Asymmetric Strategies as Strategies of the Strong

Michael Breen and Joshua A. Geltzer

One needs merely to wade into the shallow waters of today's deepest debates over American foreign policy to stub one's toe against the notion of asymmetric strategies. Like the very strategies that it describes, the concept often seems frustratingly amorphous yet disturbingly omnipresent—and, most importantly, distinctly threatening to the United States.[1]

This article takes the notion of asymmetric strategy seriously but re-conceptualizes it in a crucial way. The article questions the persistent identification of asymmetric strategies as strategies of the weak, instead revealing the many ways in which asymmetric strategies are becoming strategies of the increasingly strong. Consequently, the article also rejects the notion that asymmetric strategies can be deployed only against the United States, and aims to stimulate thinking about ways in which asymmetric strategies might be adopted for use *by* the United States. In the end, the article concludes that the American foreign policy community should cease thinking of asymmetric strategies as the exclusive province of weak nonstate actors and, instead, should conceive of such strategies as even more important when intelligently wielded by strong state actors—including America itself.

The first part of the article isolates a definition of asymmetric strategy that, unlike many definitions proposed previously, defines such strategies independently of the actors that execute them: asymmetric strategies transform an adversary's perceived strength into a vulnerability, often by revealing one's own perceived vulnerability as a strength. The article's second part employs that definition to reveal the ways in which asymmetric strategies are already being adopted by America's adversaries, including states. The final portion of the article calls for new thinking about ways in which the United States might employ asymmetric strategies against its various adversaries.

Michael Breen is Vice President of the Truman National Security Project, a former Army combat arms officer, a member of Yale Law School's Class of 2011 and a graduate of Dartmouth College.

Joshua A. Geltzer, also a member of Yale Law School's Class of 2011, received his Ph.D. in War Studies from King's College London, where he studied on a Marshall Scholarship. Geltzer is the editor-in-chief of the Yale Law Journal.

The Concept of Asymmetric Strategies

Defining Asymmetric Strategies

Asymmetric strategy has been a crucial concept in the decade following 9/11, yet it remains devilishly difficult to define.[2] Numerous attempts to define the concept are so broad that they approach the definition of strategy itself, severely limiting any practical utility.[3] For example, one foundational article on asymmetric strategy claims that "strategic asymmetry is the use of some sort of difference to gain an advantage over an adversary."[4] If this formulation is correct, it is unclear how asymmetric strategies differ from other strategies: "Emphasizing one's strengths and exploiting an enemy's weakness is what strategy is all about."[5]

Other commonly used definitions are narrower, but conflate large differences in the relative strength of the parties to a conflict and the strategies that those parties employ. In other words, these definitions seem to suggest that asymmetric strategy is almost anything that a weak actor might do when faced with a much stronger opponent, especially if that action is somehow surprising or creative: "Asymmetric warfare is violent action undertaken by the 'have-nots' against the 'haves' whereby the have-nots, be they state or sub-state actors, seek to generate profound effects . . . by employing their own specific relative advantages against the vulnerabilities of much stronger opponents."[6] Granted, the phenomenon being described here is of central concern to America in its status as the world's lone superpower. The problem is that virtually any entity that the United States may fight, state or nonstate, will be less powerful than America. If asymmetric strategy is simply what weaker actors do against stronger ones, then from America's perspective asymmetric strategies are just good strategies against the United States: "Any military plan that avoids meeting the United States in a head-on, force-on-force, 'fair' battlefield fight is also considered to be 'asymmetric.'"[7]

We acknowledge that previous definitions of asymmetric strategy have been useful in describing the post-Cold War world of weaker but unruly adversaries confronting the United States. That said, we believe that strategists, soldiers, and scholars alike would benefit from a more precise definition—one that identifies asymmetric strategy as a conceptual category unto itself, independent of the weakness or strength of the actor wielding it.

Asymmetric strategies are roughly akin to the Japanese martial art of jujutsu, which is based on the idea that an opponent's strength and energy may be used against him rather than directly opposed with strength of one's own. When facing a taller or stronger opponent, for example, a jujutsu practitioner is encouraged to view the opponent's advantages in height and muscle mass as exploitable weaknesses, as they tend to produce a high center of gravity. Similarly, jujutsu practitioners use the very force that an opponent is able to put behind a punch in order to throw him to the ground, rather than blocking the blow and attempting to respond in kind.

Such an approach offers several advantages in hand-to-hand combat—regardless of the relative strength of the two opponents. This approach helps seize the initiative, as one's opponent has the unsettling experience of having his own intentioned action and inherent power used against him. The strength of the jujutsu practitioner is greatly conserved, as it is largely the energy of the opponent that produces his downfall rather than any external force. Most importantly, jujutsu is fiendishly difficult to counter: how do you fight back against an opponent who consistently turns your own strength against you?

When properly defined and understood, asymmetric strategy is quite similar. In light of this understanding, we offer a definition of the concept: asymmetric strategies transform an adversary's perceived strength into a vulnerability, often by revealing one's own perceived vulnerability as a strength. Asymmetric strategy is an inherently relational art form—one that often exploits an opponent's mistaken perceptions about both the asymmetric actor and himself.[8] More importantly, it is available to any strategic actor, weak or strong. Sufficient skill and cunning are the only attributes that asymmetric strategy demands.

Asymmetric Strategies, More than Weapons of the Weak

Asymmetric strategies are typically conceptualized as weapons of the weak. Rod Thornton, for example, defines "the 'asymmetric adversary'" as "the smaller, weaker protagonist."[9] Thornton's voice is not alone in this regard: while asymmetric strategies have received attention since at least 1995,[10] interest in the concept has quite clearly surged since the attacks of 11 September 2001 and focused American attention on adversaries whose limited capabilities make them appear weak, at least in a traditional sense.

It is not the inherent weakness of nonstate adversaries that qualifies them as asymmetric actors. Consider Thornton's description of the "three major characteristics of the 'new' terrorists that need to be considered: their increased degree of fervor, their increased ability to implement attacks, and their increased ability to cause mass casualties."[11] Not one of these is inherently an attribute of the weak. At any given moment in the Cold War, much of what America feared about its very strong adversary, the Soviet Union, was its increased fervor, its improved capacity to attack, and its enhanced ability to cause mass destruction.

Another set of authors exploring asymmetric strategies identifies what really seems novel about "global terrorist groups" and the threat that they pose to the United States: it is the fact that "America's global economy, relatively porous borders, open source intelligence and information, and inadequate law enforcement resources allow access to a range of goods, services, and information that together can be developed into formidable weapons."[12] It is, in other words, not any characteristic of al Qaeda itself that made its attack on 9/11 a paradigmatic use of an asymmetric strategy. Rather, it is the inescapably relational manner in which the group transformed attributes of the United

States normally viewed as strengths—for example, the country's interconnected economy, open borders, and free flow of information—into devastating vulnerabilities. Al Qaeda accomplished this by making clever use of aspects of its own identity that the United States viewed as vulnerabilities, such as its small numbers, crude weapons, and limited training.

A weak nonstate actor may have greater incentive to adopt such strategies in order to overcome a lack of options, but there is no reason that a strong state actor could not do the same.[13] In the influential book *Unrestricted Warfare*, two Chinese People's Liberation Army colonels argue that strategies currently identified with terrorist groups can and should be adapted for use by states such as China: "the new and old terrorists who consistently uphold the principle of resorting to every conceivable means are still the best teachers of each nation's government."[14] Indeed, as the next part of this article will demonstrate, increasingly strong states are already using asymmetric strategies typically associated with nonstate actors. Hence, the current tendency to identify asymmetric strategies with weak, nonstate actors emerges from mere historical happenstance and conceptual confusion, rather than from anything inherent in the concept itself.[15]

While commentators focus on asymmetric strategies as the province of the weak, increasingly strong actors have begun deploying and employing these strategies, often to impressive effect. The next section examines how strong states such as China and Russia, or robust nonstate entities such as Hezbollah, have attempted to transform their adversary's perceived strengths into vulnerabilities by drawing on latent strengths of their own.

What "They" Are Doing to Us

Despite the prevailing focus on the asymmetric threats that nonstate actors pose to the United States and its allies, increasingly strong states are also developing and employing strategies that seek to exploit apparent American strengths as latent vulnerabilities. This should not come as a surprise. Motivated perhaps by Thucydides' explanatory triad of "fear, honor and interest," rising powers such as China, Russia, and Iran feel the need to develop the capability to neutralize or at least mitigate American power.[16] Given the position of economic and military dominance that America currently enjoys, states which may seek to coerce or deter the United States have an incentive to be creative. The rapid destruction of Iraq's Soviet-inspired conventional military twice in little more than a decade conveys a clear lesson to would-be state challengers: "Don't fight the United States unless you have nuclear weapons."[17]

Even as they build more conventional capabilities, therefore, some states have chosen to develop strategies designed to exploit apparent American strengths as actual vulnerabilities. As is often the case, point of view is essential. For example, the networked, software-based wizardry that permits the United States to coordinate with astounding precision various air campaigns undertaken around the world from geographically remote command centers is undoubtedly a major American strength. In the eyes of an asymmetric adversary, however, the same capability may be viewed as a dangerous dependency

that leaves America's lavishly expensive military vulnerable to comparatively cheap cyberattacks. The relative strength of America's adversary in such a formulation is immaterial—the strategy is asymmetric regardless of whether it is employed by a small group of hackers, a weak regional challenger, or a mighty global adversary.

It is no surprise, then, that a diverse array of states has began pursuing asymmetric strategies against the United States. As they do so, a kind of parallel evolution is occurring. Over the past two decades, several increasingly strong actors have developed broadly similar asymmetric strategies. We outline several below to illustrate the central claim—that asymmetric strategies, properly understood, are already being employed by increasingly strong actors, including states, and not just by weak nonstate actors.

Hybrid Warfare

Insurgency is perhaps the iconic asymmetric strategy and has proven highly effective at inverting the strengths of even the world's most powerful militaries. States have long used insurgency by proxy as a means to harass an adversary; such tactics were common during the Cold War and currently are employed in a number of locations. As a strategy to be utilized directly by a state in a military confrontation with another, insurgency is typically far less attractive. An emerging but still quite nascent cocktail of tactics, techniques, and technologies is combining some of insurgency's key asymmetric advantages with more conventional approaches to holding and controlling territory. Often referred to as "hybrid warfare," this evolving approach to ground combat may soon present states with a viable asymmetric option against the United States.[18]

Insurgency undoubtedly presents a serious asymmetric challenge to even strong conventional military powers such as the United States. The strategy is asymmetric, according to our definition, in that it seeks to transform military advantages in mass and firepower into disadvantages by exhausting the foe in a protracted campaign while goading or misleading him into misdirecting force against the civilian population. Conventional military forces tend to orient on seizing and holding key terrain, and to focus their destructive energies on the dispatch of the opposing military force; meanwhile, insurgents orient on the population and their conventional opponents, routinely yield key terrain, and tend to focus their efforts on symbolic acts of violence that shift the balance of political power in their favor. In most formulations, the insurgency then capitalizes on favorable shifts in the political balance to alter the balance of military power to its advantage. If it is unable to accomplish such a shift, the insurgency simply continues to survive while draining its opponent's will to fight, until the bloodied and dispirited conventional military withdraws from the conflict.[19]

For a nonstate actor waging a campaign against a government, foreign or domestic, insurgency has proven an effective tool over the last hundred years. As an asymmetric strategy to be used by one state against another, however,

it has serious limits. While insurgency is often a politically offensive strategy in that it frequently seeks to replace an existing government with another, it is largely defensive in geographic terms.[20] Mao Zedong, the doctrinal father of modern insurgency, famously conceived of insurgents as fish swimming in the sea of a friendly population. Clearly, this approach requires the insurgent to have a claim to membership in the population in which he swims, or at least a powerful claim on that population's loyalty.[21]

Even as a defensive strategy, insurgency is a matter of last resort for governments because it requires a government to allow a hostile force to invade and occupy its territory before the insurgency can even begin. Mao described his plans for insurgency against the onrushing Japanese army in just such terms: "The invader's strategy must be one of lightning war. If we can hold out for three or more years, it will be most difficult for them to bear up under the strain."[22] For most national leaders, taking to the hills and back alleys for three or more years while a foreign military runs rampant is a decidedly unattractive defensive option, even when confronted with extremely poor odds of success in a more conventional campaign to defend territory. Even if the enemy is ultimately defeated, the host country is likely to be devastated, and the pre-war political system is unlikely to survive. For a state, then, insurgency is unattractive because a cornerstone of the strategy itself is refusal to fight for its territorial integrity.

Hybrid warfare promises to partially rectify that flaw while retaining many of insurgency's asymmetric advantages. In theory, hybrid warfare combines insurgency's highly decentralized cell-based communications and leadership structures, light logistical footprint, and synergy with the civilian population with tactics intended to hold terrain and destroy, rather than just harass, the opposing force. Like insurgency, hybrid warfare is often based on a light infantry model that largely eschews big, conspicuous weapons platforms such as tanks and large-caliber artillery.[23] Instead, hybrid forces employ man-portable anti-tank missiles, rockets, and mortars. The proliferation of accurate and inexpensive precision-guided munitions continues to make such weapons increasingly potent against conventional armored formations, to the point that a decentralized but well-equipped infantry force capable of fading into the civilian population is also increasingly capable of standing its ground when attacked. Such a force presents few of the defensive weaknesses that tend to characterize conventional forces. For example, while the American military would typically target and destroy a conventional enemy's communications and logistical infrastructure prior to beginning an attack, such infrastructure is difficult to identify and indistinguishable from civilian systems if the opponent is a decentralized hybrid force relying on close ties within the civilian population.

While hybrid warfare remains an emerging threat, some defense analysts believe that Israel's experience against Hezbollah in Southern Lebanon in 2006 may reveal the shape of things to come. The conflict is of special note because the Israeli Defense Forces (IDF), largely equipped with American military technology and using American-style tactics, struggled to overcome the

forces of an irregular adversary in Israel's campaign to seize and hold ground.[24] Hezbollah is itself something of a hybrid in that it is a nonstate actor with roots as a terrorist and insurgent organization that also controls territory and fulfills many traditional state functions. During its 24-year history leading up to the 2006 confrontation with the IDF, Hezbollah appears to have developed an equally hybrid approach to fighting its highly trained, lavishly equipped conventional adversary. On the one hand, Hezbollah continues to emphasize a decentralized and autonomous insurgent-style cell-based organizational structure with virtually no logistical "tail" and frequently makes use of hit-and-run insurgent tactics designed for political provocation rather than military affect.[25] At the same time, however, Hezbollah forces defended southern Lebanon in 2006 using an intricate series of prepared and concealed bunker positions designed and provisioned to sustain a lengthy defense, and employed a range of sophisticated guided weapon systems against Israeli targets on land and even at sea.[26] Unlike traditional insurgents, Hezbollah fighters in 2006 consistently strove to hold ground against a determined attack by Israeli armored formations, sometimes with success.[27]

During Israel's 33-day ground incursion, Hezbollah's hybrid of conventional and unconventional warfare allowed it to inflict more Israeli casualties per Arab fighter than did any of Israel's conventional opponents in the 1956, 1967, 1973, or 1982 Arab-Israeli wars.[28] Given the similarities between the Israeli and American ways of war, this did not go unnoticed by potential adversaries of the United States. Iran, in particular, may have used the 2006 conflict as a test for strategies designed to defend against possible American invasion, and directly supplied much of Hezbollah's arsenal. As one observer put it, "Hezbollah trains Iran, not the other way around."[29] Russia originally developed and manufactured the vast majority of Hezbollah's high-end weapon systems, and Russian military planners no doubt paid close attention to their employment and effectiveness.[30] China, meanwhile, is developing its own strategy for denying the western Pacific to American forces, in part by making extensive use of guided missiles deployed in a decentralized manner—an approach that it refers to as "Assassin's Mace."[31] American observers have been quick to recognize the threat posed by such tactics.[32]

Hybrid warfare potentially allows states to enjoy some of insurgency's advantages while avoiding important costs, especially the surrender of key terrain. Such a strategy presents an asymmetric advantage in that it allows an adversary to transform an opponent's advantage in expensive, high-tech weapons platforms into a vulnerability, while at the same time converting apparent weaknesses in arms and numbers into strengths. In the aftermath of America's entrance into Afghanistan and then Iraq, states seeking to defend their borders against possible American invasion, such as Iran and North Korea, have looked to nuclear weapons as their primary defensive option. In the near future, however, hybrid warfare may allow such adversaries to mount a more credible conventional defense against the American way of war.

Cyberwarfare

In recent years, cyberwarfare has emerged as a serious challenge to the world's most technologically sophisticated nations, including the United States. The decentralized and byzantine structure of the internet itself intensifies this threat, in that it is increasingly possible for state and nonstate actors alike to develop and employ cyberwarfare capabilities anonymously or through potentially oblivious proxies, making deterrence a difficult proposition. Given the potential to level the playing field by disrupting or disabling a more technologically advanced adversary's capabilities and perhaps even to do so with plausible deniability, it is small wonder that states large and small have increasingly devoted resources to developing a capacity for cyberwarfare.

The list of nations actively pursuing cyberwarfare capabilities is extensive and includes a number of America's potential challengers. China has developed official military doctrine for cyberwarfare, trained large numbers of military officers to conduct offensive operations on the internet, and conducted an extensive series of exercises and simulations.[33] Russia has developed a robust cyberwarfare capability, partially in consultation with China.[34] Russia also has demonstrated an enthusiasm for offensive cyberwarfare over the past decade, conducting cyberattacks against Chechen sites as early as 2002.[35] Using criminal gangs as proxies, Russia used cyberattacks to cripple Georgian networks prior to Russia's conventional military attack in 2008, having seen the utility of such tactics in an earlier confrontation with Estonia.[36] In both of these instances, it was the stronger actor, Russia, that adopted an asymmetric strategy. Iran, India, Pakistan, and North Korea are also known to be developing cyberwarfare capabilities of varying sophistication and effectiveness, sometimes in coordination with criminal organizations.[37]

As several observers have noted, cyberspace is best understood not as an unprecedented forum for entirely new tactics but instead as a new venue where conflict will occur in forms roughly analogous to those seen on land, at sea, in the air, and in orbital space.[38] In this new and evolving venue, just as in more traditional ones, we will see any number of strategies develop that mix and match direct and indirect approaches, as well as outright coercion and deception. Many cyberwarfare strategies appear intrinsically asymmetric, in that the more highly developed and powerful a nation's computerized infrastructure becomes, the more vulnerable the target nation is to the consequences of a successful cyberattack. However, recall that exploiting misperception is a central feature of an asymmetric strategy. As cyberwarfare becomes a common feature of the global strategic environment, states that rely upon sophisticated computer networks will be all too aware of their vulnerability. In the near future, one can anticipate that computer networks will be viewed in the same light as aircraft carriers are today—powerful but vulnerable technological tools that must be zealously protected against attack.

As in other venues of human conflict, some small subset of cyberspace strategies will be truly asymmetric. It is probably too early in the history of

cyberwarfare to make definitive statements about which strategies will be employed, how they will evolve, and what asymmetric warfare in cyberspace will look like. We can, however, draw some very broad but useful distinctions.

Imagine an adversary that has developed a sizeable cyberwarfare capability, employing large numbers of military and intelligence personnel and computers, and utilizes this capability to launch a large-scale denial of service attack on US military computer networks. Assume that the cyberattack is intended to cripple our command-and-control capabilities during an air and naval campaign that spans vast distances, allowing the adversary's otherwise outmatched forces to mount a more credible defense. Although the attack would invert an American strength and render it a weakness in the broader sense, the means of attack is the rough cyberspace equivalent of an armored thrust penetrating an enemy line on land—concentrated power applied against a carefully chosen weak point. Such an attack may achieve surprise and shock effect, but it is not asymmetric.

Contrast this type of attack with another hypothetical attack on American networks, conducted in order to achieve similar objectives. In this case, however, imagine the attack is carried out using a network of civilian, government, and military computers from around the world. In most cases the owners are probably unaware that the attack is even taking place—imagine this clandestine network is created and controlled by a group of individuals deniably employed by the attacking state. In this scenario, four or five people could strike a serious blow against the most powerful military in the world. Their perceived weaknesses are many; they are unarmed, they are few in number, and they have relatively few resources. Yet, those perceived weaknesses provide the attacker with the anonymity and deniability required to survive and execute their attacks. The effectiveness of this cyberattack emerges from its capacity to transform an apparent American strength—the technologically advanced, elaborately synchronized American military—into a weakness.

The potential for an attack along these lines is illustrated by the saga of the now-infamous Conficker worm.[39] Like other worms, Conficker is designed to embed itself in a host computer without revealing its presence, making small changes necessary to defend itself and avoid detection, and then spreading to other systems. It also maintains regular communication with its unknown creator over the internet, and is capable of responding to instructions. The worm first appeared on November 20, 2008, and since then has successfully survived an unprecedented attempt to destroy it by a globally coordinated network of security experts. Today, the worm controls a botnet—or network of infected computers—likely consisting of millions of computers worldwide, mostly operated by entirely unsuspecting users. Such a botnet provides the worm and its controller with tremendous computing power, which could potentially be used to conduct debilitating attacks on even the largest and most secure networks in the world. For any organization, including a state, a stable botnet like the one that Conficker controls represents a powerful on-call offensive capability.

Conficker's design and subsequent adaptations indicate that it was designed by a team of individuals possessing truly world-class expertise in a number of disciplines, including cryptography and software design. According to cybersecurity experts who have studied the worm, Conficker's creators are "either incredibly sophisticated cyber criminals or a group that was funded by a nation-state."[40] Conficker's creators remain anonymous, and it is not known whether the worm is controlled by a state. It may be significant, however, that the original version of Conficker was designed to avoid infecting any computer with a Ukrainian IP address.[41]

The combination of offensive potential and deniability offered by a capability like Conficker's anonymously controlled botnet is simply too attractive for a state actor to ignore. Such capabilities represent some of the most dangerous and significant emerging threats to the United States and its allies, and are by no means exclusively weapons of the weak. Especially in combination with hybrid warfare and other asymmetric strategies discussed here, cyberwarfare may offer America's future adversaries a potentially transformational advantage. In the hands of a strong state actor with access to large amounts of intellectual capital and technical expertise, asymmetric cyberwarfare could prove devastating.

Media Manipulation

Americans often view their country's robust media as a strategic asset, and even adversaries have come to see the American media as strategically beneficial to the United States. During the Cold War, for example, the Soviet Union took great pains to restrict its citizens' access to Western media, while the United States attempted to defeat Soviet censorship. The reverse, however, was not the case—Soviet media was utterly ineffective at influencing American audiences, and the United States made no serious attempt to censor it. Broadly similar dynamics persist today between the United States and several of its rivals, with the censorship of American media ranging from the extreme in the case of North Korea to more subtle measures in the case of China.

Some adversaries, however, have recognized that the American media may also be an American weakness under certain conditions. American media outlets pervade the globe, beaming an American viewpoint into households around the world; however, that same global scope and ambition on the part of US-based news outlets permit a foreign perspective on American foreign policy to reach American audiences. More importantly, American media coverage provides the American people with an often limited but highly visceral view of the immediate day-by-day impact of US policies, many of which require a long-term popular commitment to succeed.

This effect is particularly problematic for American leaders when the United States is engaged in armed conflict with a weaker opponent, a situation that America's superpower status makes extremely likely. The problem is that a pronounced imbalance in strength produces serious moral and ethical issues for

the stronger belligerent, whose strength, self-confidence, and will to fight are continuously eroded. Martin Van Creveld memorably compares this "paradox of strength" dynamic to a grown man confronting a small child who is attacking him with a knife—virtually anything that the adult might do will appear to be either weakness or atrocity to an observer.[42] When the American people observe their own military in such situations, they tend to react negatively.

Often, this dynamic is less a strategy employed by America's adversaries than a simple fact of life. For example, reactions to graphic media coverage of devastating coalition air strikes against retreating Iraqi troops in 1991 significantly contributed to a cease-fire that permitted much of Iraq's Republican Guard to escape. As beneficial as this outcome was for the Iraqi regime, there is no evidence to suggest that the Iraqi leadership intended it to happen or even was aware that it was occurring. Similarly, China's tight-lipped and centralized formulation of foreign policy enjoys certain advantages over Washington's culture of frequent leaks, even without China actively doing anything to exploit this aspect of American policy-making.

Other actors, however, have been more deliberate in their attempts at shaping the coverage they receive in the United States. North Vietnam's use of American celebrities as spokespeople to highlight alleged American atrocities is an infamous example, but more recent strategies have been both more subtle and more effective. Modern Iraqi insurgents have at times displayed a highly sophisticated understanding of the global media, arranging attacks to coincide with media coverage of the target area and even timing major strikes to take advantage of the American prime-time television schedule. Many of America's military adversaries, including both the former government of Iraq and Iraqi insurgents, have shown an uncanny ability to direct television cameras to incidents involving civilian casualties. Iran, meanwhile, seems to have paid close attention to American media coverage and public opinion in its approach to its nuclear program, alternating between a conciliatory and defiant stance in order to avoid inducing a severe American reaction or making legitimate concessions. On the whole, what may once have been a rather unintended undermining of the United States through its media coverage seems increasingly to have become a deliberate strategic choice of American adversaries—and, in particular, an asymmetric choice that transforms a pillar of a free society into a shaky element of foreign policy formulation.

For a foreign state, manipulating American popular opinion related to foreign policy by influencing the media is certainly easier said than done. When the strategy does succeed, however, the results can be highly favorable to an adversary. For example, it was televised images of American casualties that led to an American withdrawal from Somalia in the early 1990s, not a military victory by Mogadishu's warlords.[43] Attempts to manipulate media coverage represent a potentially powerful asymmetric strategy, inverting the power of America's influential media to affect Americans themselves.

What We Might Consider Doing to "Them"

The United States should prepare to respond to asymmetric strategies employed against it by a range of foes, from localized insurgencies to would-be regional hegemons. America should also consider doing something less reactive and more innovative: America needs to craft unique asymmetric strategies of its own. By and large, this has not been our approach to date. "[T]he United States has virtually assured potential adversaries that it will respond to their actions only in particular, well-defined, reactionary, and very controlled ways."[44] In some ways, this is a consequence of America's position as the primary guarantor of global stability. Yet the United States can move beyond its "symmetric" habit of mirroring and then outmatching opponents' capabilities without compromising its global role.

Asymmetric strategies offer America a number of advantages. Asymmetric strategies tend to be economical, since they can side-step the need to match an opponent's key capabilities with expensive capabilities of one's own. Asymmetry often produces significant strategic surprise, at least temporarily permitting the user to seize and exploit the initiative as the opponent struggles to re-evaluate the situation. More fundamentally, an opponent's discovery that his strength is also in some sense a debilitating weakness can lead to considerable confusion.

The uncertainty that asymmetric strategies tend to produce make them deeply unsettling to their targets, leading to confusion about the relative strengths of adversaries, the viability of existing defenses, the utility of existing response options, and even the validity of the foundation of one's own power. This power to unsettle and confuse a target may explain asymmetric strategies' frequent association with terrorism, as the effects just described are precisely those terrorists seek when they launch their attacks. As we have seen, there is nothing about the motivations or relative weaknesses of terrorists that make them the exclusive or even most effective users of asymmetric strategy.

Just as a muscular and skilled fighter may employ jujutsu techniques to devastate a physically weaker foe, strong states may employ asymmetric strategies to achieve dramatic results against weaker opponents. Perhaps this is roughly what Thornton has in mind when he argues that "[t]here is much to be said for the idea that the powerful must become more like the weak in order to match their capabilities."[45] What we are proposing here is not that the United States emulate the particular ways in which the weak make use of asymmetric strategies. Instead, we propose that America develop unique asymmetric strategies of its own. These strategies will emerge from the unique capabilities of America itself, in relation to its adversaries. Crucially, they should be consistent with America's moral character and position of global leadership.

As it confronts a global landscape increasingly populated with challengers weak and strong, the United States would do well to consider the advantages of the asymmetric approach. We do not suggest, of course, that there is an asymmetric solution to every strategic problem, nor that a given strategy is good or wise simply because it is asymmetric. The ongoing global embrace of

asymmetry by state and nonstate actors alike should give American strategists some indication of the potential benefits of such thinking. American power is indeed vast, but it is not infinite. As it seeks to husband its own power while confronting an array of increasingly muscular challengers, the United States would do well to turn its rivals' strengths against them.

Notes

1. Steven Lambakis, James Kiras, and Kristin Kolet, "Understanding 'Asymmetric' Threats to the United States." *Comparative Strategy* 21, no. 4 (2002): 241-277. Specifically, on page 241: "'Asymmetry' is a term . . . [that] contributes to confusion in understanding modern-day threats and distorts thinking about the security challenges facing the country."

2. It is important to distinguish between asymmetric conflicts, which are interactions whose asymmetry is a simple fact resulting from some sort of disparity between the clashing parties, and asymmetric strategies, which are deliberate attempts to shape interactions. The latter constitute the focus of this article.

3. Richard Norton-Taylor, "Asymmetric Warfare," *The Guardian*, 3 October 2001, http://www.guardian.co.uk/world/2001/oct/03/afghanistan.socialsciences (accessed June 16, 2011), and Colin S. Gray, "Thinking Asymmetrically in Times of Terror." *Parameters*. Vol. 32, no. 1 (Spring 2002): 5-14. "Excluding the shared American and Soviet cold war concept of MAD—mutually assured destruction—all warfare has been asymmetric, says Phillip Wilkinson of King's College, London," Norton-Taylor (2001). A similar assertion is found in Gray (2002), 14: "all of America's wars have been asymmetrical contests"; "all warfare is asymmetrical."

4. Montgomery C. Meigs, "Unorthodox Thoughts about Asymmetric Warfare." *Parameters* 33, no. 2 (Summer 2003): 4-18; Steven Metz and Douglas V. Johnson II, *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts* (Carlisle, PA: Strategic Studies Institute, 2001). Metz and Johnson, 1. Compare this similar, if more convoluted, definition, in Meigs, 4: "Asymmetry means the absence of a common basis of comparison in respect to a quality, or in operational terms, a capability."

5. Barnett, Roger W, *Asymmetrical Warfare: Today's Challenge to U.S. Military Power* (Washington, DC: Brassey's, 2003), 15.

6. Rod Thornton, *Asymmetric Warfare: Threat and Response in the 21st Century* (Cambridge: Polity Press, 2007), 1.

7. Lambakis, Kiras, and Kolet, "Understanding 'Assymetric,'" 242. Similar is the definition offered by Steven J. Lambakis, "Reconsidering Asymmetric Warfare," *Joint Forces Quarterly*, no. 36 (2004): 102-108. On page 102, Lambakis states: "*Asymmetry* typically describes an enemy that thinks or acts differently from America, especially when faced with conventionally superior U.S. forces."

8. Thornton, *Asymmetric Warfare,* 55. Thornton comes closest to this formulation, though—as already discussed—he offers other variations as well: "The turning of strengths into vulnerabilities is obviously what the asymmetric warrior is looking for."

9. Ibid., 3.

10. U.S. Joint Chiefs of Staff, *Joint Warfare of the Armed Forces of the United States* (Washington, D.C.: Joint Chiefs of Staff, 1995), IV-10.

11. Thornton, *Asymmetric Warfare,* 27.

12. Lambakis, Kiras, and Kolet, "Understanding 'Assymetric,'" 253.

13. Thornton, *Asymmetric Warfare,* 4-5. Thornton notes that "it is useful to point out that asymmetric techniques can also be applied by the *stronger* power," and then underscores "the importance of the asymmetric threat today—from both state and sub-state actors." But see also page 76: "The real threat . . . is from the weak state asymmetric adversary." Why is the "real threat" not from the *strong* state asymmetric adversary?

14. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America* (Dehradun: Natraj Publishers, 2007), 115.

15. In practice, of course, relative strength does sometimes correlate with targets of asymmetric strategies, as actors weak along traditional dimensions must look for creative ways to approach stronger adversaries if they are to have any chance at all of prevailing. But, in addition to there being no necessary relationship between the *objective* weakness of an actor and its decision to employ an asymmetric strategy, there is nothing inherent about *relative* weakness in the concept of asymmetry: instead, asymmetry is about revealing an adversary's strength as a weakness by drawing on one's own apparent weakness as a strength, even if one is, overall, the stronger party.

16. Thucydides, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*. Robert B. Strassler, ed. (New York: The Free Press, 1976), 43.

17. Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York: Simon & Schuster, 1996), 187.

18. Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars"* (Arlington, VA: Potomac Institute for Policy Studies, 2007); Erin M. Simpson, "Thinking about Modern Conflict: Hybrid Wars, Strategy, and War Aims" Paper presented at the annual meeting of the Midwest Political Science Association, Palmer House Hilton, Chicago, Illinois, April 7, 2005, 3. http://www.allacademic.com/meta/p84945_index.html (accessed June 16, 2011). The term "hybrid war" is also occasionally used to describe conflicts involving both intra-state and inter-state warfare, rather than a fusion of conventional and irregular methods employed by a single belligerent.

19. Thomas X. Hammes, *The Sling and the Stone: On War in the 21st Century* (St. Paul, MN: Zenith, 2004); Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (London: Penguin Books, 2005); David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford: Oxford University Press, 2009). These books offer thorough discussions of insurgency and its evolving dynamics.

20. Offensive state-sponsored insurgency by proxy, such as North Vietnam's campaign against the South using the Viet Cong, is another matter. It is worth noting as well that South Vietnam was ultimately defeated by a conventional military invasion, not by insurgent activity.

21. Kilcullen, *The Accidental Guerrilla*. Che Guevara's expeditionary insurgent campaigns in Latin America, and al-Qaeda's strategy of embedding itself with local and regional insurgencies such as the Taliban, may present exceptions to this rule. However, both Che and al Qaeda relied heavily on local interlocutors and overwhelmingly used local manpower in their campaigns.

22. Mao Tse-Tung, *On Guerrilla Warfare,* trans. S.B. Griffith (Chicago: University of Illinois Press, 1961).

23. Frank G. Hoffman, *Conflict in the 21st Century*, 8, 29. Hoffman defines hybrid wars as those in which conventional and irregular methods are used by the same forces in the same battlespace, allowing for a much broader array of possible force structures and methods within his definition. While the most direct application of the concept is a decentralized, light infantry based model, other examples exist.

24. Andrew Exum, *Hizballah at War: A Military Assessment* (Washington, DC: The Washington Institute for Near East Policy, 2006), 1, http://www.washingtoninstitute.org/pubPDFs/PolicyFocus63.pdf (accessed June 16, 2011).

25. Ibid., 5. Tellingly, the 2006 war began when Hezbollah ambushed an Israeli patrol and kidnapped two IDF soldiers; Stephen Biddle and Jeffrey A. Friedman, *The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy* (Carlisle, PA: Strategic Studies Institute, 2008), 29.

26. Andrew Exum, *Hizballah at War*, 4-7.

27. Biddle and Friedman, *The 2006 Lebanon Campaign*, 35-36. This article provides an extremely useful "taxonomy" of Hezbollah's military behavior during the 2006 conflict.

28. Ibid., xv.

29. Andrew Exum, *Hizballah at War*, 7

30. Ibid., 6.

31. Andrew Krepinevich, Barry Watts, and Robert Work, *Meeting the Anti-Access and Area-Denial Challenges* (Washington DC: Center for Strategic and Budgetary Assessments, 2003). "Assassin's Mace" itself is essentially a cocktail of mutually supporting asymmetric strategies, including undersea mining, cyberattacks and anti-satellite strikes as well as guided missile attacks.

32. Matthew Rusling. "Shifting Gears: For the Military, a Future of 'Hybrid' Wars." *National Defense* 93 (September 2008): 32-34.

33. Charles Billo and Welton Chang. *Cyber Warfare An Analysis of the Means and Motivations of Selected Nation States* (Institute for Security Technology Studies at Dartmouth College, 2004), 25-40, http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf (accessed June 16, 2011).

34. Ibid., 107-119.

35. Ibid.

36. Project Grey Goose. *Russia/Georgia Cyber War – Findings and Analysis* (17 October 2008), http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report (accessed June 16, 2011).

37. Billo and Chang, *Cyber Warfare*.

38. Colin S. Gray, "The 21st Century Security Environment and the Future of War," *Parameters* 38, no. 4 (Winter 2008), 23-24.

39. Mark Bowden, "The Enemy Within," *The Atlantic*, June 2010, 72-83.

40. Ibid., 82.

41. Ibid., 77.

42. Martin Van Creveld, *The Transformation of War* (New York: The Free Press, 1991), 173-179.

43. Dominic D. P. Johnson and Dominic Tierney, *Failing to Win: Perceptions of Victory and Defeat in International Politics* (Cambridge: Harvard University Press, 2006), 205-241.

44. Barnett, *Asymmetrical Warfare*, 154.

45. Thornton, *Asymmetric Warfare,* 148.