THE PERILS OF COMPLACENCY: ADAPTING U.S. DEFENSE TO FUTURE NEEDS

STATEMENT BY

ASHTON B. CARTER
PROFESSOR OF SCIENCE AND INTERNATIONAL AFFAIRS HARVARD UNIVERSITY
AND
CO-DIRECTOR, HARVARD-STANFORD PREVENTIVE DEFENSE PROJECT

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES
UNITED STATES SENATE

MARCH 21, 2000
SECOND SESSION, 106TH CONGRESS

STATEMENT BY
ASHTON B. CARTER
PROFESSOR OF SCIENCE AND INTERNATIONAL AFFAIRS
HARVARD UNIVERSITY
AND
CO-DIRECTOR, HARVARD-STANFORD PREVENTIVE DEFENSE PROJECT

The Perils of Complacency: Adapting U.S. Defense to Future Needs

Mr. Chairman and Members of the Subcommittee on Emerging Threats and Capabilities, thank you for inviting me to come before you to testify about the vitally important business of this Subcommittee. The American military is the envy of the world. Since the Cold War ended it has consistently demonstrated prowess and flexibility in operations as diverse as Desert Storm and the securing of Haiti. The American public apparently shares with foreign friends and foes this favorable view of the U.S. defense effort: they give their approval to the military almost alone among institutions of the federal government. This approbation for the Department of Defense, however deserved, is not a birthright or a fact of nature. It will need to be earned and earned again in the decades ahead. But the success against the relatively minor challenges of the post-Cold War era to date has engendered a dangerous complacency in American national security thinking. As a result the United States might fail to adapt in ways that will both reduce future security threats and ensure that today's military excellence endures into the future.

This Subcommittee has the task of looking to the future and ensuring that DOD is adapting to meet its challenges. The creation of this Subcommittee demonstrates that the Senate Armed Services Committee is aware of the danger of complacency and willing to adapt itself to meet the new challenges head-on. I am strongly encouraged by this awareness, and the purpose of my statement is to set out some themes that might assist you as you plan the Subcommittee's work.[1]

There are four interrelated areas where complacency about defense is taking its toll and the need for change is becoming urgent. The first is strategy. The role of strategy is to set priorities amongst the almost endless list of tasks that might be taken up by the world's leading power. The kindest thing that might be said of American behavior ten years into the post-Cold War world is that it is a-strategic, responding dutifully to the *crise du jour* with little sense of priority or consistency. A less charitable characterization would be that the United States has its priorities, but they are backwards, too often placing immediate intervention in minor conflicts over a "Preventive Defense" strategy focused on basic, long-term threats to security.

[1] Portions of this written statement are drawn from Ashton B. Carter, "Adapting U.S. Defense to Future Needs," *Survival*, vol.41-4, Winter 1999-2000, pp. 101-123; and Ashton B. Carter and William J. Perry, *Preventive Defense: A New Security Strategy for America* (Washington, D.C., The Brookings Institution, 1999).

But even getting the strategy right will not preserve America's security unless the priorities are reflected in Pentagon budgets and programs. The second task is therefore to adapt defense programs to the mission of preventive defense.

A third needed focus of adaptation is defense organization and management. The United States enters the 21st century with a defense establishment whose basic structure was determined a half-century ago to deal with a challenge, the Cold War, that is now a decade in the past. Here complacency has taken the form of assigning new tasks to the old structure in incremental fashion, rather than undertaking basic renovations. The result is a growing list of new missions that find themselves institutionally homeless.

A fourth challenge results not from changes in the spectrum of military threat, but from trends in the industrial and technology base that undergirds the distinctive U.S. technological edge in military affairs. This base, once largely the creation of the Department of Defense and almost exclusively American, is commercializing and globalizing. The trends of commercialization and globalization, if embraced and adapted to by DOD, can act to the benefit of U.S. military capabilities in the future. But the reverse is also true: persisting in old innovation and procurement habits in the face of the new trends will both erode the technological edge and open up new vulnerabilities.

In my statement, I will touch briefly on each of these four adaptations in turn.

AMERICAN STRATEGY: THE CONCEPTUAL VACUUM

For a decade, we have been declaring ourselves to be living in the post-Cold War era. This formula has become awkward, even embarrassing, as the years go by. It is an admission that we do not know where we are going strategically, only whence we have come. The United States is in need of a strategic conception that admits the transition is over and charts a course into the future. Especially important is a clear sense of defense priorities. This problem bothered George Marshall at America's previous great strategic transition, after World War II. In an address at Princeton University in 1947, Marshall said, "Now that an immediate peril is not plainly visible, there is a natural tendency to relax and to return to business as usual….But I feel that we are seriously failing in our attitude toward the international problems whose solution will largely determine our future."

The central task of strategy is to identify an "A-list" of security problems that have the potential to replicate the Cold War in terms of the magnitude of security danger they pose to the United States. "A-list" problems are the ones that, to use Marshall's words, "will largely determine our future."

STRATEGIC INVERSION: "C-" and "B-" Lists

The public imagination, reflecting CNN, has begun to get the impression that the security challenges of the post-Cold War era arise in such places as Kosovo, Bosnia, East Timor, Haiti, Rwanda, and Somalia. These are the issues that have dominated the security headlines in the

1990s. Indeed, there is even talk of the post-Cold War's first presidential "doctrine," the so-called Clinton Doctrine, dealing with precisely this issue.

The Kosovos and their ilk are without doubt important problems: they represent not only atrocities that offend the human conscience, but if allowed to fester can undermine the foundations of regional and international stability. But it is also true that such problems, while serious, do not threaten America's vital security interests. Still less do they threaten the survival, way of life, or position in the world of the United States in the way the Cold War's Soviet threat did. For this reason, such problems belong on a strategic "C-list": important but lesser objects of security strategy. Because "C-list" issues do not threaten America's vital security interests, dealing with them individually or as classes – peacekeeping, peacemaking, humanitarian operations, "operations other than war" and the like – cannot make up the core national security strategy of the United States.

If one takes one's cues not from the news broadcasts but from the U.S. defense budget, one perceives a different implicit post-Cold War strategy built around the so-called "two Major Theater Wars." The 2MTWs are Desert Storm-scale conflicts in Northeast Asia or Southwest Asia. These too are important security problems. Indeed, unlike the "C list" problems they *do* implicate vital U.S. interests. The United States does not have the option to select among them or opt out of them. But in their current form they do not threaten U.S. survival, way of life, or position in the world. Thus the two MTWs should be assigned to a strategic "B-list."

THE "A-LIST"

What problems, then, belong on the "A-list?" The "A-list" is reserved for Cold War-scale problems: threats to U.S. survival, way of life, and position in the world. The answer, of course, is that there are no imminent "A-list" threats, as defined in traditional military terms, and there have not been any since the Soviet Union ended. Today's "A-list" is populated with something different: threats that *might be*, rather than threats that *are*.

There are five dangers that could, over time, evolve into "A-list" scale threats to U.S. survival, way of life, and position in the world:

-- the danger that Russia might descend into chaos, isolation, and aggression as Germany did after World War I, in a "Weimar Russia syndrome";
-- the danger that Russia and the other Soviet successor states might lose control of the nuclear, chemical, and biological weapons legacy of the former Soviet Union;
-- the danger that as China emerges it could spawn hostility rather than becoming cooperatively engaged in the international system;
-- the danger that weapons of mass destruction will proliferate and present a direct military threat to U.S. forces, territory, and allies;
-- the danger that "catastrophic terrorism" of unprecedented scope and intensity might occur on U.S. territory.

These "A-list" problems do not take the form of imminent military threat in traditional military terms. They have not as a rule made headline news or driven defense programs during

the decade-old "post-Cold War era." But while neither imminent nor certain, the "A-list" problems will, to quote George Marshall once again, "largely determine our future."

FIGURE A

The A-, B-, and C-Lists*

A-List: Potential future problems that could threaten U.S. survival, way of life, and position in the world. Possibly preventable.

- "Weimar Russia"
- Loose nuclear, chemical, biological weapons
- A rising China that spawns hostility
- Proliferation of weapons of mass destruction
- Catastrophic terrorism

B-List: Actual threats to vital U.S. interests. Deterrable through ready forces.

- Major Theater War in Northeast Asia
- Major Theater War in Southwest Asia

C-List: Important problems that do not threaten vital U.S. interests.

- Kosovo
- Bosnia
- East Timor
- Rwanda
- Somalia
- Haiti
- …

* Adapted from Ashton B. Carter and William J. Perry, *Preventive Defense: A New Security Strategy for America*, Washington, D.C., The Brookings Institution Press, 1999.

THE "A-LIST" AND U.S. DEFENSE PROGRAMS

Taking the preventive defense strategy seriously, with it's A, B, and C Lists as shown in Figure A, has two broad implications for defense. First, DOD needs to make it a mission to prevent the A-List threats from emerging. Second, DOD needs to be prepared in the event that prevention fails. In its Quadrennial Defense Review, DOD recognized the importance of

preventive defense by adding "shaping the international environment" and "preparing" for an uncertain future to the Pentagon's mission of "responding" to current threats and contingencies. As yet, however, far too little effort goes to "shaping" relative to "responding" to "B-list" and "C-list" threats. The effort to "prepare" for the future through the application of new technology in the much-touted "Revolution in Military Affairs," moreover, is devoted more to the perfection of the current force than to providing the new capabilities that "A-list" threats might require.

PREVENTION AS A DEFENSE MISSION: "DEFENSE BY OTHER MEANS"

The key feature of the "A-list" is that it calls for preventive responses that do not take the form of traditional war-winning military capabilities. It therefore requires that a portion of the national defense effort be devoted to "defense by other means." Prevention is different from deterrence, and is a new strategic departure for the United States. But in prevention the Pentagon can and should play a central role. Three examples of Preventive Defense at work are:

- The Cooperative Threat Reduction or Nunn-Lugar program and its offspring, including the Nunn-Lugar-Domenici initiatives, which have accomplished so much for American security because of the farsightedness of these Senators;
- Military-to-military contacts programs and NATO's Partnership for Peace, which acquaint foreign militaries with ours, and ours with theirs;
- The evolving national efforts to combine the capabilities of DOD, law enforcement, and emergency response to craft appropriate responses to the specter of catastrophic terrorism.

RETOOLING INVESTMENT: THE HAMMER MEETS THE SCREW

Preventive measures like the Nunn-Lugar program increase the chances that A-List problems do not develop into full-scale threats. But they do not guarantee success. Therefore we also need to prepare against the prospect that A-List threats emerge. In this connection, it is important that our investment give adequate weight to asymmetric counters to our military capabilities.

Saddam Hussein's military in 1991 was in many ways a miniature version of the Soviet army in its equipment, doctrine, and tactics. This was precisely the type of threat against which the U.S. military and its coalition partners drawn from NATO had been practicing for decades. Faced with the hammer of the U.S. military, Iraq configured itself as a nail. The outcome was never in doubt. Slobodan Milosevic's Serb forces were similarly Soviet-like, as are Kim Jong-Il's North Korean conventional forces.

The hammer that struck Iraq's nail in Desert Storm was the result of the second post-World War II "revolution in military affairs" (RMA), to use a now-popular phrase. The first revolution began during World War II and centered on the atomic bomb and the ballistic missile for strategic bombardment. The second RMA, dubbed the "offset strategy" because it was begun in the 1970s to offset Soviet numerical superiority in conventional tactical forces, centered on air superiority, dominant intelligence and communications, and precision strike. Today a third RMA is underway. While all of its implications and artifacts are not yet apparent, certain characteristics are already clear.

First, the RMA does not involve dramatically new types of "platforms" from the ships, aircraft, armored vehicles, and satellites that make up today's military. Rather, innovation is largely directed toward embedding new capabilities in the old platforms. Second, the revolutionary new military capabilities inhere not only, or even especially, in these improved platforms and systems. The revolution arises from the ability to put these systems into architectures where they act synergistically – into what the Defense Science Board long ago dubbed "systems-of-systems." For example, dominant intelligence and communications permits targeting by precision weapons. These precision weapons, when directed against air defenses, in turn permit air superiority. Air superiority in turn facilitates targeting…and so on. Third, the underlying technology fueling the current revolution does not arise from defense-sponsored R&D, as in the previous two post-World War II RMAs. The important underlying technologies spring from a technology base that is commercial and, increasingly, global. Fourth, the critical enabler of the current RMA is information technology. (In the near future biotechnology, microdevices, and new materials will probably also be recognized as having revolutionary potential as great as information technology.)

Referring back to the "A-," "B-," and "C-lists," it is clear that the RMA in its current form is well suited to meet the military challenges of the "B-" and "C-lists". The RMA is also necessary for meeting potential "A-list" challenges. But it is not sufficient.

The needed adaptations of the RMA to deal with asymmetrical threats fall into two categories. The first category is counter-countermeasures to the countermeasures opponents will devise against our RMA system-of-systems. The RMA system-of-systems is formidable, but it is quite fragile in some respects. It therefore needs to be made not only more capable, but more robust. The second category is counterproliferation against weapons of mass destruction. Biological weapons in Iraq or nuclear-tipped ballistic missiles in North Korea would catapult these "B-list" items to the "A-list." Chemical weapons in the hands of transnational terrorists or cyber weapons used by an unseen foe would open a homeland front in an otherwise foreign conflict. Augmented by biological or cyber weapons and a willingness to use them, Saddam Hussein's military is no longer a nail, but something different – a screw, perhaps. A better hammer is not the instrument we need to deal with the problem of such "asymmetric" threats as WMD. A substantial part of the new investment in defense, therefore, should properly be directed at making screwdrivers for asymmetric threats in addition to upgrading the hammer.

NEEDED ADAPTATION IN ORGANIZATION AND MANAGEMENT

The structure of the U.S. Government for managing national security was established in 1947-49 and has since undergone remarkably little fundamental alteration. Major business organizations, by contrast, have been subjecting themselves to increasingly frequent reorganizations deemed necessary to be effective in changing circumstances. It is not surprising that the Cold War structure of the U.S. Government and DOD perdured through four decades of an essentially static strategic standoff. But it is remarkable how little change has occurred since the Cold War ended.

Most policy advice on national security affairs that will be given to the next U.S. president will take the form of prescribing certain policies, advocating certain programs, or urging emphasis on certain security threats over others. These are important questions, but just

as important is whether the government, and especially DOD, has the capability to **implement** the policies the nation's leaders choose for it, to **manage** the programs they direct, and to **anticipate and adapt** to a changing world. There is mounting evidence that the national security establishment is deficient not so much in deciding what to do as in having the ability to get it done.

The upcoming presidential transition offers an opportunity to make basic changes in management and organization. In the American system this opportunity comes only every four or eight years. Early in a presidential transition, civilian jobs are not yet filled with new officials who might resist a change in their functions. The new administration has not yet settled into a pattern of making do with "the system" it inherited. Politically, the Congress and the voters are expecting change.

Within DOD, one far-reaching restructuring was in fact begun as the Cold War was ending. The restructuring was enacted in the Goldwater-Nichols Department of Defense Reorganization Act of 1986. Goldwater-Nichols ensured that the President could receive unified or "joint" military advice from a strengthened Chairman and Vice-Chairman of the Joint Chiefs of Staff rather than the homogenized advice of separate chiefs of the Army, Navy, Air Force, and Marines; and that unified Commanders-in-Chief (CINCs) would plan and fight wars, rather than having separate branches wage separate campaigns. In these objectives Goldwater-Nichols has been a great success by almost all accounts. Yet this wave of innovation left some questions unanswered. While Goldwater-Nichols made it possible to marshal joint forces for contingencies, forces are still configured, and weapons developed, by the separate armed services. There is no mechanism for procuring forces that are inherently joint in the first place. Said differently, the "joint" CINCs have little voice in what forces they get, only in how they use them. This problem is widely recognized but awaits its institutional remedy. For the time being, the CINC for the U.S. Atlantic Command (now Joint Forces Command) has the job of configuring and training "joint" forces. His role is growing into training and exercising joint forces, but in time he and the other CINCs will need a stronger role in determining how money is spent to procure forces that are inherently joint.

Another related problem is how to take full advantage of the information revolution that underlies the Revolution in Military Affairs. Here, in addition to the Army, Navy, Marines and Air Force, there is a fifth de-facto "armed service" of central importance in the information-based RMA. A welter of agencies and programs within the DOD budget, some termed "defense-wide," spend together as large a share of the acquisition budget as the U.S. Army. The defense-wide "armed service" comprises defense agencies like the Defense Information Systems Agency and the myriad agencies that make up the Intelligence Community (the Central Intelligence Agency, the Defense Intelligence Agency, the National Security Agency, the National Reconnaissance Office, and many others). These agencies, together with Service programs, make up the system of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR in the current incarnation of this growing acronym). Most of these capabilities are inherently "joint." Yet there exists no central systems architect for the information revolution and no "armed service" that recruits, trains, and equips this aspect of the military. This problem, too, is widely recognized but has not yet yielded to managerial solution.

Next are the new missions. The United States has enjoyed the luxury of distance from the sources of conflict that affect its interests. Its neighbors are Canada and Mexico. Defense of its interests has been a matter of projecting military power elsewhere, far from the homeland. Both technology (e.g., ballistic missiles) and globalization (resulting in the possibility of transnational terrorism) suggest that homeland defense is a security mission for the future. Yet the homeland is only now becoming an "area of responsibility" for a Commander-in-Chief of the armed forces – in the current formulation, the CINC for Atlantic Command/Joint Forces Command. In addition to homeland defense, defense against asymmetrical threats including weapons of mass destruction awaits its final institutional innovation. A good start has been made in the creation and strengthening of the Defense Threat Reduction Agency, but further adaptation is probably warranted. Peacekeeping, coalition warfare, and preventive defense programs are also new missions largely being carried out in old structures.

Together these organization and management challenges add up to a "threat within" that, if ignored, can have effects over time just as deleterious to our security as a new external threat.

THE SHIFTING FOUNDATION OF AMERICA'S TECHNOLOGICAL EDGE: COMMERCIALIZATION AND GLOBALIZATION OF THE DEFENSE INDUSTRY

America's unique military edge is technology, but the industrial foundation on which its preeminence rests is shifting. During the cold war, the US relied on the offset strategy—countering superior Warsaw Pact numbers with superior technology. This remains the core of the American way of ensuring a strong defense: field superior technology, simultaneously denying opponents access to the same technology. But the twin trends of commercialization and globalization of the base upon which our technological edge rests will require new approaches to both superiority and denial.

The effects of commercialization and globalization can be summed up in Figure B, portraying a sharp contrast between the defense industry of the Cold War ("THEN") and the world toward which present trends, were they to continue, would carry us ("WHERE TRENDS ARE TAKING US"). The world portrayed on the right-hand side of the Figure B has largely beneficial implications for U.S. military capabilities in the future. But is also poses profound issues of policy significance. These trends in defense technology and industry are as important as trends in the spectrum of military threat for the future of U.S. security. They pose a massive adaptive challenge to DOD.

COMMERCIALIZATION

In the days of Cold War, new technologies of importance to defense usually arose from research conducted under DOD sponsorship within defense companies, think-tanks, and universities located in the United States. Today new defense systems tend to arise when defense companies embed commercially developed technology into weapons. This transplantation of the roots of the nation's defense from one soil under its direction and control to another governed by profitmaking in the civil marketplace has profound policy implications.

To appreciate the facts, contrast the situation in 1980 with the Fiscal Year 2000 upon which we are embarking. According to the National Science Foundation, the amount of money spent on scientific research and development (R&D) in the then-western world in 1980 was about $240 billion in today's dollars, evenly divided between the United States and its G-7 partners. The U.S. Department of Defense sponsored about $40 billion, or fully one sixth of the *total*. In the year 2000, by contrast, the corresponding global total for R&D spending is $360 billion. The United States still accounts for half this amount, about $180 billion. But today DOD furnishes only one twelfth of the total – half the 1980 portion. Moreover, there are indications that this shrinking portion is not being used to press the technological frontier. Much more of the DOD R&D spending is being used for downstream engineering of mature systems than for research into new enabling technologies – more D than R (88% development and 12% research in 2000 versus 69% and 31%, respectively, in 1980). In terms of applications, much defense R&D today goes to keep old "legacy" systems going rather than to launch new leap-ahead military systems. Independent research and development (IR&D) conducted within defense companies and cost-shared with DOD, which used to be a means for keeping defense companies innovative, is also declining. All these indices point to one fact: tomorrow's defense innovations will be, in the large, derivatives of technology developed and marketed by commercial companies for commercial motives. In all but narrow custom niches, DOD has no alternative but to ride the tide of commercial development.

Closely related to commercialization is marketization of the defense industry. As the steep plunge in defense stocks testifies, the defense industry is being held to the same standards of stockholder value to which Wall Street holds other companies. Despite a wave of consolidation amongst the prime contractors (now spreading to the second and third tiers of the defense industry), the levels of profit, growth, and efficiency sought by Wall Street are proving difficult to match in the defense industry. It is likely that DOD will need to adapt is practices to keep a healthy industry, within an overall free market framework.

GLOBALIZATION

The commercial industry that will service defense in the future will not only be non-defense, it will be non-American. Defense prime contractors still tend to be national in their orientation -- American, German, French, etc. But their *suppliers* of technology and subsystems are increasingly globalized companies. Their *markets* are global. And even their *ownership* is globalizing.

Globalization of ownership is the slowest of the trends to affect the defense industry. Globalization of ownership of commercial companies is, of course, far advanced and inexorable. Ownership of defense companies, by contrast, is only now shifting from the state to private hands in Europe. The corresponding process occurred decades ago in the United States as the arsenal system was dismantled. Whether the American and European defense industries, all dependent on a globalizing commercial technology base, can stand apart from the globalization trend in ownership is the topic of fevered speculation. The outcome has important implications for defense policy. At one extreme, as shown in Figure B, the defense industry might not follow commercial industry in the globalization trend. The likely result will be American defense

companies on the one hand, and pan-European defense companies (the latter the result of mergers and acquisitions among British, French, German, Italian, and other firms under the pressure of the European Union) on the other, all acting with their governments' help to protect their home markets and competing ferociously for the export market. An economic rift within the Alliance and a parade of charges that one side was selling weapons to the potential opponents of the other would likely follow. This outcome would also probably widen the gap between U.S. and European defense capabilities, to the further detriment of Europe. At the other extreme, extensive trans-Atlantic mergers and acquisitions might result in a defense industry consisting at the prime contractor level of several trans-Atlantic giants competing among themselves for both the Alliance markets and global markets. The result would be a melding of continents and a knitting-together of NATO's military capabilities – a politically significant reinforcement of Alliance solidarity in the realm of political economy. An outcome in between these extremes is likely, but whether it will be closer to one or the other is still up in the air.

ARE COMMERCIALIZATION AND GLOBALIZATION GOOD FOR DEFENSE?

While commercialization and globalization reflected in the right-hand column of Figure B create a strange new world for defense, on balance they are strongly favorable. Riding the commercial technology tide provides defense greater capability at lesser cost than it could have by "going it alone." Defense systems based on commercial information technology enjoy near-continuous upgrades: the commercial "cycle time" to produce new products is 18 months; a program lifetime in DOD can be 18 *years*. DOD also saves money by outsourcing functions that are more efficiently performed by the commercial sector, where natural market adjustments replace painful political adjustments. Since our allies in both the Atlantic and Pacific are drawing on the same globalized technology base as we are, alliance interoperability – the capacity to fight as a coalition – and political solidarity will be strengthened.

Commercialization and globalization are, in their individual ways, both inexorable. So it is a good thing that they are also beneficial for national security. But the benefits will not be realized without effort, and they do not come without a cost. Even under the best of circumstances the scorecard is positive only because the benefits outweigh the risks.

During the Cold War, the offset strategy required us simultaneously to field better defense technology than potential opponents, and simultaneously to retard their access to the same capabilities. These should still be the objectives if we are to keep America's technological advantage in the post-cold war world, but they will need to be attained in a fundamentally different environment.

As Figure B shows, military advantage will accrue to the military that most rapidly adopts and adapts commercial technology to form defense systems-of-systems. The United States will have to "run faster" than opponents who have access to the same globalized, commercialized technology base. Running faster requires, first, acquisition reform to facilitate DOD's buying of commercial technology and second, an industrial base strategy to ensure that a healthy defense industry with close ties to commercial industry exists to do the running.

Slowing down the opposition also requires two ingredients: an export controls system to stop the flow of technology by sale; and a security system to prevent espionage and sabotage. In each case today's system is an inheritance from the previous era and is destined to become outdated as the world moves to the right in Figure B.

Let me focus on the export controls issue, where the implications of Figure B are very serious. The right-hand column of Figure B describes a world that challenges the very foundation of export controls policy, especially controls on dual-use items. We are not yet in the world to which current trends seem to be carrying us. But in not too long we will be closer to the state described on the right-hand side than to the state described by the left-hand side.

In the world to which we seem to be headed, it will still be possible to describe defense applications of technology, but difficult to speak of defense technology *per se*: most technology used by defense will be drawn from the commercial sector. Moreover, that technology will not come from American companies but from a global base. Thus U.S. denial of that technology to all potential enemies will be impossible. Opponents will have access to the same technology, and U.S. military advantage must therefore come from being better and faster at *adapting* technology to military use rather than trying to retain exclusive use of technology.

In that world, secrets will not inhere in the underlying technologies but in their military applications. This circumstance will stand on its head the so-called "Bucy principle" of Cold War export controls that the object of control should be technologies rather than artifacts. It also makes obsolete the "hermetic seal" ideal for the export controls system of the Cold War. In the hermetic seal model, an impermeable barrier was put around technology underlying defense applications. This was practical since most such technology arose in facilities directly or indirectly controlled by the United States and indeed a great deal of it originated in DOD-controlled laboratories under government sponsorship.

Debate during the Cold War – which was intense – revolved around how much of this defense technology should be allowed to diffuse *out* of defense and *into* international commerce: in effect, where to place the hermetic seal to balance the security risks of outward diffusion against the commercial benefits. But in the asymptotic state of Figure B, technology diffuses *into* defense *from* international commerce. The institutions generating this technology are not directly controlled by government, nor are they American. The issue in the new world is not balancing security and commercial interests. A host of new issues instead arise. The export controls system inherited from the Cold War does not address these issues. New approaches are needed.

One issue is to define which items are still "controllable" in practical terms. Laptop computers provide an example. These are obviously useful items for potential military opponents, and most of the candidates (North Korea, for example) cannot make them indigenously for their own military applications. It is surely desirable to deny engineers working on the North Korean missile program the use of PCs. But even if the United States government attempted to control all international sales of such computers, it could not stop the North Korean missile engineers from obtaining them. PCs are sold in such large numbers around the world, including in countless retail stores, that clandestine procurement by the North Koreans could not

be stopped. Commercial and foreign availability of the technology grows more widespread every day. Since PCs become more potent every day also, it is evident that applying export controls to them is not only a futile gesture – controlling the uncontrollable – but that a real security price is paid for living in the commercialized, globalized world. The rising tide of technology raises all boats, including those of potential opponents.

Still, all is not hopeless for making export controls effective even in the future. What is needed is not a hermetic seal, but a more discriminating system that might be likened to the human immune system. The human body does not attempt to isolate itself from all pathogens – it is not possible to breathe, eat, and come into contact with the rest of the natural world and not encounter health risks. The immune system is a highly adapted system for detecting risks and for responding to them in a proportional and discriminating manner. The same approach is needed for export controls. The first step is to have the capability to assess the levels of technology that are widely available. This analysis will indicate that for some defense items (but less and less often for "technologies") it will still be possible to configure a hermetic seal that keeps pariah states out. Increasingly, that seal cannot be applied around the United States but around a larger group of nations that collectively manufacture and market the items in question. The key here is to arrive at agreement among leading nations about which items to control and which countries to deny. Elsewhere regulators will have to permit widespread sales of sensitive items, but to require exporters (backed by government inspectors) to certify that the end user of the item is not a proscribed foreign military destination. Additionally, by refocusing scarce intelligence and enforcement resources on the truly threatening transfers rather than uncontrollables, our security will be better protected. All these adaptations await the export controls system if it is to retain any effectiveness.

CONCLUSION: OVERCOMING COMPLACENCY

The impressive performance of the American military against the relatively minor challenges of the post-Cold War era to date has made it the envy of militaries around the world but has also engendered a dangerous complacency in American national security thinking. As a result the United States is not making four related adaptations needed to ensure that today's superiority endures. Strategy should focus on a preventive defense approach to the most important long-term threats to security rather than to intervening in minor conflicts. Budgeting should reflect both preventive approaches and protection against asymmetrical threats if prevention fails. The DOD's organization should give homes to the growing number of new missions that have "no one in charge." And defense industrial policy must adapt to the commercialization and globalization of the industrial base upon which America's technological edge rests.

Calling attention to these four interrelated challenges might seem out of tune with the fact – which is emphatically true – that the United States has the most proficient military in the world, has demonstrated that fact in several recent contingencies, and will have no competitor for many years. Still, the effectiveness of the U.S. military in protecting security is not a birthright or fact of nature. To keep it will require self-scrutiny and an active effort to combat complacency. And without change it cannot meet the challenges of the future.

It is far from obvious that these changes will be made, or made in time. When the important threats are those that *might be* rather than those that *are*, when success against the lesser challenges of the moment appears to create a *prima facie* case that all is well, and where the fundamental shifts occurring in the environment are nonetheless gradual and subtle, there is no "forcing function" compelling attention to the need for change. There will be no public clamor for it. The clamor will come later, when the relative safety first post-cold war era seems like a distant golden age and the question asked of defense leaders will be, "Who lost it?"

FIGURE B

THEN (Cold War)	**NOW (2000)**	**WHERE TRENDS ARE TAKING US**

MILITARY ADVANTAGE

· Conferred by national possession of defense-unique leap-ahead technology that potential opponents cannot get.	· Conferred by rapid adoption/integration of (mostly) commercial technology/components into defense-unique systems-of-systems more rapidly than opponents (who have access to most of the same technology).
Defense Technology	
· Originates in defense technology base	· Originates in commercial technology base
· that is embedded in defense companies	· that is embedded in commercially-driven companies
· residing in the U.S.	· that are global
· for which defense is main driver.	· for which defense is niche player.
Defense Industry	
· Multi-tiered system of national (U.S. and European national) companies, primes and subs,	· Is centered in EITHER two U.S. and one pan-EU prime firm, the U.S. companies competing in the U.S. and all three competing globally OR two trans-Atlantic prime firms competing globally,
· that develop defense-unique technology and embed it in components,	· that buy commercial technology and components,
· from which they engineer systems.	· from which they engineer systems and systems-of-systems.
Industrial and Personnel Security Policy	
· A hermetic seal,	· An immune system,
· Based on denial of access,	· based on risk assessment and flexible response,
· Surrounding a well-defined defense technology base	· Operating in the midst of a global industrial organism
· That is American.	· that has no national identity.
· Protects technology (“secrets”),	· Protects systems architectures and unique military capabilities (“secrets”),
· Trusts Americans,	· trusts no one,
· Accepts dependence only on Americans.	· but depends on everyone.

THE HONORABLE ASHTON B. CARTER

Ash Carter is Ford Foundation Professor of Science and International Affairs at Harvard University's John F. Kennedy School of Government and Co-Director, with William J. Perry, of the Harvard-Stanford Preventive Defense Project.

From 1993-1996 Carter served as Assistant Secretary of Defense for International Security Policy, where he was responsible for national security policy concerning the states of the former Soviet Union (including their nuclear weapons and other weapons of mass destruction), arms control, countering proliferation worldwide, and oversight of the U.S. nuclear arsenal and missile defense programs; he also chaired NATO's High Level Group. He was twice awarded the Department of Defense Distinguished Service medal, the highest award given by the Pentagon.

Carter continues to serve DoD as an adviser to the Secretary of Defense and as a member of both DoD's Defense Policy Board and Defense Science Board, and DOD's Threat Reduction Advisory Council. Carter also serves in an official capacity as Senior Advisor to the North Korea Policy Coordinator, William J. Perry.

Before his government service, Carter was director of the Center for Science and International Affairs in the Kennedy School of Government at Harvard University and chairman of the editorial board of *International Security*. Carter received bachelor's degrees in physics and in medieval history from Yale University and a doctorate in theoretical physics from Oxford University, where he was a Rhodes Scholar.

In addition to authoring numerous scientific publications and government studies, Carter was an author and editor of a number of books, most recently *Preventive Defense: A New Security Strategy for America* (with William J. Perry). Carter's current research focuses on the Preventive Defense Project, which designs and promotes security policies aimed at preventing the emergence of major new threats to the United States.

Carter is a Senior Partner of Global Technology Partners, LLC, a member of the Advisory Board of MIT Lincoln Laboratories, the Draper Laboratory Corporation, and the Board of Directors of Mitretek Systems, Inc. He is a consultant to Goldman Sachs and the MITRE Corporation on international affairs and technology matters, a Member of the Council on Foreign Relations, and a Fellow of the American Academy of Arts and Sciences.