January 2012

INSS
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

STRATEGIC FORUM
National Defense University

Sino-American Strategic Restraint in an Age of Vulnerability

by David C. Gompert and Phillip C. Saunders

About the Authors

David C. Gompert is a Distinguished Research Fellow in the Center for Strategic Research (CSR), Institute for National Strategic Studies, at the National Defense University. Dr. Phillip C. Saunders is Director of Studies and Distinguished Research Fellow in CSR. He is also Director of the Center for the Study of Chinese Military Affairs.

Key Points

- Despite their vast power, the United States and China are becoming increasingly and mutually vulnerable to attack in three strategic domains: nuclear, space, and cyberspace. The futility of defense and dim prospects for arms control in these domains will lead both countries to develop strong offensive capabilities, at least to deter the other.
- The United States and China should deal with these vulnerabilities by pursuing mutual restraint in the use of strategic offensive capabilities in all three domains, building on a foundation of mutual deterrence based on the threat of retaliation.
- A strategic restraint agreement should include reciprocal pledges not to be the first to use nuclear or antisatellite weapons against the other or the first to attack the other's critical computer networks. These pledges should be reinforced by regular high-level communications about capabilities, doctrines, and plans, as well as concrete confidence-building measures to avoid misperceptions, provide reassurance, and engender trust.

For all their power, both the United States and China are increasingly vulnerable. Each faces a range of strategic dangers, from nuclear weapons to disruption of critical computer networks and space links.[1] Because their relationship is at once interdependent and potentially adversarial, the United States and China are especially vulnerable to each other: interdependence exposes each to the other, while the potential for conflict impels each to improve strategic capabilities against which defenses can be futile. Strategic vulnerability cannot be eliminated, only mitigated.

Of the two countries, the United States is stronger in offensive strategic capabilities, notably in nuclear, antisatellite (ASAT), and cyber weapons. Yet it is also increasingly exposed to danger in these domains, confirming that power does not necessarily reduce vulnerability. If Americans thought before the 9/11 terrorist attacks that being the only superpower made them safer, they think otherwise now. Even with a $600-billion-plus annual defense budget, the United States cannot buy its way out of strategic vulnerability.

Meanwhile, China's stunning economic and technological development is enabling it to acquire all forms of power, including offensive strategic capabilities. But China's development is also making it more vulnerable, as its economy becomes more integrated at home and with the world, more dependent on information, and thus more susceptible to disruption. While the Chinese have long felt, based on their history, that weakness breeds vulnerability, they are learning that greater vulnerability can also accompany greater strength.

This Strategic Forum, derived from our book *The Paradox of Power*, confronts the fact that as power grows so does vulnerability.[2] The basic reason is that

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Sino-American Strategic Restraint in an Age of Vulnerability	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Institute for National Strategic Studies,260 5th Avenue Ft. Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**12**	

the same factors that produce modern power—technological advancement and economic integration—also increase exposure to risk and to strategic attack. It is written from an American perspective, with U.S. interests foremost in mind. But because the United States cannot escape its growing vulnerability to China unilaterally, Chinese agreement is needed; therefore, mutual restraint must address Chinese interests as well. Our core idea is that mutual vulnerability calls for mutual restraint in the nuclear, space, and cyber domains. Whether Sino-American distrust will preclude agreed restraint is one of the questions this paper tackles. But even with distrust, self-interest in avoiding harm—in a word, deterrence—can move both powers in this direction.

Vulnerability in the Nuclear, Space, and Cyber Domains

In becoming more vulnerable, the United States and China are not alone. With global economic integration and information networking, most nations are increasingly exposed to disturbances and damage caused by other nations and transnational actors. The 300-year-old model of nation-states controlling their territory, vulnerable only to invasion, was shaken by the advent of strategic bombing and then nuclear weapons. On the chessboard where nations play, queens with stunning speed and unlimited range now endanger sovereign kings (and their realms). Against strategic offense, defense is getting more costly but not more effective, leaving fear of retaliation as the surest way to avert disaster. This has been the essence of nuclear deterrence, though neither the problem nor the remedy is confined any longer to the nuclear domain.

The increased vulnerability of states that began in the mid-20th century with strategic bombing and nuclear weapons has been compounded by two factors that mark passage to the 21st century: economic integration and information networking. The former has increased the exposure of states to each other's products, services, data, money, ideas, surveillance, migrants, and travelers, including terrorists. Integration has also opened new domains in which nations interact: no longer just on land, at sea, and in the air but now also in space and cyberspace. While economic integration has brought growth to those nations that participate in the global economy, it has also reduced their ability to escape risk.

mutual vulnerability calls for mutual restraint in the nuclear, space, and cyber domains

Information networking has accelerated economic integration not only internationally but internally as well, as China's transformation from a fragmented to a national economy shows. China now has the most Internet users in the world; the Internet plays a growing role in government propaganda, burgeoning e-commerce, and management of the local and global supply chains of Chinese companies. Information networking is also demolishing the ability of sovereigns to control what their populations know. This heightens the potential for political upheaval, a problem of more concern to Chinese than to American leaders.

Information networking increases vulnerability in another way: improved military targeting. It has yielded dramatic enhancements in sensors, data processing and sharing, geolocation precision and coverage, navigation, and guidance—thus, in the ability to deliver weapons at any distance with great speed and accuracy, and to defeat defenses. Information technology has made objects—fixed and moving, on land, at sea, and in the air—increasingly observable and vulnerable. Such advances are also evident in space and cyberspace, which are susceptible to targeting and also can serve as media for novel weapons, including electromagnetic and energy-based ones.

Although growing strategic risk affects weak and strong states alike, those that face the power-vulnerability paradox are the strong ones. Recall that the United States and Soviet Union were simultaneously at their most powerful and their most vulnerable during

the Cold War because the capacity of each to inflict nuclear destruction made it the other's primary target. Today, the conventional military superiority of the United States incentivizes adversaries, real and potential, to target its strategic vulnerabilities.[3] For all its power, the United States is hard pressed to protect its territory from nuclear attack, its satellites from ASAT attack, and its computer networks from cyber attack. China has lived with nuclear vulnerability since the 1950s, but growing dependence on space and cyberspace for both commercial and military applications will force its leaders to confront the paradox of power and vulnerability in those domains as well.

All three strategic domains are "offense-dominant"—technologically, economically, and operationally. Defenses against nuclear, ASAT, and cyber weapons are difficult and yield diminishing results against the offensive capabilities of large, advanced, and determined states such as the United States and China.

Nuclear weapons are offense-dominant because of both their destructive force and the difficulty of intercepting missiles in flight, particularly if the attack is large and equipped with countermeasures. The figure on page 4 plots the cost of missile defense (based on the U.S. SM–3 interceptor) against the cost of offense (based on the U.S. Minuteman III intercontinental ballistic missile [ICBM]).[4] If each interceptor costs the same as each ICBM, if each ICBM carried one warhead, and if it took only one interceptor to destroy each ICBM, the relationship of offense and defense would be as represented by the Equal Cost Line. But each interceptor (in this example) costs about $3 million more than each ICBM, so the cost advantage of offense grows as a function of the number of ICBMs, represented by the line just below the Equal Cost Line. If ICBMs carry multiple re-entry vehicles, the cost gap is even worse for defense—the next line down. In reality, it takes more than one fired interceptor on average to destroy an incoming missile—the next line shows the cost gap if it takes on average two interceptors to destroy each incoming missile. Moreover, the odds of intercepting a missile worsen as the size of attack increases because missile defenses can be overwhelmed by the complexity of trying to locate, track, target, and strike large attacks. This is illustrated by the lowest line. Overall—even before taking into account countermeasures to trick defenses—we see sharply declining returns for investment in defense and rewards for investing in offense.[5]

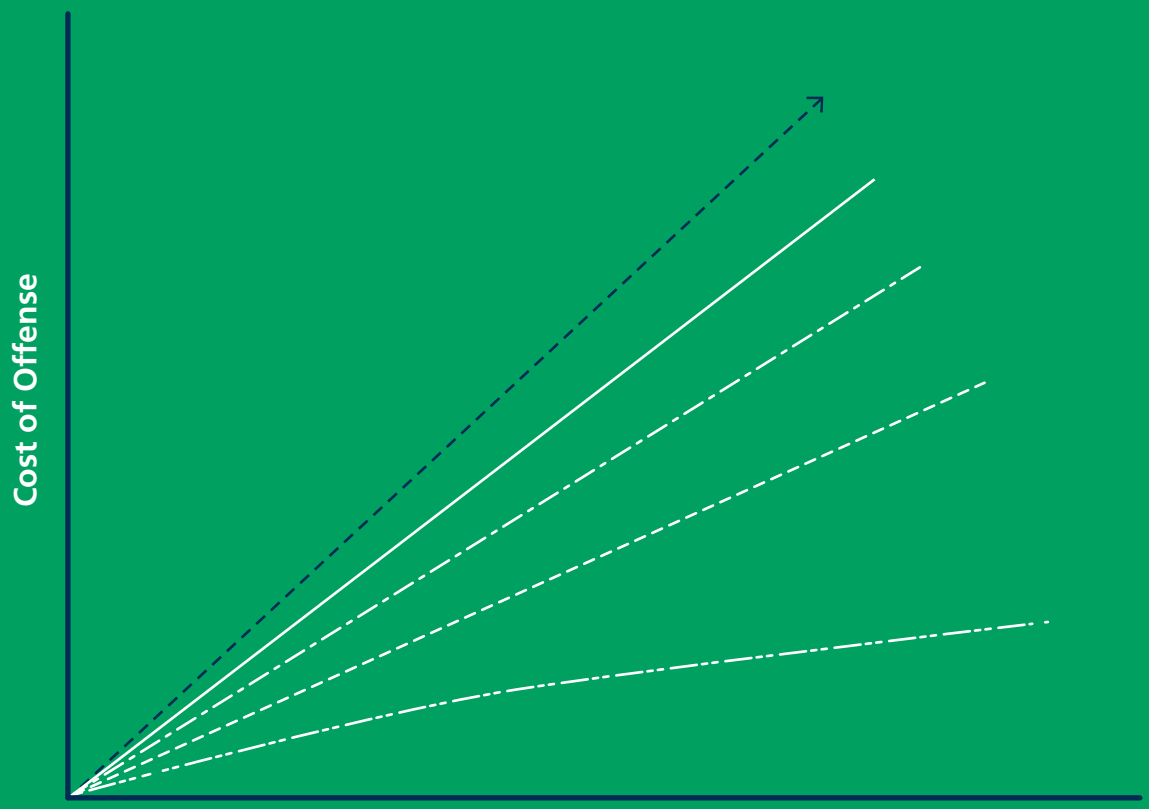
defenses against nuclear, ASAT, and cyber weapons are difficult and yield diminishing results against the offensive capabilities of large, advanced, and determined states such as the United States and China

It is easier and cheaper for China to improve the survivability of its strategic missile launchers, to multiply the number of deliverable weapons, and to penetrate U.S. missile defenses than it is for the United States to maintain a nuclear first-strike capability. Though it has yet to admit it officially, the United States cannot deny the Chinese the second-strike nuclear deterrent they are determined to have.

Satellites are inherently vulnerable: conspicuous, easy to track, and fragile. Destroying them or degrading their performance is easier than protecting them. ASAT interceptors are much cheaper than satellites, giving offense a huge potential advantage. Some degree of space security can be gained through redundancy, but replicating satellites is far more expensive than multiplying interceptors, each of which can rely on a common targeting system.

Likewise, defending computer networks becomes harder and more expensive as the scale and sophistication of the attacker increase. The woes of the cyber defender are compounded by integrated global markets and supply chains for digital components and equipment—in which U.S. and Chinese corporations are leading competitors—

Figure. Cost of Offense-Dominance in Missile and Intercept Systems



Key:

Equal Cost Line

Interceptors VS Single Warhead ICBMs

Interceptors VS MRVed ICBMs

Interceptors with 50 percent success rate VS MRVed ICBMs

Interceptors VS Large ICBM Attack

increasing the potential for strategic degradation of network infrastructure and disruption of services. The diminishing returns on investment in cyber defense relative to offense are especially striking when considering the disparity between "hacking" and "patching" in complexity, cost, and time required: advanced network-defense software contains between 5 and 10 million lines of code; malware contains an average of 170 lines of code.[6] Protection of U.S. Government networks typically requires regulated public competition and acquisition, which can consume years before solutions are contracted for and installed; an attack can be designed and launched in weeks. No sooner are effective defenses finally in place than cyber weapons to defeat them are in the works. Strategic offense dominance gives each country incentives to invest in offense, which spurs the other to do the same to keep pace.

Apart from offense dominance, the advance of technology has slashed the costs in lives and treasure of

Table 1. Human and Economic Costs of Strategic Warfare Compared

	Invasion	Heavy Bombing	Nuclear	ASAT	Cyber
Own Deaths	High	Medium	Low	Low	Low
Cost	High	High	Medium	Medium	Low
Enemy Deaths	High	High	High	Low	Low

Source: David C. Gompert and Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability* (Washington, DC: NDU Press, 2011), 11.

strategic attack. Table 1 shows the decline in the costs and casualties of strategic attack from mass invasion (pre–World War II) to heavy bombing (World War II) to nuclear attack (post–World War II) to space and cyber attack (21st century).[7] The most striking decline is in direct casualties, from millions to virtually none. If one ignores possible deaths resulting from disruption of public services, ASAT and cyber war might even be considered "nonviolent."

With expected casualties plummeting, world opprobrium and resulting inhibitions on decisionmakers could also be greatly reduced. Yet the advantage to the attacker comes from the potential economic and societal harm and resulting blow to the will of the enemy, which grow as vulnerabilities do. Under conditions in which strategic attack might be contemplated, such as crisis, war, or faulty intelligence, the calculus could shift in favor of attack. As offenses improve, thresholds for war in space and especially cyberspace—though not nuclear war—could become perilously low, absent deterrence.

The Logic of Mutual Strategic Restraint

The United States and China are not mortal enemies, as the United States and Soviet Union were. But their growing capacity to inflict strategic harm, when combined with the possibility of conflict, motivates each to be capable of striking at the other's vulnerabilities, at least for deterrence. Fortunately, there are enough cooperative aspects of Sino-American relations that the two should be able to find ways to mitigate their mutual vulnerabilities. After all, even the United States and Soviet Union, despite their animosity, were able to mitigate their nuclear vulnerabilities through mutual deterrence. But while Soviet-American strategic peace was kept by reciprocal fear, there is reason to think—at least to hope—that China and the United States can mitigate their vulnerabilities with a quotient of reciprocal cooperation.

Curbing the dangers of mutual strategic vulnerability through nuclear, ASAT, or cyber war disarmament is largely impractical and unverifiable. The disparity between the large U.S. and small Chinese nuclear arsenals makes bilateral nuclear limitations problematic, and China has been reluctant to participate in any multilateral negotiations until the United States and Russia come down to the Chinese level. Trying to limit or ban ASAT capabilities would founder on problems of definition and verification. Direct-ascent ASAT interceptors are not readily distinguishable from missiles with other missions. The problems with ASAT arms control are compounded by the advent of soft-kill ASAT weapons, whereby directed-energy and electronic attacks can degrade performance, denying use

of space without physical destruction of satellites.[8] It is not possible to monitor and control such capabilities with any confidence. Arms control is patently impossible for cyber war capabilities, in which defensive and offensive technologies are interconnected, subject to continuous and rapid change, increasingly pervasive, largely in nongovernmental hands, and embodied less in hardware than in software.

Poor prospects for arms control, the futility of strategic defense, and the plunging costs of attack mean the United States and China must consider the idea of mitigating their growing vulnerabilities in the nuclear, space, and cyber domains by agreed restraint in the *use* of strategic offensive capabilities. The bedrock of such restraint would be mutual deterrence in each domain, based on the fear of devastating retaliation and the limits of defense. Preconditions for mutual deterrence—namely, risks of retaliation that outweigh expected gains of attacking first—exist in all three domains, although this may not be fully recognized by all parties in the United States and China.

Given the importance of the U.S.-China bilateral relationship for global and regional stability and prosperity, the two countries should try to move beyond mutual deterrence to mutual restraint. The distinction between deterrence and restraint is crucial: while the former rests solely on the threat of retaliation, the latter adds reciprocal pledges to refrain from initiating strategic conflict and cooperation to reinforce such pledges. While mutual restraint does not depend on good intentions, it can ease fears of hostile intent, thus reducing the danger of miscalculation and the collapse of restraint during crises. It also invites—indeed, requires—earnest dialogue and understanding regarding the shared problem of strategic vulnerability.

To this end, Sino-U.S. mutual restraint should include regular high-level communications about capabilities, doctrine, and plans, along with confidence-building measures (CBMs) to avoid misperceptions, provide reassurance, and foster trust. Because China and the United States have both convergent and divergent interests, mutual strategic restraint is possible and necessary. Without convergent interests, there would be no hope for genuine mutual restraint; without divergent interests, conflict would be implausible, and vulnerability would not matter.

As a logical starting point, the United States should acknowledge the inevitability and accept the legitimacy of China's nuclear retaliatory capability, endorse mutual deterrence, and be prepared in principle to explore a bilateral understanding not to use nuclear weapons first against the other or its allies. However, given its severe vulnerability in space and cyberspace and the growing importance of those domains, the United States should insist on a broad and integrated approach to mutual restraint.

the United States and China must consider the idea of mitigating their growing vulnerabilities in the nuclear, space, and cyber domains by agreed restraint in the *use* of strategic offensive capabilities

Mutual ASAT restraint should take the form of agreeing not to be the first to try to deny the other country's use of space, in peace or war. This would include a ban on attacks not only on satellites, but also on any efforts to disrupt satellite functions by interfering with their communications or control, whether by physical or other means.

Mutual restraint in cyberspace, the most complex domain, should entail a pledge by each country not to be the first to attack networks critical to the other's well-being—that is, "strategic cyberspace." This restriction would not encompass noncritical networks or limit intelligence collection. In the event of armed conflict, both Chinese and U.S. forces are likely to conduct attacks on military networks, the infrastructure for which may also support civilian networks, involving an inherent danger of escalation. Therefore, as a corollary of mutual restraint, both governments bear responsibility to exert tight

political control, not to escalate, and to avoid harm to noncombatants—in effect, to create a firebreak between tactical cyber war, where deterrence may be weak, and strategic cyber war, where it ought to be strong. Only in this way can the utility of military cyber war and the imperative of avoiding general cyber war be reconciled.

Because mutual strategic restraint does not eliminate offensive capabilities—indeed, it assumes their potency—there is no guarantee that it will hold in the event of a Sino-American crisis, much less actual hostilities. Since surprise attacks in any of these domains are improbable, strategic restraint that is doomed to fail in crises is hardly worth having. If either side suspects that the other intends not to exercise agreed restraint at a moment of tension, crises could be all the more unstable. So it is fair to raise concerns about the breaching of strategic restraint. Keep in mind, however, that in all three domains, objective conditions of mutual *deterrence* are either already in place (nuclear and space) or forming (cyberspace). While mutual restraint is superior to simple deterrence because it includes reciprocal acknowledgment and confidence-building, it can be counted on in crises or conflict only if it rests squarely on mutual deterrence based on fear of retaliation.

Obstacles to Establishing Mutual Strategic Restraint

While the United States should take an integrated three-domain approach to mutual strategic restraint, doing so could be complicated and might encounter Chinese skepticism, raise regional concerns, and take patience and persistence. The main obstacles are the potential warfighting utility of different types of strategic weapons, the risks of weakening deterrence by pledging not to escalate beyond conventional combat, allied security and reactions, and asymmetric U.S. and Chinese motivations that might affect acceptance of the concept.

Warfighting Utility. Neither the United States nor China regards nuclear weapons as militarily useful, against each other or in general. China has a longstanding nuclear no-first-use policy, and the United States now seeks to reduce the role of nuclear weapons in world affairs and warfare. Moreover, regardless of whether the two sides agree on mutual restraint, U.S. nuclear attack will be deterred by China's improved retaliatory capabilities, even in the unlikely event that U.S. conventional forces are defeated.

In contrast, ASAT weapons could play a role in Sino-American military combat. The Chinese know that U.S. Armed Forces rely critically on space-based command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR) for operations in the sprawling Pacific, just as the United States knows that the People's Liberation Army's (PLA's) reliance on satellites will grow as it improves its technical capabilities and extends its military reach eastward. Yet because many satellites serve both military and civilian purposes (for example, communications, global positioning, and Earth observation), there is no clear firebreak between tactical and strategic ASAT war. The United States would be better off preserving its own use of space than denying China's during a conflict and thus should rely on ASAT weapons only for deterrence, not warfighting. Given its current conventional military disadvantages and awareness of U.S. military dependence on space, the PLA may hesitate to part with the option of initiating ASAT attacks.

mutual restraint is superior to simple deterrence but can be counted on in crises or conflict only if it rests squarely on mutual deterrence based on fear of retaliation

While deterrence may not apply against many cyber threats—in particular those from nonstate actors—it could be relevant between large and capable states. Due to the limits and costs of network

defense, strategic cyber deterrence between China and the United States is not only necessary but also possible. Because each country relies vitally on vulnerable computer networks, each has reason to fear retaliation. Determining the source of a large cyber attack would be aided by circumstances—such as an ongoing crisis—and by the fact that very few actors, all of them states, are currently capable of large and sophisticated attacks. Even without certainty of an attack's origin, the prospective attacker would be gambling its economic health by betting against retaliation and escalation to general cyber war.

neither the United States nor China can or will exclude attacking computer networks that enable enemy forces and weapons performance in combat

While both the United States and China might be deterred and accept mutual restraint in strategic cyberspace, neither the United States nor China can or will exclude attacking computer networks that enable enemy forces and weapons performance in combat. The PLA knows that U.S. reliance on networked C^4ISR for waging expeditionary warfare and conducting precision strikes is a critical vulnerability. Likewise, the U.S. military knows that the PLA will depend increasingly on systems linked through cyberspace to target U.S. strike forces (for example, aircraft carriers) and so will not want to foreclose cyber attack options in the event of war.

A firebreak between military and civil-commercial cyberspace is theoretically possible. While network infrastructure used in military operations is largely dual-use, it may be possible to discriminate on the software level between military and strategic-civilian programs that use this common infrastructure. Though this would require exceptional network intelligence, precise targeting, and tight command and control, it could prevent escalation to general cyber war without requiring that military cyber attacks be forbidden. Civilian leaders on both sides will need to review military contingency plans carefully to ensure that attacks on military networks do not pose unacceptable risks of escalation to a much broader cyber war.

Maintaining Deterrence in the Region. Mutual restraint, as we propose it, means that neither China nor the United States will attack the other first in any of the three strategic domains; nor will either escalate to strategic attacks in the event of military hostilities. Although it is in U.S. interest to avoid strategic conflict with nuclear weapons or in space and cyberspace, there is some risk that deterrence of Chinese conventional aggression in East Asia could be weakened by easing China's fear of escalation—an effect known as strategic decoupling. Such risks could be aggravated by trends in the Western Pacific conventional military balance favoring China, owing particularly to its expanding conventional missile and submarine forces—also offense-dominant—and its growing ability to strike U.S. aircraft carriers and air bases in the region.

Regardless of agreement on mutual strategic restraint, the U.S. ability to rely on the threat of nuclear escalation to deter Chinese attack on Taiwan is already slight and will decline as China improves its nuclear retaliatory capabilities. While U.S. threats to escalate to attacks on Chinese satellites and strategic computer networks are more credible, the risks and consequences of escalation argue against relying on such threats to deter Chinese conventional aggression. Instead, the United States should strengthen deterrence of Chinese aggression by conventional means—for example, conventional strikes on mainland military (but nonstrategic) targets and bringing U.S. worldwide general purpose forces to bear in a protracted conflict.

If Sino-American relations were to become fundamentally unfriendly, mutual strategic restraint might either break down or make aggression and conflict in the region more probable below the strategic level. As the local conventional military balance shifts in its favor,

China could become more inclined to try to settle territorial disputes on its terms, including over Taiwan, by use or threat of force. However, joint acceptance of mutual strategic restraint could help prevent relations from deteriorating, reduce the likelihood of armed conflict, and make the shifting conventional balance less deleterious to regional security and U.S. interests.

a rising sense of China's own vulnerabilities in space and cyberspace, along with the chance to obtain U.S. acceptance of nuclear no first use, should in time make Chinese leaders more receptive to mutual restraint across all three domains

Protecting and Reassuring Allies. Key regional states, notably Japan and South Korea, may be ambivalent about Sino-U.S. accords on mutual restraint. On the one hand, they do not want Sino-U.S. tensions or an arms race, much less conflict in any of these strategic domains. After all, they share U.S. and Chinese vulnerabilities in space and cyberspace and are part of the same integrated economy. Moreover, U.S. allies should appreciate that mitigating U.S. strategic vulnerabilities could help ensure American steadfastness in the event of any Chinese challenges. On the other hand, Japan and South Korea already are sensitive to signs of reduced U.S. commitment, and they would not want Chinese fear of escalation to be relieved by Sino-U.S. mutual strategic restraint. In the worst case, Japan could be more inclined either to accommodate China or to develop offensive strategic capabilities of its own, neither of which would be good for U.S. interests or regional stability.

The United States can and should assuage allied concerns about its strategic commitments by reaffirming its regional security bonds, maintaining its presence, and improving conventional deterrence capabilities in light of Chinese force enhancements. It should also insist that Sino-U.S. mutual strategic restraint apply to allies, which would mean that China is bound not to attack U.S. allies in any of these domains and, by implication, that the United States would be justified to retaliate in kind if it did. U.S. extended nuclear deterrence of Chinese nuclear threats to U.S. allies would thus be unaffected. Moreover, in ensuring that allies are covered by mutual strategic restraint, and thus by deterrence based on the threat of U.S. retaliation, the approach recommended here would improve allied security against Chinese strategic attack by extending the U.S. strategic umbrella to cover space and cyberspace as well as nuclear attack.

Gaining Chinese Acceptance. It is unclear how fully Chinese leaders comprehend that their country's economic growth and political stability could be endangered by warfare with the United States in space and cyberspace. China, the PLA especially, might want to confine mutual restraint to no first use of nuclear weapons—in effect, to "pocket" mutual nuclear deterrence while keeping open options to strike first in space and cyberspace. A rising sense of China's own vulnerabilities in space and cyberspace, along with the chance to obtain U.S. acceptance of nuclear no first use, should in time make Chinese leaders more receptive to mutual restraint across all three domains.

However, the PLA could see agreement not to initiate attacks on satellites and computer networks as foreclosing China's only way to neutralize U.S. military advantages by degrading U.S. C^4ISR and strike capabilities—and thus, its best chance to avoid defeat. Unless China's political leaders are convinced of the need for mutual restraint and prepared to overrule military objections, the United States may encounter Chinese civil-military discord, stalemate, or opposition regarding restraint in space and cyberspace. China does not yet have fully effective mechanisms for making unified national security policy, as warranted by its expanding interests and role in international security.

The United States can sway China toward acceptance of mutual restraint in space and cyberspace by

having effective ASAT and cyber war capabilities, by making clear its will to retaliate with those capabilities if attacked, and by insisting that nuclear no first use be accompanied by similar restraint in these other two domains. Still, it may be unrealistic to expect China to embrace agreement on mutual strategic restraint, broadly defined, until the reality of growing vulnerabilities fully registers or civilian leaders with a broader conception of China's political and economic interests prevail over the PLA's interest in gaining operational advantages over U.S. forces. One positive side effect of U.S. efforts to engage China on mutual strategic restraint is that it will force Chinese civilian leaders to confront the issue of growing strategic vulnerability in the space and cyber domains and consider whether current military thinking and contingency planning are compatible with China's long-term national interests.[9]

Sooner or later, a clear and comprehensive U.S. strategic deterrent posture, coupled with China's inescapable vulnerabilities, should convince Chinese leaders that their country is in fact deterred in space and cyberspace, just as the United States is in the nuclear domain. The PLA will not have feasible military solutions to address this reality. Recent U.S. policy statements stressing deterrence in these new domains are a good start.

The prospect that initial Chinese resistance will yield to growing interest in mutual strategic restraint argues for the United States to lay out an integrated three-domain approach early in the process. By doing so, it can frame the way the Chinese conceive the strategic vulnerability problem, futility of defense, extension of deterrence concepts to space and cyberspace, and wisdom of general strategic restraint with nuclear restraint as an element.

Building Bilateral Confidence. To buttress and sustain mutual restraint, the United States should propose CBMs in each domain: transparency in nuclear forces and doctrines, launch notification and other forms of space cooperation, and warning of and cooperation against third-party cyber threats. Regular high-level civilian-military dialogue on capabilities, plans, doctrines, and the strengthening of mutual restraint is also essential. Such exchanges will let U.S. policymakers sensitize Chinese counterparts to growing vulnerabilities, the dangers of conflict in space and cyberspace, and the need for effective political control of decisions that risk escalation. They may also provide useful means of managing competitive aspects of Sino-U.S. relations.

While mutual deterrence is a sine qua non of mutual restraint, deterrence by itself may do little more than describe conditions of equilibrium based on presumptions of prudence in the face of retaliatory threats. By institutionalizing those conditions and agreeing on terms, mutual restraint can be more adaptable, enduring, and better for Sino-American relations than threat-based deterrence alone. Deterrence relies on reciprocal fear; restraint adds and fosters shared responsibility and trust. This is more conducive to a bilateral relationship that can tackle the many pressing regional and global issues that can only be addressed through cooperation between the United States and China. By embracing mutual restraint, China and the United States can also place themselves in a position to convince others (for example, Russia) to accept the need for caution in the use of offensive capabilities in all three domains.

Prospects and Recommendations

Agreement with China to exercise mutual restraint across these strategic domains would serve U.S. interests in mitigating critical vulnerabilities, reducing the importance of nuclear weapons, permitting full and productive exploitation of space and cyberspace, and unburdening Sino-American relations of the threat of strategic conflict. Accordingly, the United States should propose such restraint founded on mutual deterrence in all three domains—including reciprocal pledges not to be the first to use nuclear weapons, to interfere with access to space, or to attack the other nation's strategic cyberspace. The United States should insist that these pledges also proscribe such attacks on allies, thus preserving its right to retaliate if an ally were attacked. In light of risks that China might try

Table 2. Levels of Mutual Trust and Cooperation in Strategic Domains

	Nuclear	Space	Cyber
Dialogue	Regular high-level contact to reinforce confidence-building measures, increase mutual understanding of these domains, and address new developments, concerns, and the participation of third parties.		
Confidence-building Measures	Transparency about nuclear doctrine, capabilities, and programs.	Launch notification.	Consultation and cooperation on third-party threats, including criminal. Mechanism for consultation on suspicious activities.
Mutual Restraint	No first use of nuclear weapons against the other.	No first interference with the other's access to space.	No first use against strategic cyber targets (critical networks). Agreement to exercise political control over military cyber operations.
Mutual Deterrence	Because both China and the United States are vulnerable *and* both have extensive offensive capabilities, this creates a situation of tacit mutual deterrence.		
Strategic Vulnerability	Due to the infeasibility of defense, there is no way for either country to reasonably believe that an attack can be stopped.		

to exploit bilateral strategic restraint to seek regional dominance, the United States should state its expectation that such restraint will strengthen prudence and security at all levels.

The framework for integrated mutual strategic restraint that the United States should pursue is summed up in table 2.

It may be neither realistic nor essential to get agreement on all terms soon. Nonetheless, the United States should lay out its complete framework with China, after first consulting with U.S. allies, and then pursue it patiently and persistently. It would be good to share U.S. analysis of common vulnerabilities in space and cyberspace with Chinese counterparts at an early date. The United States could also indicate that it is willing to discuss bilateral no first use of nuclear weapons if China is willing to discuss comparable ideas concerning space and strategic cyberspace. In parallel, the United States should reiterate that its purpose in all three domains is deterrence and that its retaliatory capabilities and resolve should not be doubted.

Regardless of the pace of progress in negotiating terms of mutual restraint, it is important to ensure strong political oversight of operational decisions that could lead to escalation in any of these strategic domains. The United States should update its protocols for delegating authority under peace and war conditions and should implore Chinese civilian leaders to do the same. Strict control is especially important for cyber war, given the relative lack of inhibition to attack.

A framework for mutual strategic restraint should be pursued not with undue urgency, but with patience,

persistence, and conviction that such restraint is right for the United States, for the security of a vital region, and for putting Sino-American relations on a stable strategic footing. Because the United States and China are in a formative stage in what will be the world's most important relationship for generations to come, the United States should not be reactive. The need for the United States to speak with one voice on these matters argues for civilian-military, executive-congressional, and bipartisan discussions. However, even with the need for more debate, there may be no better time than now for the United States and China to start together down a path toward greater safety for themselves and the world.

Notes

[1] Other, "softer" dangers, such as environmental damage, disrupted energy supplies, and turmoil in financial markets, are also exacerbated by interdependence but lie outside the scope of this paper.

[2] David C. Gompert and Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability* (Washington, DC: National Defense University Press, 2011), available at <www.ndu.edu/press/paradox-of-power.html>.

[3] Russia, for instance, is showing renewed interest in nuclear weapons and unabashed enthusiasm for cyber weapons as its inferiority to U.S. conventional military strength grows. In China's case, the appeal of asymmetric capabilities could work against acceptance of restraint in space and cyberspace.

[4] *The New York Times* Week in Review chart, March 3, 2011. Each interceptor costs about $3 million more than each intercontinental ballistic missile (not including development, platforms, support costs, or sensors).

[5] The advantages of offense over defense can be even more pronounced when taking into account measures to "fool" defense—such as with decoys, deception, and computer-network interference—which are easier and cheaper to develop and field than is the improvement or expansion of defense required to neutralize them. On the whole, states that are most capable of fielding large missile forces—such as the United States, Russia, and China—are also most capable of developing and employing countermeasures.

[6] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September–October 2010), 97–108; William J. Lynn III, "Remarks on Space Policy," U.S. Strategic Command Space Symposium, Omaha, Nebraska, November 2010, available at <www.defense.gov/speeches/speech.aspx?speechid=1515>.

[7] Gompert and Saunders.

[8] One reason to expect growing interest in soft-kill antisatellite is the concern about space debris resulting from hard-kill intercept. Another is the potential to evade responsibility for attack.

[9] Gompert and Saunders, chapter 3.

Acknowledgments

This Strategic Forum benefited greatly from research support by Ross Rustici, Roxanne Bannon, and Isaac Kardon, comments by peer reviewers Dr. Jonathan Pollack, Dr. James Mulvenon, and Elaine Bunn, and editorial input from Michael Kofman.

INSTITUTE FOR NATIONAL STRATEGIC STUDIES

The Center for the Study of Chinese Military Affairs (CSCMA) within the Institute for National Strategic Studies serves as a national focal point and resource center for multidisciplinary research and analytic exchanges on the national goals and strategic posture of the People's Republic of China. The center focuses on China's ability to develop, field, and deploy an effective military instrument in support of its national strategic objectives.

INSS
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

NDU Press

The Strategic Forum series presents original research by members of NDU as well as other scholars and specialists in national security affairs from the United States and abroad. The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the Defense Department or any other agency of the Federal Government. Visit NDU Press online at www.ndu.edu/press.

Phillip C. Saunders
Director
CSCMA

Hans Binnendijk
Director
INSS

Francis G. Hoffman
Director
NDU Press