January 2012

INSS
INSTITUTE FOR NATIONAL STRATEGIC STUDIES

STRATEGIC FORUM
National Defense University

Raising Our Sights: Russian-American Strategic Restraint in an Age of Vulnerability

By David C. Gompert and Michael Kofman

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. Michael Kofman is a Program Manager and Researcher in CSR.

Key Points

- With the New Strategic Arms Reduction Treaty in place, the United States and Russia should expand negotiations to include cyberspace and space.
- Further, the United States and Russia should agree 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. In view of its NATO obligations, the United States must insist that Allies be covered. Such strategic restraint would rely on mutual deterrence in all three domains, buttressed by cooperative measures.
- By reducing the utility of nuclear weapons and mitigating vulnerabilities in space and cyberspace, mutual strategic restraint would serve U.S. interests, and Russia should be receptive.
- The undemocratic character of Russia's government should not prevent the United States from seeking an understanding that serves its interests, though it will have to be satisfied that its partner is a reliable one.

The United States and Russia have sought to reduce the danger of nuclear war by limiting offensive strategic capabilities through negotiated agreements, relying on mutual deterrence based on reciprocal threats and the corresponding fear of retaliation. Although nuclear arsenals have been pared, this is fundamentally the same way the United States and Soviet Union sought to reduce the danger of nuclear war during the Cold War, when both were impelled to do so because they were adversaries and able to do so despite being adversaries. It is ironic—not to say unimaginative—that although the two are no longer adversaries, they stick to a path chosen when they were. This current approach is inadequate given new strategic vulnerabilities brought on by technological change. Both the opportunity and the need now exist for a different, more ambitious approach to avoiding strategic conflict—one designed for new possibilities as well as new vulnerabilities. The United States and Russia can and should raise their sights from linear numerical progress to qualitative transformation of their strategic relationship.

Accordingly, while not discarding mutual deterrence or nuclear arms control, this paper calls for three basic changes in approach:[1]

- The *scope* of the effort to prevent strategic conflict should be widened to include two additional domains: space and cyberspace.
- The *aim* of the effort should shift from controlling capabilities to eliminating threats and dangers of those capabilities being used.
- The effort's *political premise* should be that because both countries now truly seek a nonadversarial relationship, each can agree not to be the

first to attack the other or its allies in any of these strategic domains.

In brief, the United States and Russia should seek to achieve comprehensive mutual restraint in the use of strategic capabilities. The first half of this paper explains *why* Russian-American strategic restraint is important; the second half explains *how* to structure and achieve it, as well as raising some issues that have to be resolved along the way.

The need to broaden the scope of the effort to reduce strategic risks stems from:

- the large and growing vulnerability of the United States and, in time, of Russia to serious national harm if denied use of space or cyberspace
- the dominance of offense over defense in space and cyberspace, as well as in the nuclear domain
- potentially weak inhibitions against attack in space and especially cyberspace because of modest costs and minimum casualties.

While the destructive force of just a single nuclear explosion need not be detailed here, growing reliance on space and cyberspace is creating vulnerabilities of strategic significance in those domains. To illustrate, table 1 shows an estimate of the economic damage the United States could suffer in important sectors in the event of multiple severe, yet technically feasible, attacks on critical computer networks.[2]

While it is hard to conceive of a wave of cyber attacks that would cause such damage simultaneously in all these sectors, these figures strongly suggest that unrestricted cyber war with a capable state—for example, China or Russia—could have devastating effects on the health of the U.S. economy and the functioning of U.S. society. Although Russia's economy is much smaller than the U.S. economy and Russia's use of computer networking lags that of the United States, Russia can no more afford strategic cyber war than the United States could, especially as its economic and social reliance on networking increases.

The scale of harm from loss of the use of space could be of the same order. The United States and Russia depend on satellites for crucial purposes such as voice and data links, global positioning and navigation, violent weather preparedness, resource discovery and management, strategic warning, routine intelligence, and military operations. Wherever telecommunications landlines are infeasible, uneconomic, or inadequate, movement of information for all of the sectors in table 1 transits space. The first sentence of the U.S. *National Security Space Strategy* states that access to space is *vital*—a term with obvious (no doubt intended) strategic connotations.[3]

For both countries, all three strategic domains have in common the dominance of offense over defense—technologically, economically, and operationally.[4] Defenses against nuclear, antisatellite (ASAT), and cyber weapons are technologically unpromising, yield diminishing returns on investment as offensive capabilities are increased or improved, and cannot prevent grave harm from attack by large, able, and determined states, including the United States and Russia.[5]

Nuclear weapons are offense dominant because of both their destructive force and the difficulty of intercepting missiles in flight, particularly if a missile arsenal is large in number and equipped with countermeasures. Figure 1 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]).[6] If each interceptor cost the same as each ICBM, each ICBM carried one warhead, and it took only one interceptor to destroy each ICBM, the relationship between offense and defense would be 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 independently targetable reentry vehicles, the cost gap is even worse

Table 1. Preliminary Estimates by U.S. Cyber Consequences Unit

Sector	Estimated Cost (Billions USD)
Electric power	300–400
Oil and gas	100–400
Telecom/Internet	400–700
Banking and finance	900–1,300
Water and sanitation	100–100
Chemical industries	300–600
Air transport	100–300
Ground transport	300–600
Health care	1,000–2,200
Total	3,700–6,900

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), 119.

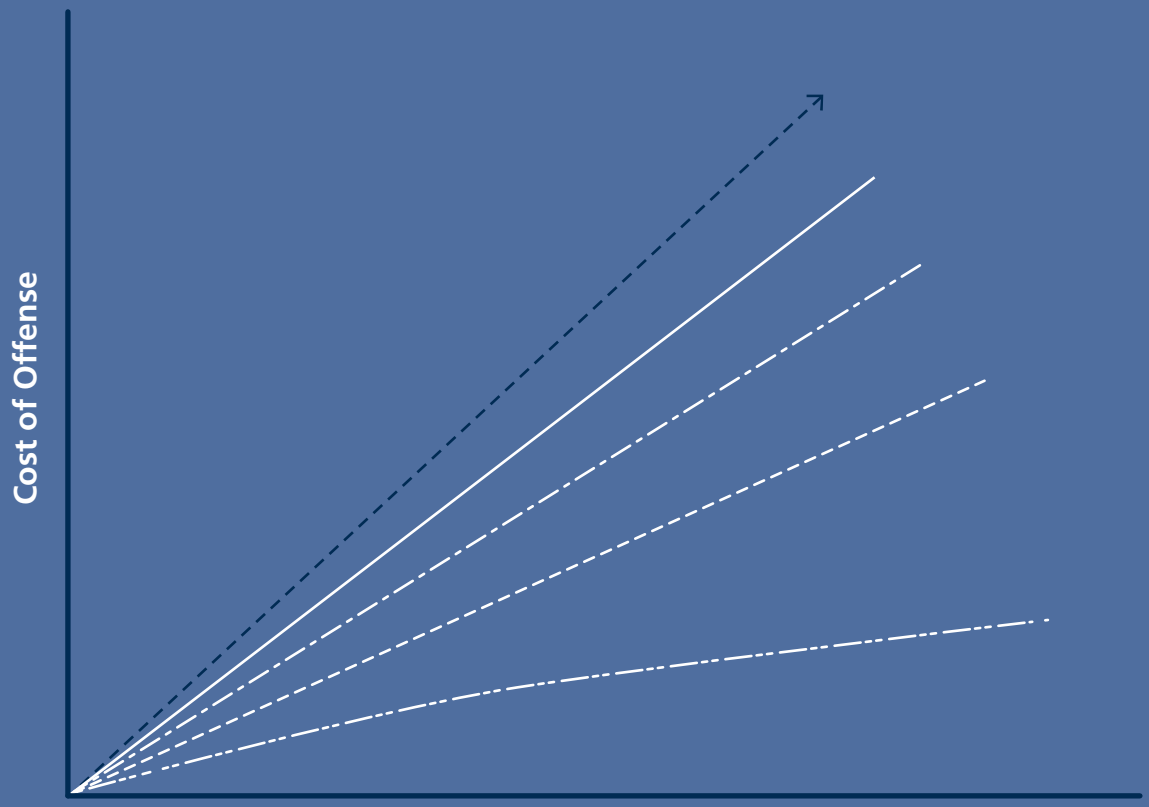
for defense—the next line down. In reality, it takes more than one interceptor on average to destroy an incoming missile—the next line shows the cost gap if it takes on average two interceptors to destroy each incoming missile. Moreover, the odds of intercepting a missile worsen as the size of an attack 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 in figure 1, which indicates the added cost of interceptors required in response to a substantial increase in the scale of attack. 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.[7]

In sum, missile defense may work, and be worth the cost, against small, simple threats like Iran, but not against large, complex, and sophisticated ones like Russia.

The plain and persistent dominance of nuclear offense over defense is germane to the prospects for U.S.-Russia strategic restraint in this domain, since any advantage of using nuclear weapons first is negated by the futility of defense and exposure to retaliation. Although the Russians worry about U.S. ballistic missile defense (BMD), the United States would need to massively increase its commitment to this capability—far beyond what it takes to defend against the likes of Iran and North Korea—to be able to destroy an entire Russian retaliatory attack, especially if Russia were to introduce measures to defeat defenses.[8] There are no signs that U.S. leaders, defense planners, or taxpayers are prepared to make such a commitment, especially in light of much higher U.S. defense priorities, such as in the Middle East and East Asia, and the need to cut defense spending.[9] Yet despite the continued dominance of offense in the U.S.-Russia nuclear relationship, the Russians oppose U.S. BMD—above all NATO BMD near Russian territory from which Russia is excluded (a pivotal issue to which we will return).

Satellites, being conspicuous, targetable, and fragile, are inherently vulnerable. Destroying or disabling them is easier and cheaper than protecting them.[10] Moreover, as figure 2 shows, ASAT interceptors cost a small fraction of high-value satellites, giving offense a huge potential advantage.[11] Some degree of space security can be gained through redundancy, but replicating satellites is

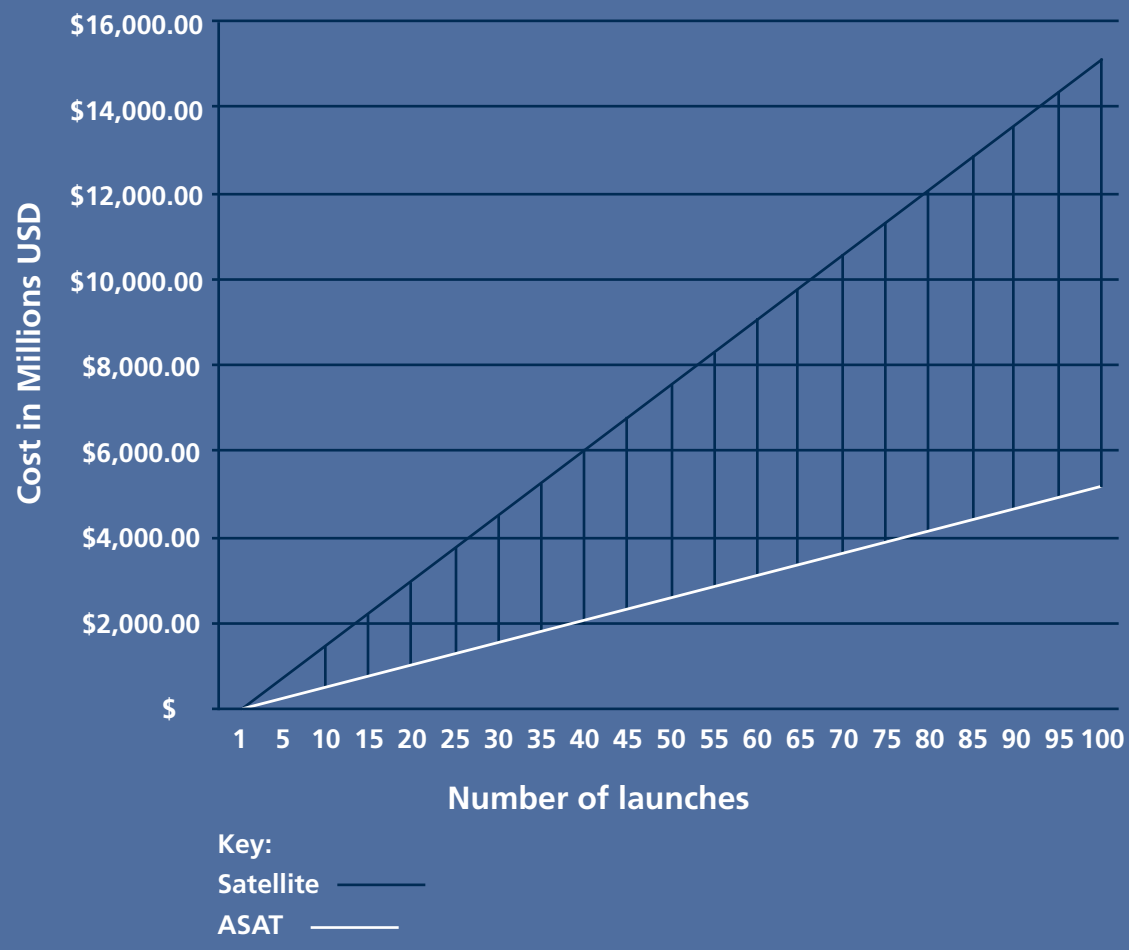
Figure 1. Cost of Offense Dominance in Missile and Intercept Systems



far more expensive than multiplying interceptors, each of which can rely on a common targeting system.

Likewise, defending computer networks gets harder and more costly as the scale and sophistication of the attacker and the attack increase. Networks designed to facilitate access, sharing, collaboration, and new applications are in great demand and deliver significant economic benefits but also are inherently hard to secure. Efforts to defend them yield diminishing returns against increasingly capable cyber attackers. Figure 3 depicts a widely accepted model of the benefit of investment in defense in terms of prevented economic losses from attack.[12] The diagonal line represents that an increment of investment in defense will prevent an equal increment of loss from attack; the curved line represents the amount of prevented loss that can be *expected* for every increment of investment in defense. It shows that network defense pays

Figure 2. Cost Per Launch

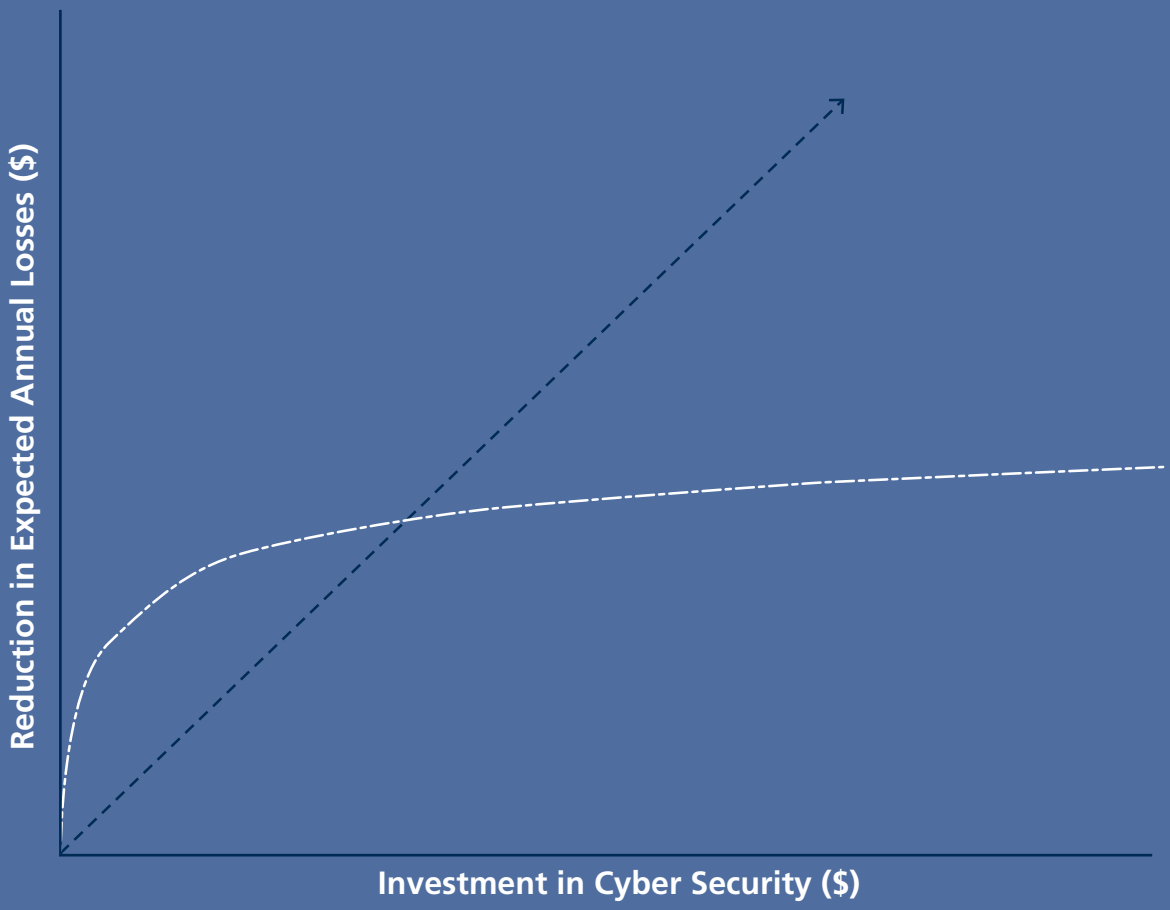


off well against threats of relatively modest losses but then offers declining benefits relative to the investment required. While the model is meant for corporations, the underlying logic and technical relationships can apply no less to other large enterprises, including governments. After decades of expanding work on defenses, computer networks are, on balance, *less* secure from those who would enter, corrupt, rob, and degrade them.

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.[13] 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.

In all three strategic domains, defenses may be effective, economic, and justified against little and simple threats but not against big and complex ones from such well-resourced actors as the United States and Russia.

Figure 3. Diminishing Returns on Investment in Cyber Security



Offense dominance thus increases the incentives of each competing side to invest in offense, which in turn stimulates the other to keep pace. Accordingly, the United States and Russia will likely maintain large and modern strategic nuclear forces and continue to improve cyber warfare capabilities. The United States is developing, and Russia may try to develop, a set of ASAT capabilities, both "hard kill" (for physical interception) and "soft kill" (for performance degradation). Although Russia does not currently have an operational ASAT capability, it has the technical competence and economic resources to acquire one, against which defense of U.S. satellites would be difficult.[14] In general, neither country can be confident of its ability to field adequate defenses against attack by the other in any of these strategic domains. Neither one can buy and build its way out of its vulnerability to the other.

Besides causing offense dominance, the advance of technology has dramatically cut the costs in lives and treasure of strategic attack to bring about an enemy's capitulation—from mass invasion, to heavy bombing, to nuclear weapons, to space and cyber war. Table 2 shows the decline in the costs and casualties of strategic attack with the advance of technology, 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).[15]

Unsurprisingly, technology is making strategic attack less costly and less bloody. As vulnerability is increasing, means of attack are being refined. The most

Table 2. 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.

striking decline is in casualties—those of the attacker as well as of the attacked—from millions to virtually none.[16] Taking into account only the immediate effects of disabling satellites and computer networks, they could even be considered *nonviolent* strategic attacks—notwithstanding the devastating ensuing effects (and even loss of life) they could cause. 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 may be shifting 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 main reasons to concentrate on restricting the *use* of capabilities are the difficulty and limited value of controlling capabilities in these domains. The danger of a U.S.-Russia nuclear arms race is now negligible; if anything, both will continue to trim their offensive forces to save money. At the same time, substantially deeper negotiated reductions in Russian and U.S. nuclear forces are obstructed by Russian concern about U.S. missile defense, by U.S. concern about Russian tactical nuclear weapons, and by mutual concern about other large nuclear powers, notably China.[17] Even if deeper cuts were made, they would not in themselves reduce the risk of nuclear war.[18]

Meanwhile, trying to limit or ban ASAT capabilities would founder on problems of definition and verification, as well as the need, at least for the United States, for ASAT capabilities to deter Chinese ASAT attack. ASAT missiles are not readily distinguishable from missiles with other missions. The problems with ASAT arms control are compounded by the advent of soft-kill ASAT, whereby directed energy and electronic attacks can degrade performance (denying use of space without physical destruction of satellites).[19] It is not possible to monitor and control such capabilities with any confidence.

If arms control is difficult in the case of ASAT weapons, it 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. In sum, for cyberspace as well as space, restricting use is far more promising than attempting to restrict capabilities, while in the nuclear domain further efforts to reduce numerical ceilings on missiles and

weapons will neither be easy nor reduce the risks that nuclear weapons will be used.

Finally, the idea that the U.S.-Russia strategic relationship should be brought into line with nonadversarial relations is as important as it may be self-evident. Strategic capabilities and concerns aside, Russia and the United States find themselves increasingly on the same side in confronting global security challenges: dangers from the spread of nuclear weapons, instability and terrorist threats emanating from the Middle East and South Asia, disequilibrium in East Asia because of China's rise. U.S. efforts to improve relations with Russia—trademarked as the "reset"—and Russian receptivity to this effort reflect not merely an urge for friendship but a converging of concrete objectives. The United States and (as we will argue) Russia increasingly take a hard-nosed view that the other can be instrumental in protecting and advancing practical interests. The era of organizing their relationship on the basis of threat and competition with each other is giving way to one shaped by the utility of cooperation.

While U.S.-Russia relations as a whole have been through a revolution since the Cold War, the U.S.-Russia strategic relationship has barely evolved. Again, the primary way of avoiding nuclear war has been mutual deterrence based on credible threats of retaliation and fears of destruction. While deterrence will last to some degree as long as the United States and Russia have nuclear weapons, the two now can and should affirm that threats, aggression, escalation, and strategic war have no place in the kind of relationship both countries claim to want. Thus, the absence of any rationale for nuclear attack will allow dependence on threats and fears of retaliation to recede.

This paper coincides with a political chill in Russian-American relations, at least on the U.S. side. Russia's flawed parliamentary election of late 2011, triggering paroxysms of public anger—possibly lasting and expanding—about growing authoritarianism, confirm that politics within Russia are not just unsavory but also unsettled. In turn, American dislike for the Russian state limits what the U.S. Government can or would want to do to improve U.S.-Russia relations, especially if it means counting on the Kremlin as a worthy security partner. Therefore, any new U.S. initiatives to mitigate strategic dangers must either be tempered by politics or else be so clearly advantageous for the United States that the character of the Russian state should be effectively ignored (as was the case in U.S.-Soviet arms control). A presumption of this paper is that a new approach to managing Russian-American strategic relations holds sufficient promise for U.S. interests that it should be pursued despite the undemocratic instincts and practices of Vladimir Putin and his ilk. The United States does not need to admire Russian governing elites in order to see merit in eliminating the danger of strategic conflict or to enlist Russian cooperation in blocking the spread of nuclear weapons. Still, before the United States enters into any new strategic agreements, it will have to be satisfied that its partner is a reliable one, as well as that entering into such agreements would not reward and strengthen undemocratic forces in Russia.

Politically, mutual strategic restraint can both contribute to and benefit from a genuine normalization of U.S.-Russia relations. American and Russian publics are more likely to accept and support a cooperative relationship if the specter of nuclear war has been erased. Strategically, the United States can accept mutual strategic restraint because it has military superiority across the board. Yet mutual restraint is also in Russia's interest because conflict of any kind with the United States would end in disaster.

Even as the United States and Russia develop a nonadversarial relationship, mutual deterrence remains a sine qua non of mutual strategic restraint. This relationship carries heavy baggage: lingering distrust born of old antagonism, plus fresher post–Cold War suspicions—on Russia's part that the United States has exploited Russian weakness, and on America's part that Russia still covets remnants of the Soviet empire. Moreover, the strategic nuclear forces of each are still structured—if largely from inertia—to deter the other (though this is gradually changing because of proliferation and the growth of Chinese capabilities). In time,

reliance on mutual deterrence based on threat and fear should wane as benefits and habits of cooperation make mutual strategic restraint the natural new norm. Meanwhile, agreeing on such a norm would contribute to the pace and irreversibility of a nonadversarial general relationship—all the more reason to pursue agreed strategic restraint, starting now. While mutual deterrence is now indispensable for mutual restraint, the importance of deterrence could decline as relations improve and mutual restraint becomes natural.

Even as the danger of nuclear conflict between Russia and the United States is declining, new vulnerabilities have arisen because of the criticality of space and cyberspace and the dominance of offense in both domains. The premise that any thought or threat of strategic attack would contradict the kind of relationship sought by both countries should apply to the use not only of nuclear weapons but also of ASAT and cyber weapons. Again, these weapons can produce grave harm, yet inhibitions against using them may be much weaker than with nuclear weapons. Moreover, failure to understand the full consequences of using counterspace weapons or large-scale cyber attacks may increase the risks of escalation in these new domains.[20]

Finally, NATO's core principle of indivisible security requires the United States to insist that mutual strategic restraint apply no less to its Allies than to itself. This means, in essence, that Russia would have to pledge not to use nuclear, ASAT, or cyber weapons first against any member of NATO, and that the United States would be justified in retaliating in kind if it did. Alliance considerations are key to the design, negotiation, and success of U.S.-Russia strategic restraint, and we will return to this point.

American and Russian Interests in Mutual Strategic Restraint

Based on this analysis of vulnerabilities and opportunities, the United States should seek agreed mutual strategic restraint with Russia to prohibit initial use of nuclear weapons, initial use of ASAT weapons, and initial attacks on critical computer networks, to include Allies. The reasoning behind prohibiting *initial use* of such strategic offensive capabilities could not be simpler: the less the danger of initial use, the less the danger of strategic conflict. While retaliatory capabilities would remain, to ensure deterrence, there would be no occasion to use them. Although elimination of the dangers of strategic war between the United States and Russia is not immediately realistic, it should be a stated goal of U.S.-Russia mutual strategic restraint. Ordinary Americans, Russians, and people everywhere can grasp what such a commitment means.

Agreement on strategic restraint would advance a number of key U.S. interests:

- further reducing the role of nuclear weapons in war and international politics
- improving Russian alignment with American efforts to counter the spread of nuclear weapons to hostile states, starting with Iran and North Korea
- reducing the danger of cyber attack by Russia
- reducing nuclear and cyber dangers to NATO Allies
- discouraging Russia's interest in developing an operational ASAT capability
- setting a standard for strategic restraint that could apply also to China, especially in regard to cyber war and the use of ASAT weapons
- creating better conditions for development of U.S.-Russia relations in ways that serve U.S. international objectives
- setting the stage for deeper cuts in nuclear forces down the road.

This article was written with U.S. interests foremost in mind, but because mutual restraint requires Russia's agreement, these ideas are tested against an analysis of Russia's interests.[21] On the whole, Russia should and likely would look favorably on a fair U.S. proposal to improve strategic relations and mitigate growing vulnerabilities.

But this depends largely on the wrenching problems and tough choices Russia now faces.

Russia's leaders, including once and future president Vladimir Putin, face certain inescapable realities: Russia's political-economic system is too dependent on high energy prices, it has entered a stage of diminishing returns, it cannot keep up with external stresses (global competition, Islamist extremism, China), its human capital is wasting, and its critical condition dictates consideration of major course corrections. The course Russia's leaders choose, internally and internationally, will affect their interest in U.S.-Russia relations in general and mutual strategic restraint in particular.

While some Russians may still prefer their country to pose as a global power, there is a growing recognition that Russia should concern itself less with its relative standing and more with its real interests, including pressing national difficulties. The economy must be made less dependent on the extraction and export of energy and raw materials, which has relegated Russia to the role of a source of resources for more productive countries. Instead, the economy should leverage and develop Russia's human talent, diversify, and become attractive to investment in value-added production that is integrated into the world economy and not plagued with corruption.

In parallel, Russia's national defense must become lean, economical, knowledge-based, professional, technologically adept, and suitable for responding to actual security risks. Russia's military forces must be able to operate effectively in local and diverse contingencies along and within its borders. Meanwhile, the growth of Chinese power in East Asia requires a response that will safeguard Russian interests without causing Sino-Russian antagonism. Finally, having recently witnessed Iranian perfidy regarding nuclear capabilities, Russians now realize that Iran cannot be trusted with nuclear weapons, and the danger of an Iranian missile force has begun to rear its head.

Increasingly, Russia's elites see that these challenges demand sweeping economic and military reforms. While the latter has begun in earnest (after many false starts), the former has been mainly lip service. Both economic and military reform would be facilitated by, as well facilitate, greater economic and technological cooperation with the West. Meanwhile, Russia's security establishment now recognizes that a conventional conflict with the West is unlikely, and future threats will instead emanate from its periphery and the Far East. The fact that NATO, but not China, is named in Russia's official statements as a potential danger is due to the reluctance to delete an old adversary and to name a new one. In this regard, Russia's official documents lag Russian thinking.

Given Russian requirements for internal reform, and a shifting perception of external threats, Moscow could see the advantage in having productive relations with the United States and its allies. After all, the United States is as concerned as Russia with threats of Islamist violence and China's growing power. At the same time, Russians observe American and European mounting debt, stubborn unemployment, political gridlock, and declining defense spending—further evidence that the Atlantic Alliance is not an actual threat to Russia.

In recent years, Russia's policy has evolved from fearing and opposing Western security arrangements to wanting to work with them—a trend that may become more pronounced as Russia contemplates its actual near-term security problems in the South and long-term security problem in the East. Russian sentiment toward NATO has shifted from hostility to disappointment. NATO has moved nearer geographically, through expanded membership and military infrastructure, yet has held Russia at arm's length strategically. Russia's frustration over exclusion from Western security arrangements will become deeper as its interest in cooperation becomes stronger. This, more than Russian fear of a U.S. nuclear threat, lies at the heart of the controversy with NATO over BMD. Conversely, progress toward Russia's inclusion in BMD could open the way for a more cooperative relationship and toward mutual strategic restraint.

This analysis of Russia's interests reflects both the logic of its predicament and the drift of public opinion.[22] Russian debate about domestic and foreign policies may not be entirely settled, but reality is constraining Russian options.

Still, with another lengthy Putin presidency looming, it is not unreasonable to question whether Russia will in fact alter its course—whether it will, under his leadership, enact genuine reform domestically and seek a closer relationship with the United States and its allies. Given Putin's popularity, power, and instincts, he and his inner circle may decide to maintain the status quo and select not to pursue energetically either reform or closer ties with the West. This, in turn, could diminish Russia's receptivity to a U.S. proposal for comprehensive mutual strategic restraint.

However, several factors suggest that the next Putin presidency will permit if not champion change in Russia:

- Evidence that Russia's economy, absent reform, cannot produce steady progress in competitiveness and living standards is now irrefutable. However powerful and popular, office holders who ignore this evidence will lead Russia and Russians further into dependency on resource exports, declining standards of living and economic opportunities, and public disaffection.
- While Putin himself may not favor reforming and reorienting Russia, he will likely and increasingly be surrounded by and be reliant on officials, bureaucracies, experts, opinionmakers, and business executives who do—including foreign investors and financial institutions.
- Regardless of what is in his famous "soul," Putin has displayed an ability to sense the practical dangers and opportunities facing Russia and to play the role of change agent in order to succeed in leadership. He is no captive of the status quo, which he largely created and has the power to change. Putin will understand that a failing Russia would preclude a successful presidency.

Even without embarking on major internal reform, Putin should recognize that a more cooperative relationship with the United States serves the interests of Russia and its leader. Although Russians remain wary of the United States, perpetuating and accenting American-Russian differences is no longer the formula for political advantage it once was. Meanwhile, China will present a growing contrast to Russia and a potential challenge to its interests and influence—a prospect no leader can dismiss. This will argue in favor of giving U.S. proposals for mutual strategic restraint a fair hearing. More than that, such U.S. proposals could signal that security cooperation with the United States and NATO is not only desirable but possible for Russia.

In sum, while far from certain, the authors foresee growing Russian acceptance of the imperatives of reform, integration, and cooperation with the West. Indeed, many Russian elites already see their current political system as unresponsive and the economic system as unsustainable. The growing budget deficit continues to drive this point home in Moscow. While the next president of Russia may or may not embrace this view, resisting those who do embrace it could lead to more primitive politics, domestic discontent, and instability and, in response, draconian rule. In contrast, the opportunity to join the United States in an ambitious new effort to eliminate the dangers of strategic conflict would refresh Russia's international image as a progressive and significant power—and Putin's image as a global mover and shaker.

Agreed mutual strategic restraint with the United States would not only serve Russia's political purposes but also mitigate growing Russian vulnerabilities. As economic and military reforms are pursued, Russia will become more successful in and reliant on information networking and the use of space. Table 3 shows the level and growth of American, Russian, and Chinese per capita Internet use. Note that Russia's use is presently at the same level as China's in 2008–2009 but is growing much more slowly—a result not only of China's faster economic growth but also of its more complex, integrated, and production-oriented economy.

If and as Russia's economy is reformed, oriented toward value-added production, and integrated internally and externally, growth should accelerate in the use of computer networking and related use of space. Russia's urban society and business class are already dependent on the Internet for daily life, and its government is increasing the use of cyberspace for provision

Table 3. Estimated Internet Users by Country (per 100 Inhabitants)

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
China	1.78	2.64	4.60	6.20	7.30	8.52	10.52	16.00	22.60	28.90
Russia	1.98	2.94	4.13	8.30	12.86	15.23	18.02	24.66	26.83	29.00
United States	43.08	49.08	58.79	61.70	64.76	67.97	68.93	75.00	74.00	78.00

Source: United Nations ITU World Telecommunication/ICT Indicators Database

of traditional services to the public. Russia also aspires not only to remain competitive as a provider of space services but also to increase its use of space for commercial and military purposes, as evidenced by its high hopes for establishing the Global Navigation Satellite System for commercial and military use.[23]

Military reform, which is under way but has far to go, will pattern Russian forces after the light, fast, networked style of operations and types of capabilities Western forces now stress. (Development of such forces is further evidence that Russia does not foresee much likelihood of conflict with NATO, just as NATO does not see much likelihood of conflict with Russia.) The need for rapid deployment, integration, and efficient logistical support corresponds to limited but intense operations on Russia's periphery. With these capabilities will come growing dependence on advanced command, control, communications, computers, intelligence, surveillance, and reconnaissance networks—largely space-based, given Russia's sprawling territory. While such capabilities are far more useful for Russia than old-fashioned mass-mechanized forces, they will result in greater vulnerability to cyber and ASAT attacks.

Thus, as Russian economic and military reforms gain strength, so should Russian interest in avoiding conflict in both space and cyberspace. At the same time, Moscow's interest in waging cyber war will be checked by its vulnerability and fear of retaliation. As for preserving Russia's option of first use of nuclear weapons, it is neither credible, given U.S. deterrence, nor helpful, given the desire for improved relations with the West. While the Russians are not prepared to say so, the option of nuclear first use is more relevant to increased fears of China than to decreased fears of NATO.

In sum, there should be a general and growing interest on both sides in mutual strategic restraint. At the same time, American and Russian situations and views differ sharply across the three domains:

- Russia's conventional military weakness has made the country more interested and the United States less interested in reserving the option to use nuclear weapons first.
- The United States is more reliant on space and therefore potentially more vulnerable than Russia to denial of access to space, though the United States has and Russia lacks ASAT capabilities.
- Likewise, the U.S. economy and military rely more on computer networking than Russia's economy and military do; and while the United States has better cyber war capabilities, Russia also possesses and has used such capabilities.

These asymmetries suggest that it could prove difficult to reach agreement on mutual restraint if pursued

along separate and independent tracks. As well, the United States might need to persuade Russia that particular terms of mutual restraint are tied to a broader and fundamentally political commitment to bring strategic relations into line with the goal and growing reality of a nonadversarial, jointly productive relationship.

Terms of Mutual Strategic Restraint

Under such conditions, the United States should propose an *integrated approach*—a package deal—to mitigate nuclear, space, and cyberspace vulnerabilities through agreed mutual strategic restraint. The approach should rest on three pillars: the belief that strategic relations should reflect nonadversarial relations; the fact that conditions of mutual deterrence exist and will persist in all three offense-dominant domains; and the need to redirect the American-Russian strategic agenda from the dangers of each other to the dangers of proliferation and other converging concerns.

The terms of mutual restraint that should interest the United States include:

- an exchange of nuclear no-first-use (NFU) pledges
- agreements to develop a joint BMD system and to take other strong joint measures against hostile nuclear states
- pledges not to be the first to interfere with the other's use of space
- pledges not to initiate attacks on computer networks critical to the other's national economic and societal well-being
- application of all terms of restraint to allies
- measures to boost confidence that the terms will be honored.

The essence of mutual nuclear restraint would be American-Russian agreement that neither state would start a nuclear conflict against the other or its allies. Having once expressly reserved the option to use nuclear weapons first if conventional defense proved inadequate against massive Soviet aggression, the United States no longer needs to confront Russia with such a threat. With its aim of reducing the role of nuclear weapons in mind, the United States has stated that it intends to work toward conditions in which the sole purpose of nuclear weapons is to deter nuclear attack.[24] A nuclear NFU agreement with Russia would be an important, even dramatic step in that direction. If Russia used nonnuclear weapons of mass destruction, such as biological weapons, against U.S. forces or Allies, the United States would have unassailable grounds for declaring its nuclear NFU pledge—indeed, all terms of mutual restraint—nullified by such a horrific Russian act.

Nuclear NFU should be negotiable on its own terms and in keeping with Russia's (presumed) growing interest in a fundamentally nonadversarial relationship. Russia's nuclear posture now states that it would use nuclear weapons first only if "the very existence of the state is under threat." This constitutes a raising of the threshold for Russian nuclear first use and a more restricted approach compared to the previous policy.[25] Surely informed Russians know that the United States and NATO will not threaten Russia itself, except in the extreme case of a Russian attack on NATO. If Russia were to attack a NATO member, it would invite not only defeat but also the possibility of a direct threat to itself, with or without agreement on nuclear restraint.

With the desire to move closer to the United States and its European allies, and the offer of a reciprocal and contingent U.S. NFU pledge, Russia would have nothing to lose and much to gain by accepting such an offer. Russia does not need a nuclear first-use option to be safe from NATO attack. While Russian generals fear that their conventional forces could be defeated in the event of hostilities with NATO, the idea that the Kremlin would start a nuclear war in that instance ignores two important facts. First, the survival of the Russian state would not be threatened by NATO even if its forces were beaten. Second, if Russia used nuclear weapons first, NATO retaliation would be devastating—indeed, the only plausible NATO threat to the Russian state's survival would be the result of Russia's first use of nuclear weapons.[26] Russia's agreement to nuclear

NFU would signal its commitment to a lasting nonadversarial relationship with the United States. Conversely, for Russia to reject such an understanding would raise doubts about the value of mutual restraint in *any* strategic domains. For both countries, a nuclear NFU pledge would also signify a transformation of the strategic relationship.

Agreement to pursue a joint NATO-Russia BMD system would fit with a nuclear NFU agreement:

- Logically, if both states commit not to use nuclear weapons first, including against allies, it follows that the United States would not have reason to anticipate either a Russian first strike or a Russian retaliatory strike. (Under conditions of mutual restraint, U.S. confidence in Russia's compliance would be undergirded by deterrence and bolstered by confidence-building measures, as addressed below.)
- Strategically, both states could turn their full attention, including cooperative BMD, to the gathering danger of nuclear proliferation, especially the Iranian missile threat. Russia's inclusion in BMD would give substance to U.S. insistence that Russia should be more concerned about Iranian nuclear intentions, which NATO's current position tends to contradict by denying Russian participation in a joint system. Because it is unable to build a complete BMD system of its own, the alternatives for Russia are to participate in a joint system or be largely unprotected as Iran expands its missile force and acquires nuclear weapons.
- Politically, the combination of NFU and Russia's inclusion in NATO BMD would take NATO-Russia cooperation to a new level. It would also send an unmistakable signal that both Russia and the United States, along with their allies, are more concerned about the threat from Iran than from each other.

NATO-Russia joint BMD would, of course, have to leave NATO no less secure and if possible more secure from an Iranian missile attack. While Russia lacks a suite of advanced warning-and-tracking sensors like those of the United States, it does have well-placed radars. If data from both NATO and Russian sensors were fused and shared, by definition both would benefit. Further, if both NATO and Russia relied on their own interceptors, by definition neither would be disadvantaged nor dependent on the other to destroy threatening missiles.[27] While NATO could benefit somewhat from such a joint arrangement, Russia could benefit greatly, for it lacks the means to build a complete system on its own.

The Russians are coming to appreciate that NATO BMD is designed against Iranian missiles, not theirs. Still, they worry that the system could someday be expanded or reoriented in a way that would weaken Russia's intercontinental deterrent, such as by placement of interceptors in Europe's northern waters.[28] The best way for Russia to guard against such an improbable development is to participate in a joint NATO-Russia system.[29] Given the political benefits of joining a major Western security initiative and the security benefits of defense against Iranian nuclear-armed missiles, Russia should seize the opportunity to participate in the NATO system.[30] For the United States, Russia's participation in joint BMD would facilitate agreement on strategic restraint, strengthen cooperation on nuclear proliferation in general and stop Iran in particular, and encourage the sentiment in Moscow that Russia should reorient toward the West.

In regard to the use of ASAT capabilities, the United States has less to gain by reserving the option to attack Russian satellites than by establishing an international precedent with Russia that unhindered access to space will be respected. While Russia does not have an operational ASAT capability, it might be dissuaded from acquiring one and would be prohibited from using it first if it were to acquire one. Both "hard" and "soft" interference with space systems must be precluded in order to discourage development of offensive capabilities that may be used.

U.S.-Russia agreement not to initiate attacks on the other's critical computer networks would ease U.S. and Al-

lied concerns with Russia's growing interest in cyber war capabilities and operations. Such agreement would require agreed definitions of both "attack" (which would not include intelligence gathering) and "critical" (which would not include entertainment and the like). Recently, American and Russian experts have made progress on a common terminology in the cyber realm, the first step toward such an understanding.[31] While it would require the United States to forego attacks on critical Russian networks, U.S. conventional military advantages and the risk of Russian cyber retaliation make this option neither essential nor attractive. To have integrity, the understanding on cyber war would need to cover attacks that originate in either country even if not by or at the behest of the state. Not to do so would be to create a tempting loophole and to concede that sovereigns are not responsible for preventing attacks on other states from their jurisdictions. Because total compliance with this standard is impossible—hacking being impossible to stop—agreement on this would signify a commitment to collaborate against third-party threats, including within each country.[32] It should be understood that third-party attack, unless instigated by government, would *not* justify retaliation against the other state or its critical networks.

The United States (and Russia) would retain the option to attack networks that enable enemy combat operations. Therefore, there would have to be an additional understanding that any such wartime actions would be strictly controlled by political authorities and kept from escalating to strategic cyber war on networks critical to each other's economies and societies. In any case, with the risks of American-Russian armed conflict declining and the strength of deterrence based on the threat of retaliation, cyber war as an extension of military combat is increasingly unlikely.

As in the nuclear and space domains, mutual cyber war restraint would depend on mutual deterrence. While there is an active debate on the applicability of deterrence theory to cyber security, there are reasons to believe that the prospect of severe retaliation can and will deter strategic attacks on critical networks by large and capable states, which are themselves vulnerable (for example, Russia, the United States, and China).[33] While certainty about the identity of an attacker may not be possible, there are only a few "high-end" candidates, and circumstantial evidence (for example, the existence of a crisis or conflict) may be strong. Moreover, for deterrence to work, the standard is not certainty of retaliation but a high enough likelihood to give a would-be attacker pause. Now that the U.S. Government has stated, in effect, that a cyber attack on itself or an ally would be taken as an act of war and grounds for retaliation, Russia has reason to fear for its own vulnerable networks before acting.[34] Deterrence may not work against many cyber attackers, but if it can work in the U.S.-Russia case, it provides a basis for agreed mutual restraint.

While American and Russian positions differ from domain to domain, there is something for each in this entire package of restraints. The primary specific benefit for the United States would be Russia's agreement not to initiate attacks on critical computer networks, given U.S. vulnerabilities and Russian capabilities. The United States would also benefit from the chance to lock Russia into an active collaborative strategy to counter nuclear proliferation, starting with Iran. The primary specific benefit—and quid pro quo—for Russia would be its inclusion in NATO BMD (as described earlier). Russia's international stature would also receive a needed boost by virtue of joining the United States in a major initiative to lessen the risks of strategic conflict. Over time, both would benefit from the mitigation of mutual vulnerabilities in space and cyberspace, from the contribution of such agreements to U.S.-Russia relations, and from having created more conducive conditions for further nuclear arms reductions down the road.

As to negotiability, given its conventional military shortcomings, Russia may be hesitant to give up nuclear or cyber first-use options. However, Russia is confronted with strong deterrence in both domains, with or without agreement on mutual restraint. While nuclear weapons and cyber war may be theoretically interesting offsets to Western military advantages, for Russia actually to escalate in either domain would be to invite catastrophic retaliation.[35] Moreover, by insisting on an integrated approach, pursuant to the "reset" in U.S.-Russia relations, the United

States would give Russia an incentive to accept even those terms about which it might be ambivalent. Establishing an understanding on NFU would alleviate Russia's growing insecurity in space and cyberspace, where rules have yet to be established, and where it continues to view itself as considerably less capable than the United States.

The U.S.-Russia understandings proposed here might be taken as unfriendly by China, yet they also provide an incentive for the Chinese to consider such mutual strategic restraint with the United States (and perhaps Russia). The Chinese already espouse nuclear NFU, consistent with their doctrine of minimal deterrence, and would welcome American and Russian reciprocity. What both the United States and Russia have more to worry about is the interest of the Chinese military in ASAT and cyber war capabilities, possibly to include initial use. Added pressure on China to exercise or pledge restraint in these domains would be a collateral benefit for both Russia and the United States. In any case, Chinese policies on using strategic capabilities should not diminish U.S. or Russian interest in a bilateral understanding.

U.S. Issues

Mutual restraint along these lines raises three issues for the United States:

- the warfighting utility of nuclear, ASAT, or cyber weapons
- the interests of Allies and solidarity of NATO
- confidence that the terms will be honored.

Cyberspace is the only area where the warfighting utility of these strategic capabilities is a serious issue for the United States. The policies of the United States are to reduce if not end the warfighting use of nuclear weapons and to rely on ASAT capabilities only for deterrence (notably of China).[36] But it will not rule out crashing computer networks that enable an opponent to target and attack U.S. military forces and operations. This consideration is less pertinent to possible combat contingencies with Russia, which does not rely heavily on military computer networking, than with China, which increasingly does.[37] Because of China, the United States needs a "firebreak" to prevent military cyber war, in which it might have to engage, from escalating to general cyber war, which it wants to avoid. Although such a firebreak is not imperative in Russia's case, for now, the United States should not pledge in any context to refrain from cyber war when it is integral and critical to combat operations. Thus, U.S.-Russia mutual restraint in cyberspace should apply to networks critical for national economic and societal well-being. Also, as noted, both should commit to ensure that military cyber operations are under the firm control of civilian authorities and that escalation is avoided.

In all three domains, the United States would insist that Russia's strategic restraint must apply to NATO as a whole, by agreement: anything less would run afoul of U.S. obligations under Article 5 of the Washington Treaty.[38] Still, some U.S. Allies, notably those bordering Russia and once part of the Soviet Union, may be concerned that for the United States to foreswear escalation beyond conventional defense, especially with nuclear weapons, could result in strategic "decoupling," weaken deterrence, and expose them to Russian aggression or intimidation.[39] In response, the United States can state that it can and would defeat *any* Russian attack on *any* NATO Ally, and also that Russian aggression, including cyber attack, would trigger a powerful response—conventional or in kind.

Such assurances might not lay Baltic worries to rest. However, given its military superiority, the United States cannot allow unsupportable fears of Russia's expansionism to abort an effort to mitigate real strategic vulnerabilities of its allies and itself. NATO already outspends Russia on defense by about 15 to 1, which should obviate the need to threaten or carry out strategic escalation.[40] If European allies of the United States are so fearful of Russian aggression, they have the option of increasing their defense spending beyond the current average of under 1.5 percent of gross domestic product (compared to nearly 5 percent for the United States). In any case, U.S. allies would benefit from Russia's nuclear and cyber restraint and from cooperation in counterproliferation.

In particular, the understandings proposed here would prohibit and help deter Russia from conducting against any U.S. ally the types of cyber attacks its agents allegedly conducted against Estonia and Georgia.

Confidence that the terms of mutual strategic restraint would be honored by Russia rests principally on strong deterrence, given the futility of Russia's defense against retaliation—because of offense dominance—in every domain. The United States has superiority not only in conventional military capabilities but also in nuclear, ASAT, and cyber capabilities. Presumably, it would not allow any of these advantages to erode because of having pledged to use them against Russia only in retaliation.

Additionally, Russia and the United States should agree to supplement and buttress pledges of restraint with practical confidence-building measures (CBMs). The purpose of strategic CBMs would be to discourage, or through noncompliance, provide indications of intent to attack first in any of the three domains. In addition to NATO-Russia BMD cooperation (as already discussed), these could include the following, some of which are already in train or under discussion in the United States or bilaterally:

- sharing more information on nuclear forces, plans, and third-country threats
- de-alerting some nuclear forces to relieve any remaining concerns about first strike without impairing readiness for retaliation
- assurance that neither will use *any* capabilities, including conventional strike forces, to degrade the other's nuclear deterrent[41]
- notification of all ballistic missile launches
- hotlines to discuss space and cyberspace attacks or incidents
- cooperation on third-party (state and nonstate) cyber threats.

Each of these measures would contribute to shifting U.S.-Russia strategic relations from the logic of threat and fear to a common effort to mitigate vulnerabilities and to confront dangers from the spread of nuclear and other strategic capabilities.

A Framework for Mutual Restraint

Taken together, CBMs would constitute a key tier of a framework of strategic restraint between the United States and Russia (see table 4).

The framework's premise is that strategic vulnerability, offense dominance, and the declining costs of mounting an attack demand restraint. It rests on a foundation of deterrence, without which mutual restraint would, for some time, be little more than expressions of good faith that might or might not withstand the stress of crisis. Building on deterrence, the framework includes explicit reciprocal pledges not to be the first to attack in any of the three strategic domains. By including CBMs as well as regular dialogue in the structure, the United States and Russia would begin institutionalizing mutual restraint, between them and within their own government and political systems.

How would this framework, taken as a whole, be viewed by Russians? As the gap between American and Russian military power grows, Moscow may become even more apprehensive of becoming formally locked into a position of inferiority, or of foreclosing options that Russia might need because of its military deficiencies—for example, the use of nuclear or cyber weapons. Yet as proposed here, mutual restraint does not constrain the strategic capabilities of either state. Russia will indeed find itself at a disadvantage in capabilities, but not because of agreement to exercise restraint in using them. It could even be argued that the side with inferior capabilities would benefit more by agreement that they should not be used. In any case, it is important for the United States to stress that proposed mutual strategic restraint would be based squarely on the principles of partnership and of equality in responsibilities, limitations, and rights.

Table 4. Levels of Mutual Trust and Cooperation in Strategic Domains

	Nuclear	Space	Cyberspace
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 forces, plans, and third parties. De-alerting. Conventional global strike assurances. BMD cooperation.	Launch notification. Communication hotline for queries on suspicious actions.	Consultation and cooperation on third-party threats, including criminal. Communication hotline for consultation on suspicious activities. Transparency about cyber doctrine.
Mutual Restraint, applying to the two states and allies	NFU of nuclear weapons against the other.	No first interference with the other's access to space.	NFU against critical networks. Agreement to exercise tight political control over military cyber operations.
Mutual Deterrence	Neither country can prevent strong retaliation by the other.		
Strategic Vulnerability	Both countries are vulnerable to nuclear, cyber, and potentially ASAT attacks		

For political reasons, Russia's leaders would have it no other way.

These ideas can energize the next phase of U.S.-Russia efforts to reduce the dangers of strategic conflict as the United States, its allies, and Russia all become increasingly vulnerable. It is unclear how Russia's leaders would react to a U.S. proposal along these lines: it depends on their assessment of Russia's strategic vulnerabilities and how committed they are to reforming and reorienting their country. Nonetheless, the United States should frame the discussion by offering a concept and possible terms for a safer strategic relationship and safer world.

Indeed, for the United States to present an ambitious, coherent set of proposals for lasting U.S.-Russia strategic restraint would send a powerful positive signal at an important juncture on the journey of U.S.-Russia relations. As it is, the U.S.-Russia strategic relationship has positive momentum but lacks a robust agenda. Admittedly, a positive response from Russia depends in part on whether its leaders are convinced of the need for reform and ever closer relations with the United States and its allies, which is uncertain. However, such uncertainty does not argue against a U.S. proposal along lines that serve U.S. interests, especially if making such a proposal could have a constructive effect on Russian strategic thinking and political direction.

It could take years for these ideas to be agreed between Moscow and Washington. Moreover, the strate-

gic restraint they prescribe should be designed to last in perpetuity. Then why rush to put such a proposal forward, especially with presidential elections looming in both countries? The need to move expeditiously, though not hastily, stems from the debate in Russia about the country's course and relations with the West. An offer to "raise the sights" of U.S.-Russia strategic relations, to mitigate growing vulnerabilities of both countries, and to include rather than exclude Russia from Western security efforts could help ensure that the debate's outcome is in American interests.

Notes

[1] This paper is a synopsis of a forthcoming book from NDU Press under the same title.

[2] Scott Borg, "How Cyber Attacks Will Be Used in International Conflicts," PowerPoint presentation at *USENIX Security '10 Technical Symposium*, Washington, DC, 2010.

[3] Department of Defense (DOD), *National Security Space Strategy* (Washington, DC: DOD, January 2011).

[4] Strategic offense dominance is explained in depth in 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).

[5] For further discussion on offense dominance in these strategic domains, see Gompert and Saunders.

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

[7] 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 (for example, the United States, Russia, and China) are also most capable of developing and employing countermeasures.

[8] This begs the question of whether U.S. leaders would be deterred from conducting a nuclear attack on Russia if they expected just a few Russian missiles to penetrate U.S. defenses. Apart from the sheer improbability of U.S. leaders contemplating a nuclear attack on Russia, it is hard to imagine stakes so high for the United States that its leaders would find even a single nuclear detonation on U.S. soil an acceptable price to pay.

[9] Leon E. Panetta, "Meeting our Fiscal and National Security Responsibilities," speech, Washington, DC, August 3, 2011.

[10] Contributing to this is a "targeting revolution," whereby advances in sensing, data processing and sharing, and precision guidance combine to permit objects to be found, tracked, and destroyed.

[11] The cost of launching a new satellite is equivalent to launching 3.75 antisatellite (ASAT) interceptors. The cost of placing a satellite in orbit was calculated by adding the average cost of a boost rocket and the average cost of a commercial payload. In reality, the cost of launching mission-critical satellites is probably far higher. The cost of launching an ASAT missile was derived from the Pentagon's estimate of how much it would cost to destroy Satellite USA 193 in 2008. Costs include acquisition of the unit being launched.

[12] Gordon-Loeb model in L.A. Gordon and M.P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security* 5, no. 4 (November 2002), 438–457.

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

[14] Pavel Podvig, "Russian Military Space Capabilities," in *Ensuring America's Space Security*, ed. Philip E. Coyle (Washington, DC: Federation of American Scientists, August 2004), 125–140.

[15] The table is extracted from Gompert and Saunders.

[16] This analysis excludes the costs resulting from retaliation.

[17] China's nuclear arsenal is an order of magnitude smaller than those of the United States and Russia. Moreover, the Chinese appear to be satisfied with a smaller force so long as effective minimum deterrence exists. However, it might be argued that the lower Russian and U.S. force levels go, the more tempted China could be to increase its force and achieve parity.

[18] The relationship between the size of strategic nuclear forces and the risk of nuclear war is, in theory, heavily influenced by the strength of deterrence, which may vary directly with the expected scale of destruction and thus the scale of forces in being. To the degree that deterrence is weakened as force levels are lowered, the risks of nuclear weapons being used might not decline but rise, all else being equal. That said, most analysts would agree that such an effect would not appear unless forces dropped below, say, triple-digit levels.

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

[20] See Vincent Manzo, *Deterrence and Escalation in Cross-domain Operations: Where Do Space and Cyberspace Fit?* INSS Strategic Forum 273 (Washington, DC: NDU Press, forthcoming).

[21] The analysis of Russian interests and perspectives is based on research of strategic and related literature and on intensive discussions of these ideas in Moscow with diverse interlocutors, both civilian and military.

[22] Opinion polls indicate a steady and significant improvement in Russian attitudes about the United States in recent years. For example, the Pew Global Attitudes Project finds an increase in Russians' favorable views of the United States from 41 percent in 2007 to 57 percent in 2010.

[23] A major share of Russian space services and products are exported, revealing the weakness of domestic demand—from an economy heavily oriented toward resource extraction.

[24] DOD, *Nuclear Posture Review* (Washington, DC: DOD, 2010).

[25] Based on the Russian revision of the threshold for using nuclear weapons in its latest military doctrine, *The Military Doctrine of the Russian Federation*, approved by the president on February 5, 2010. The threshold is more restricted compared to the military doctrine previously used. A translated text of the new document is available at <http://merln.ndu.edu/whitepapers/Russia2010_English.pdf>.

[26] Russian military chief Makarov observed in a November 2011 interview that a North Atlantic Treaty Organization (NATO)-Russia conflict (for example, over Georgia) could lead to nuclear war. What he failed to explain was, first, how such a conflict would meet Russia's

first-use standard of a threat to the survival of the state; and second, why Moscow's decisionmakers would ignore U.S. nuclear deterrence.

[27] Although Russia's missile interceptors are not at par with U.S. missile interceptors, Russia is attempting to upgrade air-defense systems for this mission. These could be adequate against an Iranian threat if Russia could use NATO warning and tracking data.

[28] In general, the Russians are especially wary of U.S. sea-based missile defense because it could be positioned flexibly to intercept Russian ICBMs.

[29] Russian insistence on a U.S. commitment not to develop or use missile defense against Russia's nuclear deterrent could be interpreted and opposed by Congress as yet another Russian attempt to derail U.S. ballistic missile defense (BMD).

[30] While there are many other important details to be settled concerning NATO-Russia BMD—such as architecture, sharing of sensitive technical and operational information, interceptor ownership, command and control, geographic scope—they are not analyzed here because none of them should block nuclear no first use or mutual strategic restraint in general.

[31] In April 2011, the EastWest Institute hosted a bilateral dialogue between American and Russian experts as part of a new initiative to achieve a common understanding on key terms in cyber security, producing the following document: "Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations," available at <www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=130080>.

[32] The United States reportedly is seeking cooperation with Russia along these lines but Russia has resisted because it would amount to external interference in Russian law enforcement.

[33] For both sides of this debate, see Martin Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009); and Gompert and Saunders.

[34] National Security Council, *The Comprehensive National Cybersecurity Initiative* (Washington, DC: The White House, 2011), available at <www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>.

[35] U.S. cybersecurity declaratory policy is increasingly clear that an attacker in this domain will face retaliation for what amounts to an act of war. National Security Council, *The Comprehensive National Cybersecurity Initiative*; National Security Council, *The Cyberspace Policy Review*, available at <www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

[36] DOD, *National Security Space Strategy* (Washington, DC: DOD, January 2011).

[37] An extensive discussion of the need for and possibility of cyber war firebreak can be found in Gompert and Saunders, *The Paradox of Power*.

[38] In effect, Article 5 calls for the United States (like all Allies) to join in the common defense of any Ally that is attacked. For the United States to rule out responding in kind if Russia attacked a U.S. Ally, but not the United States itself, in any of these domains would be to weaken the credibility and effectiveness of common defense.

[39] Notably, official NATO declaratory policy on first use of nuclear weapons does not lean as far forward as U.S. declaratory policy. Nonetheless, few if any Allies would strenuously or successfully oppose a NATO stance that favors progress toward no first use.

[40] Institute of International Strategic Studies, "Chapter Two: Comparative Major Defence Statistics," *The Military Balance* (London: IISS, 2011), 111:1, 33–40.

[41] Russia is particularly concerned that future U.S. conventional strike weapons could be used to destroy Russian nuclear retaliatory capabilities.

Acknowledgments

This Strategic Forum benefited greatly from discussions with and comments by Dr. Phillip Saunders, from comments by peer reviewers Dr. John Parker, Col Jon Chicky, and Dr. Robert Nurick, along with research by Roxanne Bannon.

INSTITUTE FOR NATIONAL STRATEGIC STUDIES

The Center for Strategic Research within the Institute for National Strategic Studies provides advice to the Secretary of Defense, Chairman of the Joint Chiefs of Staff, and unified combatant commands through studies, reports, briefings, and memoranda. The center conducts directed research and analysis in the areas of strategic and regional studies and engages in independent and leading-edge research and analysis in related areas.

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.

Nicholas Rostow
Director
Center for Strategic Research

Phillip C. Saunders
Director of Studies
Center for Strategic Research

Hans Binnendijk
Director
INSS

Francis G. Hoffman
Director
NDU Press