first century deterrence.[19] General Welsh directed the board's recommendations be implemented to enable USAF senior leaders to exert renewed intellectual leadership on deterrence.

America's Airmen know deterrence and are ready to articulate twenty-first century deterrence capabilities. The USAF has undertaken several activities and initiatives to reverse the lack of attention and interest that beset much of the DOD after the Cold War.[20] Moreover, the USAF will sustain its commitment and effort to deter extant and emerging nuclear threats in a post–Cold War world. *Myth #5 Busted—The USAF is not stuck in a Cold War mind-set—far from it.*

Conclusion

Although the United States is committed to the goal of a nuclear-weapon-free world, as long as nuclear weapons exist in foreign arsenals, there is simply no alternative path for the United States than to maintain safe, secure, and effective nuclear capabilities. As a visible signal of our intent to act if circumstances warrant, the US bomber force remains crucial for extended deterrence of threats against allies and other partners during times of crisis. ICBMs, widely dispersed around three Air Force bases, are key for deterrence of attack against the United States, because for the foreseeable future no aggressor has any prospect of disarming our land-based missile force. Ballistic missile submarines patrol securely beneath the world's oceans, ensuring a secure second-strike capability even under the direst circumstances. With the commitment of resources, the unique attributes of each leg of the triad will continue to complicate adversaries' offensive and defensive planning and contribute to America's security.

Nuclear weapons played an essential role in preventing superpower war during the Cold War. Although the potential for major state-on-state war today may be lower, it is not absent and may indeed grow; therefore, USAF nuclear capabilities, as part of the US nuclear arsenal, continue to provide essential contributions to preserve the peace. Difficult decisions lay ahead, as the United States thinks about nuclear forces and nuclear deterrence. However, focusing on facts and applying sound reasoning can make the choices clearer. SSQ

James A. Blackwell Jr.
Special Advisor to the Assistant Chief of Staff
Strategic Deterrence and Nuclear Integration
Headquarters, US Air Force

Charles E. Costanzo
Associate Professor of National Security Studies
Air Command and Staff College
Maxwell AFB, AL

Notes

[1] David Chance, "U.S. Flies Stealth Bombers over South Korea in Warning to North," *Reuters*, 28 March 2013, http://www.reuters.com/article/2013/03/28/us-korea-north-stealth-idUSBRE92R0DX20130328.

2. Congressional Budget Office (CBO), *Projected Costs of U.S. Nuclear Forces, 2014 to 2023* (Washington, DC: CBO, December 2013), 2, http://www.cbo.gov/sites/default/files/cbofiles/attachments/12-19-2013-NuclearForces.pdf.

3. *See* Tom Z. Collina and the Arms Control Association Research Staff, *The Unaffordable Arsenal: Reducing the Costs of the Bloated U.S. Nuclear Stockpile* (Washington, DC: Arms Control Association, October 2014), http://www.armscontrol.org/files/The-Unaffordable-Arsenal-2014.pdf.

4. *See* Pres. Barack Obama's speech in Prague, Czech Republic, April 2009, http://www.whitehouse.gov/the_press_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered.

5. William J. Perry, James R. Schlesinger, et al, *America's Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States* (Washington, DC: US Institute of Peace Press, 2009), xvi, http://media.usip.org/reports/strat_posture_report.pdf.

6. Ibid., xvii.

7. Amaani Lyle, "Stratcom Commander Outlines Deterrence Strategy," *American Forces Press Service*, 28 February 2014, http://www.defense.gov/news/newsarticle.aspx?id=121751.

8. Wendell Minnick, "US Report: China's Nukes Getting Bigger and Better," *Defense News*, 19 November 2014, http://www.defensenews.com/article/20141119/DEFREG03/311190050/US-Report-China-s-Nukes-Getting-Bigger-Better.

9. Bill Gertz, "China Tests ICBM with Multiple Warheads," *Washington Free Beacon*, 18 December 2014, http://freebeacon.com/national-security/china-tests-icbm-with-multiple-warheads.

10. Kyle Mizokami, "The Dragon's Fire: Welcome to Chinese Nuclear Weapons 101," *National Interest*, 5 January 2015, http://nationalinterest.org/blog/the-buzz/the-dragon%E2%80%99s-fire-welcome-chinese-nuclear-weapons-101-11968.

11. Nuclear Threat Initiative, "Russia Test-Launches Two Strategic Missiles," *Global Security Newswire*, 2 January 2014, http://www.nti.org/gsn/article/russia-test-launches-two-strategic-missiles; and Tamir Eshel, "A Missile Testing Blitz Revamps Russian ICBM Modernization," *Defense Update*, 29 November 2014, http://defense-update.com/20141129_russian_icbm_blitz.html.

12. Benjamin H. Friedman and Christopher A. Preble, "Ending Nuclear Overkill," *New York Times*, 13 November 2013, http://www.nytimes.com/2013/11/14/opinion/ending-nuclear-overkill.html; and Christopher Preble and Matt Fay, "To Save the Submarines, Eliminate ICBMs and Bombers," *Defense One*, 14 October 2013, http://www.defenseone.com/ideas/2013/10/save-submarines-eliminate-icmbs-and-bombers/71879/.

13. Jonathan W. Greenert, "Payloads over Platforms: Charting a New Course," *U.S. Naval Institute Proceedings* 138, no. 7 (July 2012): http://www.usni.org/magazines/proceedings/2012-07/payloads-over-platforms-charting-new-course.

14. Naval Doctrine Publication 1, *Naval Warfare*, March 2010, 27, https://www.usnwc.edu/Academics/Maritime--Staff-Operators-Course/documents/NDP-1-Naval-Warfare-%28Mar-2010%29_Chapters2-3.aspx.

15. Perry and Schlesinger, *America's Strategic Posture*, 25.

16. Ibid., 26.

17. *See* the remarks of Maj Gen Garrett Harencak, assistant chief of staff for strategic deterrence and nuclear integration at the US Strategic Command Deterrence Symposium in August 2014. US Strategic Command, "Panel 6 - 2014 Deterrence Symposium," *YouTube*, 19 August 2014, http://www.youtube.com/watch?v=PFMtS4MhKyc&list=PLzO_KvP4phUYPNAqhWK_cDE73i7FteVQ5&index=10.

18. Eric K. Fanning and Mark A. Welsh III, *Flight Plan for the Air Force Nuclear Enterprise* (Washington, DC: Department of the Air Force, 26 June 2013), http://www.af.mil/Portals/1/documents/news/FlightPlanfortheAirForceNuclearEnterprise.pdf.

19. Committee on USAF Strategic Deterrence Military Capabilities in the 21st Century Security Environment, Air Force Studies Board, Division on Engineering and Physical Sciences; and the National Research Council, *U.S. Air Force Strategic Deterrence Analytic Capabilities: An Assessment of Tools, Methods, and Approaches for the 21st Century Security Environment* (Washington, DC: The National Academies Press, 2014), http://www.nap.edu/catalog/18622/us-air-force-strategic-deterrence-analytic-capabilities-an-assessment-of.

20. Secretary of Defense Task Force on DOD Nuclear Weapons Management, *Report of the Secretary of Defense Task Force on DOD Nuclear Weapons Management, Phase II: Review of the DOD Nuclear Mission* (Washington, DC: DOD, December 2008), http://www.defense.gov/pubs/pdfs/PhaseIIReportFinal.pdf.

Mission Statement

Strategic Studies Quarterly (*SSQ*) is the strategic journal of the United States Air Force, fostering intellectual enrichment for national and international security professionals. *SSQ* provides a forum for critically examining, informing, and debating national and international security matters. Contributions to *SSQ* will explore strategic issues of current and continuing interest to the US Air Force, the larger defense community, and our international partners.

Disclaimer

The views and opinions expressed or implied in *SSQ* are those of the authors and should not be construed as carrying the official sanction of the US Air Force, the Department of Defense, Air Education and Training Command, Air University, or other agencies or departments of the US government.

Comments

We encourage you to e-mail your comments, suggestions, or address change to: **StrategicStudiesQuarterly@us.af.mil**.

Article Submission

The *SSQ* considers scholarly articles between 5,000 and 15,000 words from US and international authors. Please send your submission in Microsoft Word format via e-mail to:

StrategicStudiesQuarterly@us.af.mil

— — — — — — — — — — — — — — — —

Strategic Studies Quarterly (SSQ)
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112–6026
Tel (334) 953–7311
Fax (334) 953–1451

View *Strategic Studies Quarterly* online at **http://www.au.af.mil/au/ssq/**

Free Electronic Subscription

Like Air University Press on Facebook at https://www.facebook.com/AirUnivPress
and follow us on Twitter at https://www.twitter.com/AirUnivPress

A forum for critically examining, informing, and debating national and international security.

"AIM HIGH… FLY-FIGHT-WIN"

http://www.au.af.mil/au/ssq/

AIR UNIVERSITY