

Executive Summary

The United States and China each have or will soon have the ability to inflict grave harm upon the other by nuclear attack, attacks on satellites, or attacks on computer networks. Paradoxically, despite each country's power, its strategic vulnerability is growing. Particularly since September 11, 2001, Americans have sensed this vulnerability. The extent to which the Chinese sense it is unclear.

Vulnerability to nuclear attack is familiar to both countries. But the United States and China are also becoming exposed to damage in space and cyberspace because of their growing reliance on those domains for their prosperity and security, as well as each side's increasing antisatellite (ASAT) and cyber war capabilities. For China, economic integration, production, and commerce—and thus, sustained growth and perhaps political stability—depend vitally on data sharing, making networks and satellites as strategic as they are for the United States.

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 patently offense dominant because a single explosion can destroy a city. Moreover, it is easier and cheaper for China to improve the survivability of its strategic missile launchers, to multiply 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, 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. 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 state-affiliated Chinese corporations are leading competitors—increasing

the potential for strategic degradation of network infrastructure and disruption of services. In general, strategic offense dominance gives each country an incentive to invest in offense, which in turn spurs the other to keep pace.

Apart from offense dominance, the advance of technology has slashed the costs in lives and treasure of strategic attack, as capabilities have graduated from mass invasion to heavy bombing to nuclear weapons to ASAT and cyber war. If one ignores possible deaths resulting from disruption of public services, ASAT and cyber war might even be considered “nonviolent.” As the number of expected casualties from strategic attack options drops, so could international opprobrium and the inhibitions of decisionmakers. Absent deterrence, thresholds for war in space and cyberspace could become perilously low as offenses improve.

Establishing Mutual Strategic Restraint

Curbing these dangers through Sino-U.S. nuclear, ASAT, or cyber war disarmament is largely impractical and unverifiable. Because of this, along with the futility of strategic defense and the plunging costs of attack, the United States and China must consider ways of mitigating their growing vulnerabilities in these domains by mutual 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 both the United States and China.

Augmenting deterrence, Sino-U.S. mutual restraint should include reciprocal pledges to refrain from attacking first; regular high-level communications about capabilities, doctrine, and plans; and concrete confidence-building measures (CBMs) to provide reassurance and avoid misperceptions. Because China and the United States have both convergent and divergent interests, mutual strategic restraint is both 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 reality 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.

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. 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 would not encompass non-critical networks or intelligence collection. In the event of armed conflict, Chinese and U.S. forces are likely to conduct attacks on military networks, the infrastructure for which may also support civilian networks, involving a danger of escalation. Therefore, both governments bear responsibility to exert tight political control, to not 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 necessitate elimination of offensive capabilities, 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.

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.

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 if U.S. conventional forces may be 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 (C⁴ISR) 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 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 use of space, the PLA may hesitate to part with the option of initiating ASAT attacks.

While deterrence may not apply against many cyber threats, it could be relevant between large and capable states, especially at times of crisis. 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 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.

While both the United States and China might be deterred and accept mutual restraint in strategic cyberspace, neither one 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 C⁴ISR 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 hardware used in military operations

is partly 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 on both sides, it could prevent escalation to general cyber war without requiring that military cyber attacks be forbidden.

Maintaining Deterrence in the Region

Mutual restraint, broadly cast, means that neither China nor the United States will attack the other in any of the three strategic domains; nor will either one escalate to strategic attacks in the event of military hostilities. Although it is in the 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 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.

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. C⁴ISR and strike capabilities—

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 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 until political and economic leaders prevail over PLA interest in gaining operational advantages over U.S. forces.

Sooner or later, a clear 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 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, the reality of offense dominance, the extension of deterrence concepts to space and cyberspace, and the wisdom of general strategic restraint with nuclear restraint as an element.

Building 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. Additionally, regular high-level civilian-military dialogue on capabilities, plans, doctrines, and the strengthening of mutual restraint is 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.

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. By embracing mutual restraint, China and the United States can 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 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.

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 care 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.

This study is not the last word on mutual strategic restraint. Like most research, it ends with an appeal for more work on a number of questions:

- What missile defense capabilities would afford assured protection against small, hostile nuclear weapons states or unauthorized missile launches without raising doubts about Chinese deterrence?
- How can computer networks used for military C⁴ISR be partitioned from those that enable civilian and commercial information-sharing, even with common infrastructure, so that more robust firebreaks can prevent escalation to strategic cyber war?
- What CBMs beyond those proposed here could bolster trust in Chinese and American mutual restraint in the use of offensive capabilities?
- What methods of Sino-American notification of third-party or ambiguous attacks in space and cyberspace could prevent mistakes, miscalculations, and inadvertent conflict?
- What other forms of Sino-American cooperation in space and cyberspace could inculcate a sense of shared interests and complement restraint?
- How could other states, such as Russia, be brought into a regime of mutual strategic restraint?
- How will advances in science and technology affect strategic offense dominance and the logic of mutual restraint?

Even with a need for more study and 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.