Old Wine in New Bottles: The Nature of Conflict in the 21st Century

by Ryan Grauer

Every so often, something big happens that changes how wars are fought. It may be the development of a new weapon like the longbow or the atomic bomb. It could be the emergence of novel tactics like the infantry square, which helped end the dominance of cavalry on the battlefield, or the "modern system" of warfighting, which, with its emphasis on cover and concealment, small-unit independent maneuver, and close coordination between infantry and artillery, enabled the Germans to break nearly four years of stalemate on the Western Front in the spring of 1918.[1] Or it may be something even more dramatic, like the opening of an additional domain of warfare like those that accompanied the development of the airplane and submarine.[2] Every time such a change occurs, many soldiers and observers hail the coming of a new age of warfare in which the previous rules simply do not apply. Giulio Douhet, for example, famously claimed that airpower, in its capacity to rain hellfire on civilians and shatter morale, would fundamentally change the nature of war and henceforth be the key to victory.[3] Bernard Brodie similarly argued that the advent of nuclear weapons changed war so much that militaries would change from war-fighting to war-preventing organizations.[4] Always, it is argued that the rules of warfare are hopelessly obsolete and, as a result, political and military elites must fundamentally rethink how they are going to use force on the battlefield.

We are living through another such period today. Advances in information processing and networking capabilities have not, as some predicted, lifted the fog of war to allow soldiers and commanders to see the battlespace with perfect clarity, but they have combined with developments in weapons technology to enable a host of previously unimaginable military activities.[5] Pilots in Nevada and Virginia control unmanned aerial vehicles that strike targets in far-flung places like Somalia, Yemen, and Pakistan; soldiers routinely rely on robots to perform dangerous battlefield tasks like bomb disposal and reconnaissance; private and state-sponsored hackers spy on

Ryan Grauer is an Assistant Professor of International Affairs at the Graduate School of Public and International Affairs, University of Pittsburgh. The author would like to thank Luke Condra, Matthew Tubin, and the editors of this journal for comments on earlier versions of this argument.

and attack networked civilian and military computer systems; and the spread of kinetic and directed-energy anti-satellite technology has military planners deeply concerned about how they would wage war in a conflict opening with an attack on space-based resources. This technological revolution has made science-fiction concepts such as robot wars, cyber "Pearl Harbors," and space combat conceivable in the real world, and many contemporary analysts have followed the well-trod path of their forebears in arguing that twenty-first century wars will be fundamentally different from those that have gone before.[6]

These analysts, however, overstate their claims. Just as airpower has yet to end a war by shattering civilian morale and many wars have been fought in the shadow of nuclear weapons, today's technological revolution will not change the essential nature of war. Violent conflicts in the twenty-first century, whether they involve states, non-state actors, or an amalgamation of the two, will remain political at their core. As theorists discovered at the height of nuclear strategizing during the Cold War, there are only a few ways in which force can be used to advance political aims. Emergent technologies will necessarily alter the appearance of future wars and may well endow actors previously incapable of confronting states with the means to do so. But such superficial changes are not indicative of a deeper transformation in the nature of war itself. To paraphrase the Prussian strategist Carl von Clausewitz, future wars may have a distinctly different grammar, but their logic will be indistinguishable from those of the past. Accordingly, scholars and policymakers must resist the temptation to throw out the twentieth century playbook. Classical strategic theory not only remains relevant in today's high-tech world, but points the way toward an effective and efficient twenty-first century national security strategy that emphasizes the importance of defense and deterrence rather than raw offensive capabilities.

The Use of Force in International Relations

War, as Clausewitz tells us, is the "continuation of political intercourse, carried on with other means."[7] In this oft-quoted and misunderstood phrase, Clausewitz emphasizes two points. First, just as individuals can disagree about social status, access to resources, and the fulfillment of real or supposed obligations, political communities do not always coexist harmoniously. When disagreements cannot be resolved peacefully—perhaps because one or both parties misperceives the true strength of its bargaining position—the lack of a higher arbiter means that resorting to force is often required to resolve conflicting claims.[8] Escalation to the use of organized violence, however, does not remove or alter the fundamentally political nature of the dispute. The second point is that war is political communication in its own right. The use of force, whether it takes the form of a Greek phalanx fighting in formation, a German armored division rolling through the Ardennes, a mushroom cloud over Hiroshima, or a hijacked plane crashing into a building, is analogous to the trading of diplomatic notes. War reveals information about each side's capabilities and resolve.[9] It differs from peaceful political communication in its

cost; words are cheap while the actual use of force is not. However, by revealing credible information actors might not otherwise have when calculating their own interests and capabilities, the use of force enables belligerents to reach a settlement on questions that previously seemed intractable.

Force can be used in political discourse in six ways.[10] The first two are the direct and concerted application of either offensive or defensive violence through the actual use of military capabilities. Operation Overlord and the Wehrmacht's defense of the French coastline in June 1944 are examples, as are the American drive on, and Iraqi defense of, Baghdad in March 2003. Martial strength and resolve are on display when force is used directly and actors typically come to a swift resolution of their dispute.[11] Force can also be used indirectly in one of four ways. First, an actor might threaten to use force to punish an adversary if it attempts to change the status quo. Deterrence, as this kind of threat is called, is most famously associated with the mutual threats made by the United States and the Soviet Union during the Cold War to obliterate one another if either launched nuclear weapons, but it is also used in conventional disputes.[12] Second, an actor can threaten to use its overwhelming military capabilities to prevent the adversary changing the status quo. This kind of threat, sometimes called denial but more properly termed dissuasion by defense, is implicit in China's development of anti-access and area-denial capabilities; the United States is meant to understand that it will not be able to insert its forces into the region in the event of a shooting war in the Taiwan Strait and, moreover, it would be foolish to try.[13]

THE USE OF FORCE ENABLES BELLIGERENTS TO REACH A SETTLEMENT ON QUESTIONS THAT PREVIOUSLY SEEMED INTRACTABLE.

Third, an actor can attempt to alter the status quo by threatening to punish an adversary if it does not change its behavior. Compellence, as Thomas Schelling called this kind of threat, often requires the limited use of force. After all, a target is unlikely to believe that a threatener will use force to change the status quo without some demonstration of that actor's strength and resolve.[14] Compellence is distinguished from the offensive use of force, however, in that the bulk of the threatener's capabilities are perceived to be held in reserve; the threat works because of the target's fear of the violence that could be forthcoming. This is the logic that drove debates about "limited strikes" and escalation up the nuclear ladder during the Cold War; a few nuclear weapons, it was argued, could be fired in a crisis to signal resolve, demonstrate a willingness to increase the stakes of the conflict, and foreshadow the horror that could be unleashed if the adversary did not capitulate.[15] Today, al Qaeda employs a similar strategy in its fight against the West. It does not have the capability to physically force the United States out of the Middle East or to end its support for Israel, so it inflicts pain through attacks of varying size. The implicit threat that the group wishes to convey is, if the United States does not comply, it will continue and possibly even increase the number and destructiveness

of its attacks. The United States' decade-long war against al Qaeda has reduced the credibility of the group's threat, but the logic mirrors that of adversaries in earlier eras. The final way that an actor might use force indirectly is by threatening the overwhelming use of violence to change the status quo—regardless of any defense proffered—if the target does not accede of its own accord. The United States employed this type of persuasion by offense threat in March 2003 when President Bush announced that Saddam Hussein and his sons must leave Iraq in two days or see the regime changed forcibly. The ultimatum was apparently not sufficiently credible, and the United States and its partners were forced to resort to the direct use of offensive force to make good on the threat.[16]

Emergent Technologies and the Use of Force

Emergent technologies can be used for many purposes, several of which are unrelated to interstate and intergroup conflict. Cyber espionage operations like Shady Rat and Ghostnet, as well as the possibility of Mexican drug cartels using drones to scout for unguarded border-crossings, pose new difficulties for law enforcement and the protection of private information, but they do not constitute the use of force for political purposes.[17] Accordingly, I set aside such uses and focus on the ways in which those capabilities shape actors' abilities to use direct and indirect force as a means of political intercourse. In doing so, I argue that the three most prominent emergent technologies have mixed impacts on the conduct of war. While the use of force is generally made easier and potentially more effective for adopters of the new tools of war, advances in the use of drones, space systems, and cyber capabilities can be costly to implement, and reliance on such systems introduces new vulnerabilities that must be addressed if the United States is to ensure its security in the twenty-first century.

Unmanned and Robotic Systems

Unmanned and robotic weapons represent the latest iteration of the centuries-long progression in which men of war have sought to increase standoff ranges. From daggers, swords, and spears to bows, artillery, and firearms to airplanes, cruise missiles, and intercontinental ballistic missiles, improvements in weapons design over time have enabled combatants to identify and kill each other from ever-increasing distances. Unmanned weaponry—controlled remotely by human operators—and robotic weaponry—capable of fully autonomous operation, including target selection and elimination—continue this trend by enabling soldiers to kill while not physically present on the battlefield, sometimes from half a world away. Such weapons also conform to trends in weapons design by offering significant improvements in accuracy. Drone aircraft, for example, are frequently criticized for causing excessive civilian casualties. Available evidence from Pakistan, however, suggests that, between 2004 and 2012, the average number of civilians killed per strike fell from about eleven to almost zero.[18] At the very least, current capabilities

cause much less collateral damage than did many weapons systems of yore. Unmanned and robotic systems are thus different from weapons of the past, but the difference is centered primarily on their increased standoff and targeting capabilities and is one of degree rather than kind.

Unmanned and robotic weapons, as sophisticated kinetic tools of war, enhance actors' capabilities to use direct and indirect force. Offensively, mounting cameras and guns on remote-controlled tracked vehicles such as the Special Weapons Observation Remote Direct-Action System (SWORDS) or aerial platforms like the Predator drone enable militaries to push firepower into areas and situations where it might be too dangerous to send a person.[19] New attack weapons under development that employ swarms of miniature drones to assault targets are more sophisticated—yet still kinetic in function—and further improvements in robotics could theoretically obviate the need for human presence on the battlefield during an attack.[20] Defensively, drones and robotic systems can be used to guard perimeters. Surveillance drones currently patrol American borders to monitor for illegal crossings.[21] Improvements in observation, lingering, and air-ground coordination capabilities could portend the development of a combat-ready system useful for force-protection purposes. Though weapons like the Patriot missile defense system are not yet sufficiently sophisticated in their capacity to distinguish genuine from false targets to operate reliably without human input, improvement in sensory capabilities will eventually enable automated systems to react to and destroy incoming threats much more quickly than their manned counterparts. Sophisticated as today's unmanned and robotic weapons are, however, they are functionally analogous to Ford's Model-T in terms of their potential.[22] Future versions of such systems will only increase the amount of direct force that technologically capable actors can bring to bear in coming conflicts.

By increasing an actor's offensive and defensive capabilities, unmanned and robotic technologies also enhance the actor's ability to use force indirectly. The capacity to project force into areas beyond the easy reach of conventional armies opens new vistas for credible deterrence and compellence. The Hindu Kush, for example, remains a formidable obstacle for any would-be coercer. As many Taliban and al Qaeda fighters have discovered to their detriment, however, it does not provide quite as safe a haven as it once did; the groups must take more seriously American threats to apply force to compel a change in their operational behavior. At the same time, the increased accuracy of such technologies allows for more finely tuned threats; when it is possible to strike an individual rather than a general area, it would be foolish for a target to believe that concerns about collateral damage will preclude a threatener from acting. Similarly, dissuasion by defense and persuasion by offense are enhanced by unmanned and robotic weapons. As force multipliers, such tools increase the credibility of an actor's claims that it possesses sufficient defensive or offensive capabilities to achieve its ends regardless of what the target chooses to do.

The beneficial effects that unmanned and robotic weapons have on the use of

direct and indirect force come at a significant cost, however. While drones and other remote-controlled weapons can go places that men and more conventional military equipment cannot, they require extensive human and technical support. For example, 168 ground personnel are needed to keep a Predator aloft, 180 are required for a Reaper, and 300 support the Global Hawk spy drone.[23] Given that conventional American military forces tend to field about three support and administrative personnel for every one combat soldier, there is substantially more manpower behind such "unmanned" systems than there is in more traditional platforms.[24] Effective use of such tools also requires extremely large numbers of analysts to sift through the veritable mountains of data collected—many more than are currently available in the US military and intelligence community.[25] Beyond the human requirements for operation and exploitation of such tools, the bandwidth needed for control of and communication with unmanned and robotic systems is enormous and growing. With such systems adding to the demands of conventional tools like radio communications, it is unclear that battlefield bandwidth-provision capabilities can keep pace with operational requirements.[26] Finally, such weapons are ultimately limited in their technical and operational capabilities and are unlikely to ever serve as a complete substitute for human presence on the battlefield. Technically, overhead cover stymies aerial drones while mundane challenges like walls, the natural folds of the earth, and a child with a can of spray paint are able to defeat the camera lenses of land-based unmanned systems. Operationally, soldiers will still be needed for follow-on mop-up and occupation duties no matter how well such systems perform their combat tasks. While it is true that unmanned and robotic weapons can enhance the direct and indirect use of force on future battlefields, without substantial investments of manpower for support and combined operations, as well as economic resources for developing all of the supplementary technologies required for effective use, there is no guarantee that they will.

Space Warfare

Space-based communications, navigation, and coordination capabilities are essential in modern warfare. Manned ground and aerial platforms have long relied on such resources and, as the number of diverse assets used in military operations has increased over time, dependence has risen. Unmanned aerial systems are even more reliant on space assets. Though drones capable of flying without the assistance of GPS are currently under development, virtually all of the unmanned and robotic aerial weapons discussed in the previous section are unable to operate without the vast network of communications satellites orbiting the earth.[27] Accordingly, when considering the impact of space warfare on future conflicts, the topic under consideration is not the kind of directed-energy battles depicted in science fiction or even the placement of weapons intended for terrestrial targets in space. States have scrupulously complied with the 1967 Outer Space Treaty banning the weaponization of space.[28] Rather, the issue is an actor's capability to use its space assets for navigation, communication, and coordination purposes while defending against the

adversary's attempts to use electronic, kinetic, directed-energy, or electromagnetic means to attack satellites and ground-control stations and impede or block the transmission of signals between the two.

There is an inherent duality in the realm of space warfare, where offense and defense are tightly linked. Assuming for the moment that an actor can preserve its space-based systems, the direct and indirect use of force is made easier. Considering first the direct use of force, there are two ways in which the exploitation of such assets can enhance offensive and defensive actions. The first is by enabling the use of modern navigation, communication, and coordination technologies.[29] From Abrams-class tanks to the new F-35 (when it enters service) to the Predator and Reaper drones discussed above, effective movement, cooperation, and striking power are almost impossible without the network of military and civilian space assets that relay data around the globe. Though the United States projected tremendous power during World War II without the assistance of satellites, it would be quite hard pressed to do so again today; the high-powered weapons platforms on which it relies to project force today were built with the assumption that space-based relay and guidance capabilities would be available in future wars. The second way in which space assets can enhance the direct use of force is by eliminating an adversary's space assets. If an actor can disrupt, degrade, or destroy an adversary's capacity to use its space assets at the outset of a future war, then the target of the attack will be significantly weakened and the aggressor will be better able to exploit its own offensive and defensive capabilities.[30] By facilitating the direct use of force, some capabilities for indirect force are also strengthened. Threats to use military power in the absence of preemptive cooperation by an adversary are made more intimidating and perhaps more credible. In addition, sophisticated spy satellites can render deterrent and compellent threats more credible by improving the threatener's knowledge regarding the target's compliance; if the target knows that the threatener has the means to check compliance (in addition to the capability to punish malfeasance) it will be more likely to accede to the demands made upon it.

IF AN ACTOR CAN DISRUPT, DEGRADE, OR DESTROY AN ADVERSARY'S CAPACITY TO USE ITS SPACE ASSETS AT THE OUTSET OF A FUTURE WAR, THEN THE TARGET OF THE ATTACK WILL BE SIGNIFICANTLY WEAKENED AND THE AGGRESSOR WILL BE BETTER ABLE TO EXPLOIT ITS OWN OFFENSIVE AND DEFENSIVE CAPABILITIES.

Yet few belligerents in future conflicts will be able to assume that their space-based resources will remain wholly intact. Satellites and their links to terrestrial users are exceptionally fragile; literally anything more than four millimeters in size that flies through space has the potential to destroy satellites and signal jamming transmitters

are widespread.[31] Accordingly, reliance on space systems for navigation, communication, and coordination purposes exposes new vulnerabilities that facilitate the indirect use of force by adversaries less reliant on such assets. First, as noted above, the loss of space systems can seriously disrupt and even inhibit the effective use of military force. An adversary that possesses sufficiently capable anti-satellite or communications-jamming technology can issue especially threatening and credible warnings designed to dissuade by defense. Second, because satellites orbit the earth in predictable, easily tracked paths, they are attractive soft targets for adversaries.[32] Just as cities were held hostage in many nuclear war plans, satellites can be attacked for offensive or defensive purposes or held hostage as the targets of deterrent and compellent threats.[33] Thus, space-based communication, navigation, and coordination resources can significantly enhance the direct and indirect use of force, but reliance on those same capabilities renders a technologically sophisticated actor at risk for manipulation by moderately capable actors in possession of tools to disrupt, degrade, or destroy space assets and their links to the earth.

Cyber Capabilities

Though there are myriad ways in which actors with malevolent intentions can use cyber capabilities to cause harm, most cannot be logically equated with the use of force. Cybercrime—the theft or destruction of personal information on networked systems—is increasingly prevalent and bothersome to individuals, but it does not constitute the use of force. Cyber espionage, or the use of networked systems to spy on and steal crucial operational information from civilian, military, or governmental entities, is conceptually closer to the use of force, but these activities are more akin to traditional forms of surveillance and spycraft than the use of violence for political purposes and are not properly considered acts of war. Cyber attacks, on the other hand, are efforts directed at civilian, military, and governmental networks with the purpose of disrupting, degrading, or destroying information, computers, and the systems those computers control; they are the digital domain's equivalent to the conventional use of force to, in Clausewitz's words, "disarm the enemy."[34] These are the activities that have implications for the direct and indirect use of force in future conflicts.

Cyber attacks, whether they take the form of logic bombs, denial of service attacks, or the distribution of malicious software that corrupts the normal performance of computing tasks, will be central components in future wars, though not for the reasons often assumed. Many argue that two features of warfare in the cyber domain will make such attacks especially potent and potentially war-winning in twenty-first century conflicts. First, stealth and anonymity are much more easily achieved in the cyber domain than in more conventional arenas of warfare. Targets are likely to be hard-pressed to defend against unknown threats and, when struck, not know at whom to retaliate. Second, increasingly sophisticated cyber capabilities will allow for devastating independent cyber assaults on networked civilian, military, and governmental systems. These arguments, while technically correct,

misunderstand the way in which cyber capabilities must be used in political conflicts as opposed to activities like crime and espionage. To realize their potential in future conflicts, cyber attacks cannot be anonymous nor can they be used without the accompaniment of more traditional tools of war.

On the first point, because war is political in nature, the anonymity offered by cyber attacks is counterproductive. Using force for political purposes, whether it takes the form of direct offensive or defensive action or indirect deterrent, compellent, offensive, or defensive threats, requires that actors—whether they are states, groups, or individuals—make themselves and their desires known.[35] If an actor were able to successfully cause power outages, plane crashes, or some other spectacular disaster through a cyber attack, without revealing both who it was and what it wanted, the target would not know if the attack were a one-off event or the opening salvo in a potentially long and deadly campaign. In addition, if the attacked party were inclined to give in to the aggressor's demands, it would not know how or to whom to signal submission. Beyond being undesirable for the purposes of political intercourse, anonymity is likely to be infeasible even for those actors that would wish to remain secret. Only rarely is force used in a "bolt-from-the-blue" attack. Rather, it is most often employed in the context of some visible and palpable political crisis. In such situations, a target will rarely have trouble discerning who was behind a cyber attack. Georgia, for example, cannot prove that Russia or hackers affiliated with that state conducted the denial of service attacks launched simultaneously with Russian ground forces in 2008, but there is little reason to believe that some other group was behind the assault. Similarly, prior to the United States' 2012 tacit admission of the role it played in the creation and distribution of the Stuxnet, Duqu, and Flame worms, Iran had little doubt that the United States and Israel were the likely authors of the cyber attacks on its nuclear program.[36] Anonymity is not the reason that cyber attacks will be useful in future conflicts.

BEYOND BEING UNDESIRABLE FOR THE PURPOSES OF POLITICAL INTERCOURSE, ANONYMITY IS LIKELY TO BE INFEASIBLE EVEN FOR THOSE ACTORS THAT WOULD WISH TO REMAIN SECRET.

Similarly, the potentially devastating effects of isolated cyber attacks are unlikely to be sufficient to resolve the political disagreements. While it is true that cyber attacks can cause significant damage—Stuxnet delayed Iran's progress toward nuclear weapons by two or three years; the 2007 distributed denial-of-service (DDOS) attacks on Estonia rendered financial transactions temporarily impossible; the 2008 attacks on Georgia impeded its ability to communicate with the outside world; and the 2011 North Korean DDOS attacks on South Korean targets shut down stock trading capabilities for a few minutes—the defining feature of all such assaults is their transitory nature. As of this writing, Israel is seriously contemplating a

conventional strike on Iranian nuclear facilities because neither Stuxnet and other cyber efforts nor economic sanctions have brought the program to a halt. Similarly, Estonia, Georgia, and South Korea have not suffered measurable long-term effects from their cyber victimhood. It is conceivable that future cyber attacks could result in a high-tech "Pearl Harbor;" electric grids could be shut down, trains could derail, planes could crash, and people might even die. However, without the use of conventional forces to follow on and exploit the chaos created by cyber attacks, the targeted actor will recover and, very likely, retaliate against the attacker.

Cyber attacks, though they will not benefit from the anonymity offered by the cyber domain when used in war and are especially unlikely to independently resolve political disputes, will be helpful in future conflicts because, like space-based assets, they enhance actors' capabilities to use force directly and indirectly in the pursuit of political ends. As Russia showed in 2008, combining cyber attacks with conventional operations can hobble the adversary and enable the attacker to apply offensive force more effectively than would otherwise be the case.[37] Though it has not yet been tested in warfare, a targeted actor could theoretically use cyber attacks to blunt an attacker's assault. Iran claims to have hijacked a US spy drone through a spoofing attack in 2011, and researchers at the University of Texas successfully spoofed a civilian drone through the unencrypted GPS network on which it relied.[38] There is little reason to think that such techniques could not be improved and used against surveillance and strike drones. The indirect use of force is simultaneously enhanced through the force multiplying effects of cyber attacks; persuasion through offense and dissuasion through defense are easier when a potential threatener is powerful along many dimensions of military capability. Cyber attacks could also serve as a tool for deterrent and compellent purposes but, as is evidenced in the case of Iran, even highly sophisticated and powerful cyber attacks have, to date, failed to coerce determined actors.

As is true with unmanned and robotic weapons and space systems, cyber capabilities do not come cheap and they introduce new vulnerabilities for adopters. While the barriers to entry to the cyber domain are extremely low—a laptop and an internet connection—"size still matters."[39] Stuxnet and other sophisticated worms are extremely complex and require teams of skilled designers with access to resources that few outside states can provide. Moreover, to do serious damage, cyber operations must be based on an intimate understanding of the adversary's computer and network infrastructure—precisely the kind of knowledge that is the result of long-term efforts and difficult for non-state entities to procure.[40] Without the resources, time, and personnel to dedicate to the creation of worms and other attacks that are effectively one-shot efforts (Stuxnet is not useful for an attack on anything but the Iranian centrifuges running at the Natanz facility), actors are limited in the damage they can inflict upon others in the cyber domain. At the same time, however, highly networked and cyber-reliant actors are exposed to many new threats. As they become more reliant on networks to control government, military, and civilian systems and infrastructure, many more critical nodes and avenues of attack

are laid open to adversaries. A network-dependent actor is vulnerable to deterrent and compellent threats of cyber attack in a way that technologically primitive belligerents are not.

What is to be Done?

Conflicts in the twenty-first century will feature new tools and new actors; they will look very different from conflicts fought in the past. Facing such an environment, it is tempting to surrender to the siren call of practitioners and analysts who claim that war has fundamentally changed and new thinking about the use of force is required. Looking beyond the sometimes-dazzling effects of emergent technologies, however, it is clear that, while the new tools of war offer unique ways of applying force, they do not in themselves change either the nature or logic of violent political disputes. There are still only six ways of employing force in war. Unmanned and robotic weapons, space-based communications resources, and cyber capabilities merely enhance an actor's ability to apply force. Relying on the tenets of classical strategic theory and thinking carefully about the advantages and drawbacks of reliance on each emergent technology provides a few important insights about the future security requirements of the United States.

The first insight is that, while offensive tools are good to have, defense will be the paramount virtue in the twenty-first century. The United States must emphasize and improve its defense at home and in space if it is to remain a preponderant military power in the future. Turning first to terrestrial defenses, the physical homeland itself is secure; no state is likely to violate the territorial integrity of the United States with man or machine in the near future. The same cannot be said of the cyber realm, however. The challenges of protecting this domain are legion. The government can develop and deploy firewalls and other defenses to protect state and military networks, but the systems that govern much of the nation's critical national infrastructure—including electrical grids, nuclear power plants, water and sewage treatment plants, and other essential utilities—are held privately. Commercial incentives govern decisions regarding the appropriate level of cyber security in such instances and the market does not often reward more than the bare minimum levels of protection that are easily circumvented by determined hackers.[41] Working to bolster public-private partnerships for the purpose of defending critical national infrastructure networks is essential, as is the development of plans to take threatened systems offline, if only temporarily, in a crisis. Cyber attacks can only threaten networked systems; eliminate the external connections and there can be no threat.

In space, the need for improved defenses is just as urgent. The US can bring tremendous firepower to battlefields virtually anywhere on the globe, but that firepower rests on an extremely fragile space infrastructure. As bandwidth demands grow along with the use of advanced weapons platforms, so, too, does the United States military's reliance on commercial satellites incapable of defending against anti-satellite weapons or jamming.[42] The Department of Defense's Fiscal Year 2013 Budget Request calls for only $8 billion to be allotted to space-based systems—

approximately 1.5% of the total request and less than the $9.17 billion earmarked for research and development on and procurement of twenty-nine F-35 Joint Strike Fighters.[43] While it may be helpful to have fifth-generation fighters in service, it is just as important to ensure that they, and all of the weapons platforms currently in use, can navigate around the globe and communicate with one another. Retooling budgetary allocations to bolster programs designed to increase the maneuverability and blast protection of satellites, developing anti-jamming capabilities, and increasing the number of satellites available for military use will do more to ensure American military preeminence than the purchase of weapons systems that, to date, have not proven usable or necessary in major conflicts.

The second significant insight that classical strategic theory provides is that deterrence will be almost as essential as defensive capabilities in future conflicts. The diffusion of emergent technologies to many and smaller actors around the globe will render robust preemptive action virtually impossible in the near future. Instead, the United States must be more willing to rely on deterrence for protection of its interests. Deterrence in the future will necessarily rely on different tools and threats than it did during the Cold War, but it can be achieved through conscious and conspicuous procurement strategies. Emphasizing the importance of and increasing the US Cyber Command's budget from the paltry $182 million dollars requested for FY 2013—less than one-seventh of the aid earmarked for Egypt's military in the coming fiscal year—could speed the development of improved offensive and defensive cyber capabilities that could be used to visit tremendous punishment on those that attack America's cyber systems.[44] Additionally, though much progress has been made in the field of attribution (determining who is behind cyber attacks), further improvement of such cyber forensic skills would reduce potential attackers' faith in the anonymity nominally provided by the Internet and lend credibility to latent and explicit deterrent threats.[45] Finally, continuing to develop the optical, strike, and loitering capabilities of drone aircraft and other unmanned systems while reducing the number of support personnel needed for keeping the new tools in combat will make it easier for the United States to credibly claim that it will punish those that violate the peace.

After a decade of war that has cost much blood and treasure, the United States cannot afford to throw overboard the collective strategic wisdom of past ages. Fortunately, it does not need to. Frameworks developed in the past to understand how nuclear weapons might be used in war illuminate how today's new technologies will influence conflicts. The future that they suggest is not one that is radically different from the past, but it is one that will require a reorientation of Pentagon programs and budgets. Delay in adjusting to the realities of the direct and indirect use of force, whether the product of legacy programs or parochial Congressional interests in creating jobs for constituents, cannot serve the United States well and may inhibit America's effort to remain the dominant global military power.

Notes

[1] Stephen D. Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton: Princeton University Press, 2004).
[2] On military revolutions in general, see Bernard Brodie, *From Crossbow to H-bomb,* Rev. and enl. ed. (Bloomington: Indiana University Press, 1973); Geoffrey Parker, *The Military Revolution: Military Innovation and the Rise of the West*, 1500-1800, 2nd ed. (New York: Cambridge University Press, 1996); Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest*, no. 37 (Fall 1994): 30–42.
[3] Giulio Douhet, *The Command of the Air*, trans. Dino Ferrari (New York: Coward-McCann, 1942).
[4] Bernard Brodie, *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace and Company, 1946), 76.
[5] William A. Owens, "The Emerging System of Systems," *Proceedings of the Naval Institute* 121, no. 5 (May 1995): 36–39; William A. Owens, *Lifting the Fog of War* (Baltimore: The Johns Hopkins University Press, 2000).
[6] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!," *Comparative Strategy* 12, no. 2 (Spring 1993): 141–165; Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Ecco, 2010). For a more qualified and nuanced argument about the impact robotic technology is having on the nature of warfare, see P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Books, 2009).
[7] Carl von Clausewitz, *On War*, ed. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 87.
[8] Geoffrey Blainey, *The Causes of War*, 3rd ed. (New York: Free Press, 1988); James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (Summer 1995): 379–414.
[9] R. Harrison Wagner, "Bargaining and War," *American Journal of Political Science* 44, no. 3 (July 2000): 469–484.
[10] Avery Goldstein, *Deterrence and Security in the 21st Century* (Stanford: Stanford University Press, 2000), 26–32.
[11] D. Scott Bennett and Allan C. Stam, "The Duration of Interstate Wars, 1816-1985," *American Political Science Review* 90, no. 2 (June 1996): 239–257.
[12] George H. Quester, *Deterrence Before Hiroshima* (New York: Wiley, 1966); John J. Mearsheimer, *Conventional Deterrence* (Ithaca, NY: Cornell University Press, 1983).
[13] Thomas G. Mahnken, "China's Anti-Access Strategy in Historical and Theoretical Perspective," *Journal of Strategic Studies* 34, no. 3 (June 2011): 299–323.
[14] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966).
[15] Herman Khan, *On Thermonuclear War* (Princeton: Princeton University Press, 1960).
[16] Kevin M. Woods and Michael R. Pease, Mark Stout, Williamson Murray, and James G. Lacey, *Iraqi Perspectives Project: A View of Operation Iraqi Freedom from Saddam's Senior Leadership* (Norfolk, VA: Joint Center for Operational Analysis, 2006), 14–16.
[17] Ellen Nakashima, "Report on 'Operation Shady RAT' Identifies Widespread Cyber-spying" *Washington Post*, August 2, 2011, http://www.washingtonpost.com/national/national-security/report-identifies-widespread-cyber-spying/2011/07/29/gIQAoTUmqI_story.html; "Major Cyber Spy Network Uncovered," *BBC News*, March 29, 2009, http://news.bbc.co.uk/2/hi/americas/7970471.stm; Eugene Robinson, "The Emerging 'Drone' Culture," *Washington Post*, August 2, 2012, http://www.washingtonpost.com/opinions/eugene-robinson-the-emerging-drone-culture/2012/08/02/gJQARYbtSX_story.html.
[18] *The Year of the Drone*, Counterterrorism Strategy Initiative (Washington, DC: The New America Foundation, August 24, 2012), http://counterterrorism.newamerica.net/drones. This count of civilian deaths strikes a middle ground between higher counts that include all killed individuals not conclusively proven to be militants as civilians and lower counts that include all killed men and boys of fighting age as militants. For higher and lower estimates of civilian death counts, see the Pakistan Body Count project, at http://www.pakistanbodycount.org and Brian Glyn Williams, Matthew Fricker, and Avery Plaw, "New Light on the Accuracy of the CIA's Predator Drone Campaign in Pakistan," *Terrorism Monitor* 8, no. 41 (November 11, 2010).
[19] Noah Shachtman, "First Armed Robots on Patrol in Iraq (Updated)," *Danger Room*, August 2, 2007, http://www.wired.com/dangerroom/2007/08/httpwwwnational/.
[20] P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Books, 2009); David Axe, "From Bug Drones to Disease Assassins, Super Weapons Rule US War Game," *Danger Room*, August 24, 2012, http://www.wired.com/dangerroom/2012/08/future-warfare/.
[21] Brian Bennett, "Predator Drones Have Yet to Prove Their Worth on Border," *Los Angeles Times*, April 28, 2012.

[22] P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Books, 2009) 110.
[23] Micah Zenko, "10 Things You Didn't Know About Drones," *Foreign Policy*, no. 192 (April 2012); Defense Science Board, *The Role of Autonomy in DoD Systems* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, July 2012), 58.
[24] John J. McGrath, *The Other End of the Spear: The Toot-to-Tail Ratio (T3R) in Modern Military Operations* (Fort Leavenworth, KS: Combat Studies Institute Press, 2007).
[25] Davi M. D'Agostino, *Intelligence, Surveillance, and Reconnaissance: Overarching Guidance Is Needed to Advance Information Sharing* (Washington, DC: Government Accountability Office, 2010).
[26] Jeremiah Gertler, *U.S. Unmanned Aerial Systems* (Washington, DC: Congressional Research Service, January 3, 2012), 17; Axe, "From Bug Drones to Disease Weapons."
[27] Larry Hardesty, "Autonomous Robotic Plane Flies Indoors," *MIT's News Office*, August 10, 2012, http://web.mit.edu/newsoffice/2012/autonomous-robotic-plane-flies-indoors-0810.html.
[28] United Nations General Assembly, "United Nations Treaties and Principles on Outer Space" (United Nations, New York 2002) Available at: http://www.oosa.unvienna.org/pdf/publications/STSPACE11E.pdf.
[29] Barry Watts, *The Military Use of Space: A Diagnostic Assessment* (Washington, DC: Center for Strategic and Budgetary Assessments, 2001), 13.
[30] Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Phoenix, 2006), 308–309.
[31] Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Phoenix, 2006), 291–313; Michael E. O'Hanlon, The Science of War: Defense Budgeting, Military Technology, Logistics, and Combat Outcomes (Princeton: Princeton University Press, 2009), 190.
[32] Colin S. Gray, *Another Bloody Century: Future Warfare* (London: Phoenix, 2006), 294-302.
[33] For a discussion of various state's anti-satellite capabilities, see Eric Sterner, "Beyond the Stalemate in the Space Commons," in *Contested Commons: The Future of American Power in a Multipolar World*, ed. Abraham M. Denmark and James Mulvenon (Washington, DC: Center for a New American Security, 2010), 105–135.
[34] Carl von Clausewitz, *On War*, ed. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 91.
[35] Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University Press, 1966), 89–90.
[36] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012), 188–225.
[37] Ariel Cohen and Robert E. Hamilton, *The Russian Military and the Georgia War: Lessons and Implications* (Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2011).
[38] Lorenzo Franceschi-Bicchierai, "Drone Hijacking? That's Just the Start of GPS Troubles," *Danger Room*, July 6, 2012, http://www.wired.com/dangerroom/2012/07/drone-hijacking/; Greg Jaffe and Thomas Erdbrink, "Iran Says it Downed U.S. Stealth Drone, Pentagon Acknowledges Aircraft Downing," *Washington Post*, December 4, 2011, http://www.washingtonpost.com/world/national-security/iran-says-it-downed-us-stealth-drone-pentagon-acknowledges-aircraft-downing/2011/12/04/gIQAyxa8TO_story.html.
[39] Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011), 117.
[40] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012), 344.
[41] See, for example, the recent attacks on Aramco in Saudi Arabia. Nicole Perlroth, "Connecting the Dots After Cyberattack on Saudi Aramco," *New York Times*, August 27, 2012, http://bits.blogs.nytimes.com/2012/08/27/connecting-the-dots-after-cyberattack-on-saudi-aramco/.
[42] Michael E. O'Hanlon, *The Science of War: Defense Budgeting, Military Technology, Logistics, and Combat Outcomes* (Princeton:: Princeton University Press, 2009), 179–180, 187–200.
[43] "Fiscal Year 2013 Budget Request," *Department of Defense*, http://comptroller.defense.gov/budget.html.
[44] "Executive Budget Summary: Function 150 & Other International Programs, Fiscal Year 2013", *Department of State* (2013), 172, http://www.state.gov/documents/organization/183755.pdf; Keith B. Alexander, *Statement of General Keith B. Alexander, Commander, United States Cyber Command* (Washington, DC: 2012), http://www.armed-services.senate.gov/statemnt/2012/03%20March/Alexander%2003-27-12.pdf.
[45] John Reed, "Is the 'Holy Grail' of Cyber Security Within Reach?," *Foreign Policy*, September 6, 2012, http://killerapps.foreignpolicy.com/posts/2012/09/06/is_the_holy_grail_of_cyber_security_within_reach.