Rethinking the U.S. Strategic Posture

A Paper Presented to the Commission on the Strategic Posture of the United States

Dr. Daniel Goure
Vice President
The Lexington Institute

September 10, 2008

Defining a New Strategic Posture

The term strategic posture generally is associated with the means and methods by which nations pursue their national interests -- principally military forces and the way they are organized and employed. The link between national interests and strategic posture is determined by a nation's strategic objectives. A nation's most fundamental national interest is survival. Hence, its foremost strategic objective is to secure the homeland from attack. A strategic posture must first have adequate means and methods to ensure that objective. During the Cold War, the United States entered into a series of alliance relationships that extended the protection provided by its strategic posture to allies in Europe and the Pacific. U.S. national security policy also left open the possibility that nuclear weapons might be employed if other vital interests were threatened.

As technology has advanced, so too have the capabilities that constitute the strategic posture in a series of what historians term "revolutions in military affairs." The invention of gunpowder, the internal combustion engine, electric current, nuclear fission and the integrated circuit all produced transformations in both the means and methods that characterized the strategic posture. Some new technologies led to the expansion of the definition of a strategic posture to include new domains for warfare, notably the oceans, airspace and outer space.

After World War Two, the term strategic posture came to be almost singularly associated with nuclear weapons and the long-range means to deliver them, as well as the infrastructure to build and support them.

What distinguished the strategic posture of the Cold War from that of previous eras was the acceptance by both sides of mutual vulnerability. The strategic posture was designed and built primarily to deter a nuclear attack, rather than to defeat one or otherwise prevail in the event of a conflict.

Two new conditions have changed the way the U.S. should view its strategic posture. The first of these is the changing nature of the nuclear threat to the homeland. The United States and Russia no longer confront each other as adversaries. The strategic arsenals of both sides have been substantially reduced. More significantly, Russia no longer possesses the advantage in

conventional forces that once necessitated the threat of escalation to first use of nuclear weapons. Nuclear forces will remain an important, even central, element of the U.S. strategic posture for the foreseeable future. However, the danger of a large-scale nuclear attack on the U.S., its allies or other vital interests is extremely small.

The collapse of the Soviet Union also opened up the ability to deploy defenses as part of the U.S. strategic posture. Homeland vulnerability was no longer a prerequisite for a credible deterrent. The U.S. decision to withdraw from the Anti-Ballistic Missile (ABM) Treaty allowed it and Russia to deploy both defenses of the homeland and advanced theater missile defenses. While such capabilities are insufficient as yet to significantly impact the Russian or Chinese strategic deterrents, they hold forth the prospect for a highly capable defense against more limited threats.

The reduction in the risk of a major nuclear conflict did not result in the elimination of the danger of attacks on the homeland or on U.S. allies. During the Cold War, Russia rejected the Western concept of limited nuclear strikes, particularly if strategic forces were involved. However, the new Russian military doctrine, promulgated in 2000, overturned this long-standing policy. The new doctrine explicitly called for the use of limited nuclear strikes as a means of halting regional aggression. Analysts have interpreted this doctrinal shift as reflecting Russian concerns regarding its ability to defeat a U.S./NATO conventional threat.

Even as the Soviet threat was disappearing, the proliferation of nuclear weapons and their means of delivery raised the specter of limited attacks against the U.S. homeland or vital U.S. interests by others. While some have argued that regimes such as North Korea and Iran would be the most likely to employ such weapons covertly, the fact that both nations are investing heavily in long-range ballistic missiles suggests that this threat be treated as equally plausible.

The second condition impacting any appreciation of the U.S. strategic posture is the revolution in computing, communications and information technologies (IT). The U.S. has taken advantage of these technologies to promote a transformation of its intelligence activities as well as its military capabilities. As it impacts the U.S. strategic posture, this transformation has allowed the creation of so-called non-nuclear strategic capabilities.

But the U.S. does not have a monopoly on these technologies. Nor are these technologies any longer primarily the province of governments. The IT revolution is being driven by the global marketplace. It is largely commercial in character. The rate at which information technology is refreshed -- eighteen months or less -- challenges any government, including the U.S., to keep up. Most of the chips and much of the software that is at the heart of all U.S. IT systems is now acquired from overseas. It is almost impossible to ensure that the hardware and software are secure. The costs associated with the development of proprietary systems and software are becoming prohibitive even for the U.S.

At the same time, the IT revolution is putting new weapons in the hands of hostile interests. Terrorists, criminal organizations and rogue regimes can now access military-quality communications, information and targeting capabilities that only a few decades ago were solely the province of a handful of intelligence and military agencies. Groups have arisen, such as the Russian Business Network (BNN), which specialize in cyber crime.

What is even more ominous is the rapid advancement that has occurred in sophisticated and automated tools for attacking networks and computers. As a result, those seeking to attack networks do not need to recruit computer experts. Virtually anyone with access to a computer can now serve as a foot soldier in hacking attacks. There is a significant and growing asymmetry between cyber offense and cyber defense.

The commercial and military investments in IT are producing enormous benefits. They are also creating new vulnerabilities. U.S. government and commercial IT systems are being subjected to a constant and growing threat of intrusion and interference. The sources of this threat range from malicious individuals to criminal operations, foreign intelligence services and stateless terrorists. The *National Strategy to Secure Cyberspace* (NSSC) described the threat as follows:

> Cyberspace provides a means for organized attack on our infrastructure from a distance. These attacks require only commodity technology, and enable attackers to obfuscate their identities, locations, and paths of entry. Not only does cyberspace provide the ability to exploit weaknesses in our critical infrastructures, but it also provides a fulcrum for leveraging physical attacks by allowing the possibility of disrupting communications, hindering U.S. defensive or offensive response, or delaying emergency responders who would be essential following a physical attack.

This threat has been raised to a new level with recent massive cyber attacks on Estonia and Georgia. While these events inflicted only limited damage or disruptions they are certainly a portent of things to come. Also, these recent attacks highlight the difficulty in providing adequate forensics to support high confidence attribution. Although there is not incontrovertible proof, the educated guess is that the Russian government was behind the recent attacks. It is possible that these attacks were not carried out directly by Moscow, but rather by the BNN under contract to the Russian intelligence services or the Ministry of Defense. Chinese military doctrine refers to something called “The Assassin’s Mace,” which a number of experts believe is a massive, preemptive cyber attack designed to render an opponent’s military, governmental and major infrastructure systems inoperable.

What has emerged from the IT revolution is the prospect for a new form of warfare consisting of the manipulation of bits and bytes in an artificial environment, cyberspace. The U.S. military speaks of computer network operations, which includes actions taken to leverage and optimize the information networks on which weapons systems and forces are increasingly dependent, as well as offensive and defensive operations to gain information superiority and deny the enemy this enabling capability.

The U.S. effort to appreciate this new form of warfare and develop relevant policies and plans for both offensive and defensive actions in cyberspace has barely begun. Moreover, the nature of the cyber domain suggests that a conflict conducted there will be quite different from any involving conventional or strategic forces. For example, understanding the cyber battlefield (as distinct from collecting intelligence) may require penetration of networks and data bases owned or operated not only by adversaries or military organizations, but commercial as well as governmental systems in the hands of neutrals, even allies. Most of this effort will have to be

conducted in peacetime. It may be possible for a nation or group to conduct a successful preemptive attack, placing cyber "time bombs" in critical software or even in the processors that are at the heart of modern computers, days, months, weeks and even years before triggering them. The nation might not know that the war was over and had been lost until its adversary transmitted the terms of surrender. Even then, after the conflict was over, much less when it was underway, there might be difficulty establishing the adversary's true identity.

Finally, there is the challenge posed by apocalyptic terrorism. While the threat of terrorism is very old, that posed by the intersection of radical fundamentalism and technology is unlike any the United States has heretofore confronted. For 20 years, Western civilization, generally, and the United States, in particular, has been challenged by an adversary whose implacable hostility to modernity and extreme interpretation of Koranic law permits the use of any means in the pursuit of its millenarian objectives. In short, the terrorist's goals are so extreme that they transcend politics. It is a conflict without compromise, and hence, without limits with respect to means and targets. It also makes the possibility of deterring such groups, at least by the threat of retaliation, extremely problematic.

A terrorist group that possesses malevolent intent but lacks capabilities is perhaps of interest to political scientists, but is of relatively little concern to security experts. The problem is that a globalized economic and transportation system has given these terrorists potential access to advanced military technology and the means to deliver weapons to the U.S. homeland.

Many observers consider nuclear terrorism to be the most significant threat to U.S. security today. However, other potential means of attack, most particularly with biological weapons or using cyber techniques, could pose an even greater danger. Gaining access to nuclear materials or weapons is much more difficult than to sources of biological agents. Biological weapons are easier to transport and employ.

Countering this threat requires a balance between offensive measures, counterterrorism and counter proliferation and defensive measures, and homeland security. What is new here is the importance of defensive measures. Unlike the Cold War, when the sheer scale of the Soviet threat rendered both active and passive defenses irrelevant, now both kinds of defensive actions have purpose. The mere existence of defensive measures may well deter terrorist actions, if only because they heighten the risk of failure. A layered defense system, beginning with intelligence collection overseas, then border security and improved internal policing could actual defeat terrorist threats. In addition, a combination of infrastructure protection and enhanced response capabilities could limit the effects of any attacks that do succeed. Many of these same measures to secure the homeland from terrorist threats would also be effective in limiting the impact from limited strikes by states possessing weapons of mass destruction.

A New Strategic Triad

Meeting these challenges will require a new strategic triad. The first leg of that triad consists of a restructured and modernized strategic nuclear force coupled to a robust strategic defense capability. Some missions that once could be accomplished only with nuclear forces may now be doable with advanced conventional ordnance. The second leg of the triad might, for want of a

more elegant term, be called cyberspace forces. Such forces would consist of both offensive and defensive capabilities. The third leg can be called strategic protective capabilities. These would include the efforts by the Department of Homeland Security (DHS) and other civil agencies to prevent terrorist attacks and reduce the consequences of both manmade and natural disasters.

The impact of emerging capabilities for non-nuclear strikes, strategic defenses, information operations and cyber war for the U.S. strategic force posture is reflected in the mission statement of U.S. Strategic Command.

> Provide the nation with global deterrence capabilities and synchronized DoD *[Department of Defense]* effects to combat adversary weapons of mass destruction worldwide. Enable decisive global kinetic and non-kinetic combat effects through the application and advocacy of integrated intelligence, surveillance and reconnaissance (ISR); space and global strike operations; information operations; integrated missile defense and robust command and control.

Clearly, there is a blurring of the line between traditional military elements of the U.S. strategic posture -- those involving offensive and defensive weapons systems and supporting infrastructure -- and those involving broader measures to secure the homeland against a range of potential dangers and provide force protection for the military. Current activities intended to increase the resilience of critical infrastructure or the capability to recover from an attack harken back to civil defense and continuity of operations efforts undertaken during the Cold War. Although homeland security investments are explicitly focused on the threats posed by terrorist attacks and natural disasters, when considered in light of the expanded potential for strategic defenses of various types, they suggest the possibility for a damage limitation capability against rogue regimes possessing limited numbers of weapons of mass destruction and their delivery means.

Each leg of the new strategic triad will require shaping and investments. With respect to strategic nuclear forces, the United States continues to live off the decaying legacy of the Cold War force. For as long as it is retained, the strategic nuclear posture must possess three features. First, it must be of a size and character to deter attacks. The size of the force, the number of warheads and delivery means, is important if the U.S. is to ensure that no adversary believes that they can escape devastating retaliation. It must be postured in ways that make it extremely costly, if not impossible, for an aggressor to believe that he can initiate a disarming first strike. This means retaining both the land-based and sea-based legs of the erstwhile triad. In fact, the land-based force, with 450 silos requiring individual targeting, may be the most stabilizing force in an environment of reduced nuclear arsenals.

Second, to achieve its deterrent objective the nuclear force must be seen as a credible, hence usable, force. This may continue to be true for the existing force, in the event of a massive attack by Russia or China. It is not clear that the threat to turn North Korea or Iran into “a sheet of glass” is credible or desirable. Hence, at least some part of the force needs to be designed for limited or surgical missions against targets in those or similar countries.

Third, the force must be responsive to changes in the threat environment without recourse to actions that may increase instabilities. Efforts to de-alert strategic forces have been repeatedly shown to be either unverifiable or so complex as to make the force unresponsive. More significantly, many of the proposed de-alerting measures create a potential for a rearmaments race in the event of a change in the international environment.

The United States will require a credible, reliable and flexible strategic offensive posture for decades to come. Therefore, it is imperative that a plan be developed to provide for next-generation delivery systems. This means a new nuclear-capable strategic bomber and a follow-on ballistic missile submarine with a new missile. The land-based missile force has recently completed a refurbishment program. However, it is important to take the steps necessary to preserve the industrial base and design capabilities that support the intercontinental ballistic missile (ICBM) force.

Revitalization of the nuclear infrastructure is essential. There is a clear danger that the United States will lose critical skills in the design of weapons and parts. This form of disarmament by erosion is unacceptable, even if the decision is taken to begin down the long road to denuclearization. Revitalization must involve not just the weapons complex but many parts of the military infrastructure and weapons handling system as well. Recent events demonstrated that the Air Force let its skills in the management of nuclear weapons atrophy. Not only will a lot more money need to be spent to deal with the deterioration, but the Air Force needs to think about the career paths for new nuclear personnel.

The United States is only at the early stages of developing and deploying strategic and theater defenses. Only recently has the Missile Defense Agency been able to take full advantage of the opportunities provided by the withdrawal from the ABM Treaty in the development of weapons systems and operational concepts. Current systems such as the Ground-Based Midcourse Interceptor (GMD), Aegis Ballistic Missile Defense System (BMDS) and the Theater High Altitude Area Defense (THAAD) will provide one layer of defense against either intercontinental or shorter-range missiles. The ability to send tracking information from distant sensors to the missiles -- something prohibited by the ABM Treaty -- will increase the effectiveness of these and follow-on systems.

The U.S. has the opportunity to deploy layered defenses. In particular, it is developing systems that will be able to intercept many types of ballistic missiles in the early part of their flight trajectory. These systems will also be mobile, allowing U.S. defenses to alter their deployments in response to emerging threats. The Airborne Laser is scheduled to demonstrate that it can shoot down a boosting missile in 2009. The Kinetic Energy Interceptor (KEI) is a very fast missile with tremendous range that can be either sea-based or deployed in a land-mobile configuration. It could also serve to augment the GMD deployments in the United States and Europe. In the future, KEI could also be deployed at sea, providing a highly mobile and extremely secure means by which to deploy missile defenses to confront emerging threats. The Network-Centric Airborne Defense Element (NCADE) will be carried by fighter aircraft or unmanned aerial vehicles (UAVs) and will provide a tactically responsive boost-phase defense. NCADE is relatively low-cost and can be highly effective against the numerically small and technically

unsophisticated threats posed by North Korean or Iranian ballistic missiles. By operating in layers, the effectiveness of missile defenses can be multiplied.

In addition to robust missile defenses, the homeland is likely to require defenses against air-breathing and sea-based threats. Such a defense need not be large, given the relatively small number of strategic aircraft in foreign inventories. However, such aircraft or even ocean-going vessels may deploy high-speed cruise missiles. Intercepting these will require advanced fighter aircraft such as the F-22, Global Hawk UAVs conducting broad area maritime surveillance, and command and control aircraft such as the Hawkeye E2-D and the Airborne Warning and Control System (AWACS). Aegis-equipped surface vessels employing the new Standard Missile 2 and soon the Standard Missile 6 can also contribute to effective air defenses.

The sea-based threats of concern are not the missile submarines or aircraft carriers of foreign nations. Rather, the threat is of non-state actors attempting to smuggle a weapon into the United States, or a rogue nation employing a commercial vessel to deploy a launch system within range of U.S. shores. Defense against sea-based threats is as much about intelligence and warning as it is about active defenses. Indeed, actually defeating such threats is relatively easy if they can be identified and tracked. The Navy/Coast Guard program for maritime domain awareness is intended to identify potential threat vessels allowing conventional maritime forces to inspect and, if necessary, intercept them.

Cyber offense seems to be the natural province of the Intelligence Community and the Department of Defense. The question is whether or not enough resources are being devoted to the tasks of understanding foreign networks and to conducting operations against them. Computer networks have become ubiquitous in the U.S., complicating efforts to define who should be in charge of their defense and how that should be accomplished. Currently, responsibility for cyber defense is spread across a number of government departments and agencies. Each government entity is responsible for its own defense. This is an area which cries out for effective coordination and strategic planning across the federal government, between levels of government and with the private sector.

It is even more important to consider ways of improving the defense of privately-owned and operated computer networks. DHS and the FBI have responsibilities in this area but limited authorities and resources. The broad responsibilities of both DHS and the FBI make it unlikely that they will be able to devote the resources and executive attention that cyber security requires. Reliance for protection solely on the private sector is problematic, at best. There may be a requirement for a new federal agency that can monitor the cyber domain, identify threats and respond to attacks on private networks and, perhaps, those on some parts of the government, as well. To perform its mission, this new agency would require unique authorities.

The concept of strategic defense needs to be expanded to include many of the measures now being taken to protect the homeland against terrorist use of weapons of mass destruction (WMD) and to assist in response and recovery in the event of a successful attack. Effective controls and surveillance of the borders is one aspect of a homeland security capability. Given the magnitude of the problem, much of this will have to be done using sensor technologies and networks. SBINet, a concept for instrumenting the borders, can provide part of the solution. In addition,

DHS is deploying advanced sensors to provide automated detection of biological and nuclear threats. Additional cargo screening capabilities are needed at the nation's ports of entry.

Improving the security of the critical infrastructure, national resilience and responses to catastrophic events are of equal value whether the threat is catastrophic terrorism, natural disaster or an attack by another country using WMD. Minimum standards need to be set for the survivability of critical infrastructure. Continuity of operations plans should be required for the private sector as it is for the departments and agencies of the federal government. The National Guard must be funded, equipped and structured to provide a ready force to respond to any catastrophic event. Perhaps most important, the National Disaster Medical System must be organized, equipped, staffed and funded to provide a timely and effective response to any significant medical emergency.

It is quite possible to envision a slow evolution of the U.S. strategic posture away from its current reliance on strategic nuclear offensive forces and towards a situation characterized as defense dominant. Indeed, uncertainties regarding the stability of deep reductions could be ameliorated by the deployment of robust strategic defenses. As noted above, the combination of strategic defenses and homeland security measures could create the opportunity to replace a retaliatory strategy with one based on damage limitation or even damage denial, at least with respect to small threats.

Nuclear weapons will continue to serve a number of important roles in U.S. national security. Ultimately, their presence forces an aggressor to consider the possibility that the U.S. might employ its arsenal in an escalatory or retaliatory role. The search for conventional capabilities that can serve in lieu of nuclear weapons is laudable and should be continued. However, in the face of well-documented limitations on conventional strike capabilities and countermeasures already being pursued by adversaries, it is by no means certain that a credible all-conventional deterrent can be developed.

Arms Control Issues

It is taken as almost an article of faith in the national security community that it is both possible and desirable for the United States to "put the nuclear genie back in the box." This is wishful thinking. Moreover, the effort to achieve a denuclearized world is more likely than not to create conditions of extreme instability -- one which will diminish U.S. security.

With respect to nuclear weapons, the Strategic Posture Commission is confronted by the need to choose between two clear and mutually exclusive paths to the future. The first is one that while hoping for the elimination of all nuclear weapons believes that day is far off, if ever. In the meantime, nuclear weapons will continue to play an important role in U.S. security. Although the first path could be achieved with a reduced strategic nuclear arsenal, that force, both delivery systems and warheads, would have to be modernized.

An equal or even more important role will be played by strategic defenses. These include not only defenses against ballistic missiles but air defenses and homeland security, as well. Many of the measures being undertaken to protect against WMD terrorism or to increase the resilience of

the U.S. infrastructure will serve double duty in the event of a deliberate attack on the homeland by a state actor.

The second path seeks complete and total denuclearization within a relatively short period of time, perhaps 20 years. This goal is necessitated, advocates argue, by the dangers created by a proliferated world. Unless all nuclear weapons, materials and knowledge are placed under strict international controls, it is inevitable that the United States will be struck by either a state or non-state actor.

In order to pursue this second path, nuclear weapons need to be devalued, their utility marginalized and their use inhibited. Moreover, the pursuit of a global no-nukes goal means that the United States and Russia must take the lead in this process. They must reduce their arsenals, eschew modernizing their forces and avoid any measures, however slight, which might give pause to other nuclear states or would-be proliferators.

The problem is that any steps taken to enhance the U.S. strategic posture, whether by modernizing nuclear forces, deploying strategic defenses or even providing for enhanced security of the homeland against WMD, undermines the pursuit of the zero-nukes goal. Nuclear forces cannot be modernized, even for purposes of enhanced safety and security, without a loss of credibility in the zero-nukes goal. Strategic defenses are also anathema because they could encourage others to increase the size of their nuclear arsenals. Even homeland security must be carefully controlled lest it create the potential for survival in the event of a nuclear attack.

The two paths are mutually exclusive. In fact, even support for the eventual goal of total denuclearization makes it difficult to argue the case for modernizing the force in the interim. The greatest danger is that the United States will be able to achieve neither a modernized strategic posture nor zero nuclear weapons. This would be the worst outcome because the United States would be forced to continue to rely on nuclear deterrence for its security with a strategic posture that is obsolete, of uncertain performance and able only to wreak massive damage.

This still may be the preferred strategy to that of failed denuclearization. In order for the zero-nukes strategy to be successful it must achieve an unprecedented level of intrusive monitoring and inspection. Moreover, these controls must extend not just to nuclear weapons and materials but also to biological and, even possibly, to cyber “weapons.” No system of controls can guarantee 100% against the possibility of surreptitious biological breakout or the acquisition of a WMD by a non-state actor. Thus, pursuing the zero-nukes path is more dangerous for U.S. security than continuing to allow its strategic posture to erode.

Despite assertions regarding the dangers of a proliferated world for U.S. security, it is not clear that those dangers outweigh the risks created by a denuclearization path that is only partially traversed. This author would go so far as to assert that the potential threat of a single nuclear weapon in the hands of a non-state actor would pose less of a threat to U.S. security than would a brittle and potentially failure-prone strategic deterrent.

There are a number of other factors that argue for the retention of a strong and capable nuclear deterrent. These include the growing nationalism and even militancy of Russia, China’s large-

scale investments in its military most notably in anti-access capabilities unquestionably intended to deny the U.S. a military presence in the western Pacific, and Iran's race to acquire a nuclear weapon. A number of members of the so-called nuclear club are not about to give up their nuclear capabilities. Indeed, some such as Russia have made it clear that they intend to rely heavily on nuclear forces for their security. The same can be said for Pakistan and India.