6

Keeping the Technological Edge

ASHTON B. CARTER

WITH MARCEL LETTRE AND SHANE SMITH

Rather than attempting to match the Warsaw Pact tank for tank or soldier for soldier during the Cold War, the United States evolved an "offset strategy" whereby superior American technology would counterbalance greater opposing numbers.[1] The offset strategy had two components. The first was to field superior technology through aggressive pursuit of military R&D, and developing a high-technology defense industrial base. The second was to deny opponents that technology through a system of export controls and protection of technological secrets.

This strategy of superiority and denial worked: the offset strategy secured deterrence of the numerically superior forces of the Soviet Union and its allies, and forced the Soviet Union to bankrupt itself in the pursuit of military technology it could not easily obtain from the West. Elsewhere, denial slowed proliferation of weapons of mass destruction. The success of the offset strategy was demonstrated in 1990–91, in a war no one had anticipated: in DESERT STORM, U.S. reconnaissance satellites, stealth aircraft, precision weapons, and other technologies — unmatched by any other military — made quick work of Iraq's Soviet-equipped army. Americans liked the offset approach, and superiority and denial remain the distinctive American

The insights and information provided by Denis Bovin, Herbert S. Winokur, Jr., and Philip A. Odeen are gratefully acknowledged. They bear no responsibility for errors of fact or judgment.

1. William J. Perry, "Desert Storm and Deterrence," *Foreign Affairs*, Vol. 70, No. 4 (Fall 1991).

way of defense, now applied to the post–Cold War era's new missions.

But a challenge looms to the preservation of America's technological edge in the post–Cold War era. The challenge results not from new types of military threat, but from trends in the industrial and technology base that undergirds the U.S. technological edge in military affairs. This base, once largely the creation of Department of Defense (DOD) spending and almost exclusively American, is increasingly becoming commercialized and globalized. *Commercialization* refers to the fact that the technology of central importance to national security, especially information technology, increasingly originates in commercial rather than defense companies, without the sponsorship of DOD and outside its control. Related to commercialization is the *marketization* of the defense industry: defense companies must justify themselves to shareholders by the same standards of profits and cash flows as civilian commercial companies, and the industry is today having difficulty withstanding the market's pressures. *Globalization* is the related trend whereby leading technology companies are increasingly global rather than purely American in their outlook, ownership, workforce, and markets.

The United States cannot accomplish the national security objectives its people expect without the offset strategy, but the Pentagon cannot carry out the offset strategy without access to a strong industrial and technology base willing to serve its needs. Maintenance of this base in the face of commercialization and globalization requires that the Defense Department adapt its approaches toward maintaining U.S. technological superiority. Meanwhile the denial component of the offset strategy requires a new definition of the "secrets" that must be protected if it is to remain effective. This chapter describes three types of adaptation that should be encouraged by the new U.S. administration and its defense team. The first two seek to preserve the *superiority* dimension of a continuing offset strategy: first, aligning defense procurement practices with market forces, and second, remaining the world's fastest and best integrator of commercial technology into defense systems. The third adaptation is meant to preserve the *denial* dimension: protecting secrets by means of an "immune system," rather than a hermetic seal as during the Cold War.

ALIGNING DEFENSE PROCUREMENT PRACTICES WITH MARKET FORCES

DOD must have access to an industrial base to which it can turn for superior military systems. Commercialization requires DOD to align its own practices more closely with the market forces affecting the commercial companies that increasingly supply vital technology for defense, and the defense companies that integrate technology into military systems. This is emphatically not a call for an "industrial policy" that would prop up weak defense companies and accentuate the isolation of the defense industry. Instead, the United States needs an approach that works *with* rather than *against* market forces, leveraging commercialization to secure the needs of defense. Globalization means facing the implications of trans-border and especially trans-Atlantic links within the defense industry.

REMAINING THE WORLD'S FASTEST INTEGRATOR OF COMMERCIAL TECHNOLOGY INTO DEFENSE SYSTEMS ("RUNNING FASTEST")

Second, the U.S. military must be the world's *fastest* adapter and adopter of commercial technology into defense systems. Potential opponents will also have access to much state-of-the-art technology, since they can purchase it on the open global market. Thus DOD must "run faster" than others, rapidly feeding on the global base rather than relying almost exclusively on its own sponsored R&D as it did during the Cold War.

PROTECTING SECRETS THROUGH AN IMMUNE SYSTEM RATHER THAN A HERMETIC SEAL

Third, the United States must abandon the "hermetic seal" model: denying technology to others by seeking to put an impermeable barrier around the American defense technology base. Globalization and commercialization mean that crucial technology now arises *outside* this barrier as well as inside, and cannot be protected by a simple barrier. Second, it is in the U.S. interest to have technology diffuse *inward* to defense from a globalized, commercialized base, and in these cases the hermetic seal approach impedes DOD from "running faster." Third, the unique sources of U.S. military advantage that will need to be protected will increasingly rely on U.S. systems-engineering capability, rather than component or subsystem technologies. The latter will be widely available and impractical to contain. The U.S. export controls

system must focus on unique sources of military advantage rather than technology across the board if it is to be truly effective at slowing the competition. Finally, accompanying the new meaning of secrets must be new ways of protecting them. Much technology that is "foreign" will find its way into defense systems and must somehow be made trustworthy. Meanwhile the new technology of networks and compact data storage make "insiders" as potentially dangerous as "outsiders." To deal with these changes, rather than applying simplistic and outdated bureaucratic rules, export controls and security systems must be capable of identifying and reacting to real security threats, just as the human immune system works not by trying to isolate the body from the environment, but by sensing dangers and combating the most dangerous ones selectively.

The magnitude of the conceptual challenge to America's technological edge, and the profound nature of the adaptations needed in these three areas, can be seen from Figure 6-1, which contrasts the technological context of the Cold War's offset strategy with the world toward which commercialization and globalization appear to be carrying us, which differs from the Cold War world in virtually every determinant of superiority and denial.

Can the offset strategy and America's technological edge be preserved in the new world? While commercialization and globalization create a strange new world for defense, on balance they are strongly favorable. Riding the commercial technology tide provides DOD greater capability at lesser cost than it could have by "going it alone." Defense systems based on commercial information technology enjoy nearly continuous upgrades: the commercial "cycle time" to produce new products is typically 18 months or less, compared to a program lifetime in DOD that might be years or even decades. DOD also saves money by outsourcing functions that are more efficiently performed by the commercial sector, where natural market adjustments replace painful political adjustments. Strong market forces, if properly harnessed, can be used to keep the defense industry innovative and efficient (for more on this point, see Chapter 7). Since our allies in both the Atlantic and the Pacific are drawing on the same globalized technology base as we are, alliance interoperability both the Atlantic and the 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.

Figure 6-1. COLD WAR .... ⇨ .... FUTURE

Defense 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 United States	⇒ that are global
▫ for which defense is main driver.	⇒ for which defense is niche player.
Defense Industry	**Defense Industry**
▫ is a multi-tiered system of national (U.S. and European national) companies, primes, and subs;	⇒ is centered in a few large prime contractors that are: *either* separate U.S. and pan-European continental champions protecting home markets and competing in third markets (Fortress America, Fortress Europe); *or* fully merged trans-Atlantic primes competing across the Atlantic and globally; *or* U.S. and pan-European primes united by joint ventures, strategic partnerships, and teaming arrangements; and competing across the Atlantic and 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.
Export Control and Industrial & Personnel Security Policy	**Export Control and Industrial & 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 without checking,
▫ accepts dependence only on U.S. citizens.	⇒ but depends on everyone.
Military Advantage	**Military Advantage**
▫ is conferred by national possession of defense-unique leap-ahead technology that potential opponents cannot get.	⇒ is conferred by rapid adoption and integration of (mostly) commercial technology and components into defense-unique systems-of-systems more rapidly than opponents (who have access to most of the same technology).

Commercialization and globalization are both inexorable, so it is a good thing that they can be beneficial for national security if they are embraced rather than resisted by DOD. But if DOD were to persist in old approaches to superiority and denial, the new trends will both erode the technological edge and open up new vulnerabilities. Even under the best of circumstances, the scorecard can be positive for the offset strategy only if the increased benefits can be made to outweigh the undeniably greater risks of the new world. It is a policy choice whether the United States will fully avail itself of the benefits and fully mitigate the risks. If it does not, the alternative is a bleak one: when the Pentagon turns to industry to support the offset strategy, it might find no companies willing or capable to do so.

Commercialization

Commercialization is affecting defense in two ways: first, most new technologies of relevance to defense originate in the commercial sector. Second, defense companies are undergoing marketization — or increased focus on shareholder value — and are consequently under intense pressure in a competitive industrial marketplace that is demanding higher margins, valuations, and growth.

GROWTH OF THE COMMERCIAL TECHNOLOGY BASE

In the days of the 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.

To appreciate the facts, contrast the situation in 1980 with the year 2000. According to the National Science Foundation, the amount of money spent on scientific research and development 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.[2] The U.S. Department of Defense sponsored about $40 billion, or one-sixth of the entire total. In the year 2000, by contrast, the corresponding global total for R&D spending is $360 billion, half again as much, in

2. National Science Board, *Science and Engineering Indicators—1998*, NSB 98-1 (Arlington, Va.: National Science Foundation, 1998), pp. 4–5, 4–24, 4–37.

constant dollars, as in 1980. The United States still accounts for half the total, about $180 billion. But today DOD furnishes only one-twelfth of the total: half its 1980 share.

Moreover, there are indications that this shrinking portion is not being used to press the technological frontier. Much more of DOD's R&D spending is being used for downstream engineering of mature systems than for research into new enabling technologies: that is, more "D" than "R" (88 percent development and 12 percent research in 2000, compared to 69 percent and 31 percent, respectively, in 1980).[3] In terms of applications, much defense R&D today goes to keep old "legacy" systems going or to prop up faltering programs, rather than launching new leap-ahead military systems. Independent research and development (IR&D), conducted within defense companies and cost-shared with DOD, used to be a means for keeping defense companies innovative; this, too, is declining, amounting in 2000 to only half its mid-1980s value.[4] All these indices point to one fact: tomorrow's defense innovations will largely be derivatives of technology developed and marketed by commercial companies for commercial motives.

3. Ibid., p. 4–23.

4. Independent R&D (IR&D) refers to basic or applied research, development, or systems or other concept formulation studies devised and conducted within industry. Each year the company proposing an IR&D program submits its plans to DOD. When DOD agrees that a portion of the proposed program contributes to DOD's purposes, it permits the company to include that portion in its indirect costs (overhead) on its contracts. In other words, DOD reimburses industry for a portion of industry's own R&D. The overall amount of IR&D has been declining. More seriously, over time the government is tending to dictate more of the programs, making them less truly the result of the independent judgment of non-government scientists and engineers. See John D. Moteff, *Defense Research: A Primer on the Department of Defense's RDT&E Program*, Congressional Research Service Report 97-316, May 5, 1998; Frank Lichtenberg, "U.S. Government Subsidies to Private Military R&D: DOD's IR&D Policy," *Defense Economics*, Vol. 1 (1990); Testimony of Under Secretary of Defense for Acquisition, Technology, and Logistics Jacques Gansler before the Military Research and Development Subcommittee, House Armed Services Committee, March 1, 2000; and Defense Science Board (DSB) Task Force Report, *Preserving a Healthy and Competitive U.S. Defense Industry to Ensure our Future National Security*, Summer 2000.

A telling example is software. Since the defense market is a small portion of the overall software market, it has no alternative but to adopt the most popular software systems. The alternative is to develop its own hothouse software, which would inevitably be inferior and more costly than the widespread commercial versions. In all but narrow custom niches, DOD has no alternative but to ride the tide of commercial development.[5]

The cases of information technology, biotechnology, and space technology show the variety of challenges posed by commercialization. As the software example highlights, the cutting edge in information technology (IT) has passed from defense to commercial companies. Once upon a time DOD pioneered the microchip, massive parallel processing, the Internet, software engineering techniques, and other technologies that are now spearheaded by the well-financed commercial e-revolution. In all but niche areas, DOD will be a consumer rather than an originator of technology in this sector. But at least in the IT sector, DOD has strong engineering capability in its own laboratories and industry, a legacy of its earlier preeminence. In biotechnology, by contrast, there is no such legacy. The biotechnology industry has no tradition of working for defense. Indeed, in some cases biotechnology companies have exhibited an aversion to working on defense applications, citing onerous federal acquisition rules and sometimes fearing damage to their reputations. Yet biotechnology poses fearsome possibilities for biowarfare and bioterrorism. Indeed, it is likely that the biotechnology revolution will prove to be as profound as the information revolution in altering the possibilities for armed conflict, both offensive and defensive. The United States has rightly foresworn offensive biowarfare, but DOD will need protective devices such as detectors and vaccines. For these technologies, DOD must establish a working relationship with the new biotech industry. A third example is that of space technology, which occupies a position between IT and biotechnology in terms of the impact of commercialization. DOD and NASA still occupy a commanding position in this field, but the number of commercial communications, imaging, navigation, and launch services busi-

5. Defense Science Board studies in 1987 and 1994 analyzed the issue of software management, and other DSB studies on international arms cooperation (1996), information warfare (1997), and globalization and security (1999) have continued to draw attention to the software challenges for DOD.

nesses is growing. The flow of technology, which has run from DOD to commerce since the Space Age began, will in time begin to reverse direction.

To benefit from commercialization, DOD must buy from commercial companies. This sounds easy enough, but current rules and procedures governing the spending of public monies frequently get in the way. These rules impose accounting burdens on companies selling to defense and frequently involve contracting vehicles that are foreign to commercial practice. Some commercial companies, simply unwilling to tolerate DOD's eccentricities, refuse to sell to the Pentagon. Their place is taken by specialized defense-only companies adapted to the arcane ways of the Federal Acquisition Regulations (FAR); they generally pass on their high costs and inefficiencies to the military. This problem has long been recognized, and in recent years a determined start has been made at acquisition reform.[6] However, the process is unfinished. At stake is much more than simple budgetary efficiency. If the U.S. military cannot "run faster" than other militaries, it cannot sustain the technological lead that is the key to its preeminence.

MARKETIZATION OF THE DEFENSE INDUSTRY

For companies specializing in engineering defense systems, whether using commercial or defense-developed technology, the business climate has changed as dramatically as the international environment since the end of the Cold War. In the mid-1970s, then Chief of Staff of the U.S. Army Edward C. Meyer warned that the United States had a "hollow army." There is now more reason to fear a hollowing out of the industry upon which America's technological edge depends.

The U.S. defense industry is still by far the world's largest and most technologically proficient. The U.S. defense budget, $279 billion

6. Calls for acquisition reform began in the 1980s. See Packard Commission, *A Quest for Excellence*, Final Report by the President's Blue Ribbon Commission on Defense Management, The White House, June 1986. See also Chapter 6 of Ashton B. Carter and William J. Perry, *Preventive Defense: A New Security Strategy for America* (Washington, D.C.: Brookings Institution Press, 1999); and Steven J. Kelman, Michael J. Lippitz, and John P. White, *Reforming the Department of Defense: The Revolution in Business Affairs*, Preventive Defense Project Publication Series, Vol. 1, No. 4 (1999). See also Chapter 7 in this volume by Michael J. Lippitz, Sean O'Keefe, and John P. White.

in FY 2000, is at least 20 percent larger than the aggregate of all its European and Asian allies.[7] Moreover, this budget is increasing, whereas Europe's budgets are flat or declining. The critical investment portion of the defense budget, covering procurement and R&D on new weapons, is $92.5 billion in FY 2000, and is growing more rapidly than the overall budget. This is about 50 percent more than is spent on defense investment by all the U.S. allies combined. However, the U.S. defense industry has shrunk dramatically during the 1990s, as the rest of the economy has grown robustly. Today's defense budget is only 69 percent of its 1985 peak (measured in FY 2000 dollars), and investment is only 55 percent.[8] The FY 2000 defense budget consumes 3 percent of gross domestic product (GDP), just half of 1985, when it consumed 6 percent of GDP.[9] Employment in the defense industry had dropped to 878,000 in 1999, from 1.4 million in 1990 (a decline of well over one-third).[10]

DOD and the industry attempted to contend with the shrinking market by consolidating the prime contractor base. By 1999, just eight consolidated primes existed where there had been 36 in 1993.[11] The shakedown has begun to affect the lower tiers of the defense industry — companies that supply the primes with subsystems and crucial

7. *Department of Defense Annual Report to the President and Congress*, 2000, Appendix B: Budget Tables; Office of the Undersecretary of Defense (Comptroller), *National Defense Budget Estimates for FY 2001*, Table 1-1 (March 2000). For allied defense expenditures, see *World Military Expenditures,* Center for Defense Information, at <http://www.cdi.org/issues/wme/>; *CIA World Factbook,* January 1, 1999, country listings at <http://www.cia.gov/cia/publications/factbook/country.html>; country summaries in *The Military Balance 1999–2000* (London: International Institute for Strategic Studies, 1999); and Loren B. Thompson, *The Post-Deconstruction Defense Industry: Now What?* Lexington Institute, September 9, 1998.

8. Office of the Undersecretary of Defense (Comptroller), *National Defense Budget Estimates for FY 2001*, Table 6-1 (March 2000).

9. Office of the Under Secretary of Defense (Comptroller), *National Defense Budget Estimates for FY 2001*, Tables 6-1 and 7-7, (March 2000).

10. Bear Stearns, *The Consolidation of the Defense Industry: Winners and Losers*, February 7, 2000.

11. Bear Stearns, *The Consolidation of the Defense Industry: Winners and Losers*; and Bear Stearns, *The Consolidation of the Aerospace Industry/Defense Merchant Supplier Base*, April 17, 2000.

technology. The number of these companies has decreased by about half since 1993, from 85 to 44. But further consolidation at the second and third tiers is needed: many of these companies are too small by themselves to provide the critical mass that is necessary for innovation. They should be encouraged to merge with each other or with units spun off from the primes (units regarded as "non-core") as the latter rationalize their portfolios.

Accompanying the dramatic change in industry structure is an equally important change in the types of products DOD is asking these firms to produce. An increasing share of the procurement budget goes to upgrading the electronic and weapons systems aboard aircraft, ships, spacecraft, armored vehicles, and intelligence and command centers, rather than to new procurement of the platforms themselves. These subsystems are themselves more complex: they are truly systems in their own right and not just "black boxes" added to the platforms as if in afterthought. The electronic "innards" are an increasing share of the value of new platforms. For example, the electronic warfare suite aboard tactical aircraft now under development is a complex system uniting radar, targeting, communications, electronic countermeasures, and attack warning functions previously attached to the aircraft system as separate subsystems.

The cost of developing defense systems is high because of their increasing complexity, and these costs can rarely be recovered by contractors, as they once were, in long production runs. In the 1980s, contractors absorbed losses on R&D contracts in the expectation that they would recover the losses in production contracts: every dollar of defense R&D in 1985 was followed by three dollars of procurement spending on the weapons developed. Today these losses cannot be recovered: only about $1.50 of procurement follows each dollar of R&D.[12] The companies accordingly perform less R&D.

Today's defense *systems* — platforms, weapons, and sensors — are being incorporated into synergistic *systems-of-systems*.[13] For example, a reconnaissance aircraft might spot a target — perhaps an air defense battery — and give its coordinates to a precision weapon, which then destroys the air defense battery. Elimination of the air de-

12. Office of the Undersecretary of Defense (Comptroller), *National Defense Budget Estimates for FY 2001*, Table 6-1.

13. The term "system-of-systems" was coined by the Defense Science Board in 1990.

fense in turn makes the collection of further targeting data by the aircraft easier, and the cycle continues. The key skill this requires of defense companies, therefore, is systems engineering: making defense-unique systems and systems-of-systems (for the primes) and complete subsystems (for the second tier) from a base of underlying technology that is increasingly commercial. Both military advantage (the offset strategy) and economic value to the industry (cost of the program and, accordingly, profits) therefore increasingly inhere in the systems engineering rather than in the technology underlying individual components.

Firms attempting to stay in the defense business in the face of these changes must do so under increasing market pressures. On the whole, of course, the decision by the United States after World War II to rely on the private marketplace to serve most of its national security needs has been vindicated. Nations that opted to preserve government-owned and operated arsenals have regretted that decision. However, DOD's needs for a healthy defense industry to preserve the offset strategy are not now well aligned with the market forces pressing on the industry.

First, the defense industry must compete in the stock market for capital. Here the signs in recent years are negative. The newly consolidated prime contractors, saddled with debt as a result of overpaying during their consolidation binge, have seen their credit ratings plunge. A stock market looking for high margins, growth, and predictable cash flows has observed that the primes have been subject to increasing government pressure on profits, abrupt terminations of programs, and flat or decreasing defense spending for a decade. The result is sunken market capitalizations of the major defense companies, during a period of overall rapid growth in stock market valuations. The total market capitalization of the defense industry had become, by the end of 1999, about half that of Wal-Mart and a quarter that of Microsoft.[14] There is plenty of blame to go around for this predicament. The big primes paid too much to acquire one another, and the resulting giants are deep in debt. They are having difficulty managing centrally the ungainly portfolios they have amassed. DOD promised to share the savings from consolidation

14. Market capitalization figures as of the end of calendar year 1999 are from Defense Science Board Task Force Report, *Preserving a Healthy and Competitive U.S. Defense Industry*.

with industry, but the efficiencies realized were smaller than hoped and DOD reneged on its pledge to share them. Finally, the defense industry has suffered along with other "metal-bending" industries from the stock market's infatuation with "dot-coms." In this climate, defense companies cannot afford to make investments in future defense systems: they are concentrating on making it through the next quarter. They often see little market incentive to emphasize innovation and efficiency: in contrast to the commercial market, innovation rarely feeds further market growth, while the DOD or Congress either blocks plant closings or captures the benefits of cost-cutting measures for itself.

Second, marketization implies that managers, directors, and stockholders have alternatives for the capital they are devoting to defense. Large conglomerates that formerly pursued both defense and non-defense businesses voted with their feet during the 1990s: the list of premier U.S. industrial companies that have exited the defense market reads like a Who's Who of industrial America, including IBM, Texas Instruments, Ford, Chrysler, GE, and Westinghouse. Meanwhile, the "new economy" companies are wholly absorbed in the pursuit of rapidly growing commercial markets rather than the constrained defense market.

Third, defense companies compete in a labor market where executives are rewarded with stock options and engineers want to be on the cutting edge. Here too, the market appears to be working against defense. The drop in defense stocks has wiped out the fortunes of many of its top and middle managers. They, like their stockholders, are wondering why they should remain in the defense industry. Scientists and engineers who relish the challenge of systems engineering will still find defense work rewarding, but those whose skills are focused on the underlying technology (especially information technology) are leaving defense for commercial industry.

Defense must find ways to align its needs under the offset strategy to the market forces in which industry must survive. Properly aligned, market forces will harness the dynamism of the modern American economy to its national security needs as well as its material welfare. The alternative would be an isolated and increasingly backward defense industry that will not support the offset strategy.

Globalization

The industry that will provide the underlying technology to support U.S. defense in the future is not only increasingly non-defense, as described above, but increasingly non-American. Defense prime contractors still tend to be national or regional — American, European, etc. — in their orientation. But their suppliers of technology and subsystems are increasingly globalized companies; their markets are global; and even their ownership is globalizing. Each of these trends to globalization has important implications for DOD.

Once again, software provides an important example, this time of the globalization of suppliers. For example, India is fast becoming the world center of software engineering.[15] India may soon far surpass the United States in lines of computer code it produces that find their way into widespread commercial — and thus perforce defense — applications furnished to DOD by supposedly "U.S." companies.

Globalization of defense markets is occurring more slowly, but perceptibly. Since the Cold War ended, the worldwide arms market has shrunk by about one half. U.S. defense companies, however, have increased their market share, and with Pentagon procurement budgets shrinking or flat until the past few years, many firms have looked to overseas sales as a key source of growth. Still, U.S. firms are far less dependent on exports than are European firms. The U.S. defense sector exports about one-quarter of its production, whereas European firms tend to sell half to three-quarters of their output abroad.[16] European firms are eagerly eyeing the U.S. defense market, which is large and, unlike European acquisition budgets, growing (although

15. In 1999, the Indian software industry posted revenues of $3.9 billion, of which $2.7 billion were accounted for by exports. The number of engineers graduating in the field, a current force of 200,000 software engineers, and the country's comparative labor advantage in low wages pushed industry growth at annual rates in excess of 50 percent through the 1990s, and an Indian national task force has called for building it up into an $85 billion per year business by 2008 (predictions that struck some as overly conservative). See Pankaj Ghemawat, Murali Patibandla, and William J. Coughlin, "The Indian Software Industry at the Millennium," *Harvard Business School Case*, N9-700-036, September 7, 1999.

16. *Report of the Defense Science Board Task Force on Globalization and Security*, December 1999, pp. 9–11.

slowly). Market globalization creates two sources of trans-Atlantic tension. First, U.S. companies and European companies compete with each other for sales around the world. Second, disagreements between European countries and the United States about which foreign customers might end up as foes rather than friends are amplified by the market pressure on both U.S. and European companies to sell enhanced versions of weapons to third countries. Air defense systems and anti-ship systems are two categories of military systems where the capability that can be procured on the open market has increased dramatically in recent years because the United States and its partners have not been able to agree on restraints.

Globalization of ownership is the slowest of the trends to affect the defense industry. While globalization of ownership of commercial companies is far advanced and inexorable, ownership of defense companies in Europe is only now completing the shift from the state to private hands. The corresponding process occurred decades ago in the United States as the arsenal system was dismantled. Whether the U.S. 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.[17] The outcome has important implications for defense policy.

At one extreme, as shown in Figure 6-1, the defense industry might not follow commercial industry in the globalization trend. The result would likely be national defense companies in the United States, on the one hand, and on the other, pan-European defense companies (resulting from mergers and acquisitions among British, French, German, Italian, and other firms under the pressure of the European Union), all acting with their governments' help to protect their home markets, and competing ferociously for the export market. An economic rift within the North Atlantic 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

17. See, for example, "Pentagon Mulls Overseas Sale of Lockheed's Sanders Unit; Deal May Test Limits," *Defense Daily,* June 19, 2000, p. 1; John D. Morrocco, "Consolidation Poses Transatlantic Quandary," *Aviation Week & Space Technology,* July 24, 2000, p. 4; Pierre Sparaco, "U.S., Europe Explore Transatlantic Partnerships," *Aviation Week & Space Technology,* September 13, 1999, pp. 37–40; Howard Banks, "Foreign Entanglements," *Forbes,* September 6, 1999, p. 5.

probably also 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 intermediate outcome seems most likely. While there might be some additional trans-Atlantic mergers and acquisitions among the large primes, there will surely be a host of other relationships that will tend to join continents and reinforce alliances: joint ventures, strategic partnerships, teaming arrangements, and consolidation of second and third-tier sectors. In addition to its political benefits, evolution towards a trans-Atlantic industry serving all allied defense establishments will also provide the classic economic benefits of free trade.

To enjoy the benefits of this form of intermediate globalization, the United States will have to work around three problems that are certain to arise. First, there seems little prospect of entirely free and open competition for U.S. and European defense dollars. National protection of jobs will require offsetting purchases every time the Pentagon buys weapons made in Europe (even if by an American-owned company), and vice versa. Cutting costs by combining manufacturing operations is usually a key economic motive in industry consolidation, but governments want to share work out among plants in different countries. Clearly the pressures to "buy American" or "buy French" will inhibit the business motives that lead to consolidation. Second, U.S. policy sharply limits offshore companies from exercising "foreign ownership, control, or influence" (FOCI) over defense companies that deal with classified information. The rules are especially strict when the U.S. company acquired by a foreign company does work on highly classified compartmented or "black" programs. This problem is a matter of trust in the ability of allies to protect secrets. A third problem sorely tests this trust: the United States and an ally with whom it has a defense business alliance might not agree about sale to a third-country destination of items produced jointly. Such items are, in essence, re-exports of U.S. technology from the foreign

company or joint venture. Are such re-exports subject to U.S. or rather allied export controls regulation and enforcement? Unless the nations agree on what arms and secrets should be controlled, and on destinations to be denied certain arms, international business ventures can be the source of inter-allied tension rather than solidarity.

New Meanings of "Secrets" and their Protection

The right-hand column of Figure 6-1 describes a world in which the very foundations of export controls policy are undermined, especially controls on items with inherent dual-use applications.[18] We are not yet in the future world to which current trends seem to be carrying us, but it will not be long before we are closer to it than to the world that became familiar during the Cold War.

In the future world, it will still be possible to describe defense *applications* of technology, but increasingly meaningless to speak of defense *technology* as such: most technology used by defense will be drawn from the commercial sector.[19] Moreover, that technology will not come exclusively from U.S. companies, but from a global base. Thus, permanent U.S. denial of such technology to all potential enemies is impractical. Rather, 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 the future world, secrets will not inhere in the underlying technologies but in their military applications. In the future, the basis of the U.S. edge in military technology will be the defense-unique systems and systems-of-systems — made mostly from commercial technology ingredients — and the systems engineering skills that go

18. For challenges stemming from these trends already faced by U.S. export control policies, see William A. Reinsch, "Export Controls in the Age of Globalism," *The Monitor: Nonproliferation, Demilitarization, and Arms Control*, Vol. 5, No. 3 (Summer 1999), pp. 3–6; and *Report of the Defense Science Board Task Force on Globalization and Security*, December 1999.

19. An example of the difficulty of distinguishing military from commercial technologies came in early 2000: Sony's new mass-marketed gaming console faced Japanese export regulations because its technology was deemed to be usable in a missile guidance system. "Sony Game Sparks Fears: So Powerful It Could be Used to Guide Missiles," *The Gazette (*Montreal*)*, April 17, 2000, p. B-4.

with them. It is their architectures and modes of operation that will be the secrets that need protection. This circumstance will stand on its head the principle of Cold War export controls, that the object of control should be component technologies. It also makes obsolete the "hermetic seal" ideal for the export controls system of the Cold War. Then it was practical to think of placing an ostensibly impermeable barrier around the technology underlying defense applications, since most such technology arose in facilities directly or indirectly controlled by the United States government; indeed a great deal of it originated in DOD-controlled laboratories under government sponsorship.

Intense debate during the Cold War revolved around how much of this defense technology should be allowed to diffuse *out* of defense and *into* international commerce; in effect, the issue was where to place the barrier in order to balance security risks against the commercial benefits of outward diffusion.[20] But the flow of technology is increasingly in the opposite direction: technology diffuses *into* defense, *from* international commerce. The institutions generating this technology are not directly controlled by government, nor are they exclusively American. The issue in the new world is not simply balancing security and commercial interests. Instead, a host of new and more complex issues emerge that the export controls system inherited from the Cold War is ill-prepared to address. New approaches are needed.

One challenge is to define which items are still "controllable" in practical terms. Laptop personal computers, for example, are obviously useful items for potential military opponents, and most control candidates (such as North Korea) are unable to make such items indigenously for their own military applications. It is surely desirable to deny engineers working on the North Korean missile program the

20. For historical and Cold War perspectives on export controls, see Richard T. Culpitt, *Reluctant Champions: U.S. Presidential Policy and Strategic Export Controls* (New York: Routledge, 2000); Gary K. Bertsch, ed., *Controlling East-West Trade and Technology Transfer: Power, Politics, and Policies* (Durham: Duke University Press, 1988); and the report from the National Academy of Sciences Panel on the Impact of National Security Controls on International Technology Transfers, *Balancing the National Interest: U.S. National Security Export Controls and Global Economic Competition* (Washington, D.C.: National Academy Press, 1987).

use of powerful laptop computers. But even if the United States were to attempt to control all international sales of such computers, it could not stop the North Korean missile engineers from obtaining them: laptop PCs are sold in such large numbers around the world, in countless retail stores, that clandestine procurement by the North Koreans could not be stopped. It is evident that applying export controls to PCs is futile — attempting to control the uncontrollable. Since PCs become more potent every day, a real security price will be paid for their ubiquity in the future world. The rising tide of technology eventually raises all boats, including those of potential opponents.

Still, all is not hopeless for making some export controls effective. 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 without encountering health risks. Rather, the immune system is a highly sophisticated system for detecting risks and for responding to them in a proportional and discriminating manner. The same type of approach is needed for export controls. It requires a better capability to assess the levels of technology that are widely available.[21] Such an 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 prevents potentially antagonistic states from acquiring them. Increasingly, that seal cannot be applied around the United States but must instead be placed around the group of nations that manufacture and market the items in question. The key here is to arrive at agreement among those nations about which items to control and which countries to deny. Elsewhere, regulators will necessarily have to permit widespread sales of sensitive items, but should require exporters (backed by government inspectors) to certify that the end user of particular items is not a proscribed foreign military destination. By refocusing scarce intelligence and enforce-

21. In determining controllability, the Commerce Department's Export Administration Regulations (Part 768, "Foreign Availability Determination Procedures and Criteria") currently focuses on an item's foreign availability: whether it is readily available "without effective restrictions" from sources outside the United States, and is in "sufficient quantity" and of "comparable quality" so as to render a control "ineffective in achieving its purpose."

ment resources on the truly threatening transfers rather than on the "uncontrollables," security will be better protected.

The current export controls system has few of the attributes of the immune system model. It shows all the signs of a government regulatory system in distress. Morale, training, and workforce skills are low.[22] Bureaucratic battles consume more attention than program execution. Slow processing of paper copies persists, even two decades into the era of office automation. Where there should be an underlying logic to guide the regulators' actions, instead there is layer upon layer of complex and arcane rules, many embedded in statutes written by different congressional committees and administered by different agencies.[23] Enforcing the rules takes precedence over accomplishing their purpose of stopping harmful transfers. Senior policymakers attempting reform cannot get a logical handhold; overwhelmed by the tangle of rules and put off by the intense infighting of the bureaucracy, they give up in frustration, leaving the field to political fringes and interest groups.

The export controls system can still serve a vital security function if it is properly adapted to the commercializing, globalizing new world of defense. The system must modernize and streamline, define a new conceptual basis for control, employ better intelligence concerning threats and assessment of foreign availability, emphasize enforcement as much as licensing, and make better use of other control tools such as end-use controls.

22. For example, recent reports from the Inspectors General of the controlling agencies noted frustration among their personnel resulting from such concerns as resource constraints, overlapping priorities, increasing responsibilities, and lack of guidance. An interagency report stated that nothing better than "on-the-job training was the primary training available" for licensing officers. Offices of the Inpectors General of the Departments of Commerce, Defense, Energy, State, Treasury, and the Central Intelligence Agency, "Interagency Review of the Export Licensing Processes for Dual-Use Commodities and Munitions," Report No. 99-187, Vol. I and II, June 18, 1999.

23. Currently, export controls are established by several different statutes: the Arms Export Control Act is administered by the State Department, the Export Administration Act by the Commerce Department, the Trading with the Enemy Act by the Treasury Department, and the International Emergency Economic Powers Act by the Treasury and Commerce Departments.

Fighting against traitors, spies, and saboteurs is not the usual stuff of high-level defense policymaking, but here too the changing technological context will require basic adaptations directed from the top. The Cold War security model here, too, was simply based on the hermetic seal. Once it was applied (after some controversy in the 1950s) to the communist bloc, the hermetic seal model became ingrained in the industrial and personnel security system. The system did not work perfectly, but the model was generally understood and accepted. The key attributes that signified trustworthiness were U.S. citizenship and, for those working in defense institutions, a security clearance. But in a globalized, commercialized world, many of the people who will make important contributions to maintaining the U.S. technological edge in defense will be outside both perimeters. At the same time, technology is changing the nature of the threat to information security. As shown by recent sensational cases — nuclear scientist Wen Ho Lee's downloaded files at Los Alamos, the computer hard drives that went missing at the same laboratory, and the "Love Bug" Internet virus — entirely new security risks are emerging. In the future world, secrets will be hard to define and even harder to confine. Globalization and commercialization present difficult problems. The hermetic seal approach to personnel and industrial security will be increasingly unable to protect secrets in the new environment. A very different and more discriminating approach is needed, and the immune system model is the appropriate one.

The way changing technology is posing new risks is perhaps illustrated best by the risks in the information technology area of cyber traitors, cyber spies, and cyber saboteurs, all of which are very different from their Cold War counterparts. For example, a computer network might be used for sharing intelligence information among analysts, for planning contingency operations, or for designing a secret weapon. A spy trying to get access to information on the network is barred from doing so by a system that controls access, such as by requiring passwords and by preventing workers who are using the network from tapping into information they do not need to know. Some workers have higher clearances than others, with senior managers having access to all the information. However, it is well known that the greatest security risk in this system is not the senior managers with the highest clearances, but rather the systems administrator who installs and operates the safeguards. That individual might be

able to alter the software that controls the system of passwords, allowing an accomplice broad and completely undetected access to the network.

Even having a completely reliable administrator to run the system does not provide full protection. The software that controls the passwords is part of an enormous network management program consisting of millions of lines of computer code. Increasingly, this is commercial software, even in the most secret defense networks. DOD cannot develop such complex software on its own (and it should not, since superior software in wide usage, periodically upgraded, can be bought cheaply). Substantial parts of this software are likely to have been designed in foreign countries by individuals without U.S. security clearances. Since the cost of computing and storage are falling so rapidly, developers have little incentive to streamline software, and so problems are often fixed by adding a new layer of software rather than redesigning from scratch. Since software is easy to change in this way, it is changed frequently and by many people. The result of all these factors is complex, opaque, "bloated" code. Software engineers agree that systems of this nature are so complex that there is simply no way to "verify" the software, that is, to make certain that its designers or modifiers have not embedded changes that would allow an outsider to get access to a network it controls: neither by scrutinizing all the lines of code, nor by insisting that all its authors have security clearances. Instead, some other means must be found for thwarting cyber saboteurs. Such methods do not follow the hermetic seal model. One method is to operate the software for a time, deliberately accepting the attendant risk, to see whether certain pieces of the software show suspicious patterns, e.g., are not called into use during normal operations and might have been added solely to permit clandestine penetration. A more radical method would be to open the software to the "hacker" community: if after a year or so this highly motivated and competent community has not penetrated the system, one may conclude that it is "secure" enough to begin using it for classified operations.

If information is difficult to confine in the networked world, it is also difficult to detect or even to destroy. Workers can download enormous amounts of information onto a high-density medium and walk out of the office with it. Early in 2000, two hard drives were reported missing from a vault at Los Alamos National Laboratory.

These two small devices reportedly contained all the data on U.S., foreign, and hypothesized makeshift bombs that would be required for protection against nuclear weapons terrorism and accident; such information would be invaluable to a terrorist. This incident illustrated the new problem of *density*: enormous amounts of information can be stored in compact media. Erasing stored data on such media does not destroy it; subtle traces remain on a hard drive that could allow information to be recovered. Even physically smashing a hard drive does not help: tiny fragments of the drive can contain large amounts of information, enough, for example, to reveal the nature of a secret project.

The ultimate challenge to *defining* secrets in the information age is presented by the unclassified World Wide Web itself. DOD has found that well-meaning information officers had placed on the Web seemingly innocuous and clearly unclassified information that, nonetheless, posed a threat. For example, a video walking tour through the home of the Chairman of the Joint Chiefs of Staff was, for a time, accessible on the Web, potentially giving terrorists just what they would need to plan an attack. In the past, it would have required painstaking and risky work for terrorists to collect such information, and without it, they would be far less capable of mounting a successful attack. While no one would suggest that all such information should be classified, the fact remains that the very volume of information on the Web and the ease of access to it poses a security threat. Once again, a hermetic seal is not possible; a more subtle immune system approach must be designed and implemented.

Finally, information is available to opponents to a greater degree simply because, during the 1990s, the U.S. military has been employed much more frequently and visibly than during the Cold War. These operations have given potential opponents an unprecedented view of U.S. defense systems and concepts of operations. Operational security is hard to maintain in the glare of modern media. Balancing the need for allies and the public to be informed about ongoing operations against the revelation of capabilities to potential opponents is a task that is only now beginning to be addressed.

Recommendations to the New President and the New Defense Team

Recommendations for preserving the U.S. technological edge revolve around three principles: the United States should align its defense procurement practices with market forces; it should remain the world's fastest integrator of commercial technology into defense systems; and it should abandon the "hermetic seal" model of protecting secrets in favor of an "immune system" model.

ALIGN DEFENSE PROCUREMENT PRACTICES WITH MARKET FORCES

Commercialization and globalization are ineluctable: DOD cannot escape or "manage" them through command-and-control regulation of industry. Powerful market and technological forces drive these changes. Resistance is futile; instead, DOD can achieve many of the nation's goals for the offset strategy by aligning its own procurement practices with the forces at work in the global economy as a whole. Where a regulatory approach would ultimately result in a weak and isolated defense industry, propped up by the government, that falls short of prevailing standards of innovation and efficiency, a market approach will give DOD the ability to ride the tide of the dynamic global world industrial economy.

Reward the Defense Industry When it Follows Sound Business Practices in Pursuit of Innovation and Efficiency

Too often the incentives given to private industry by the government are adverse to the government's interests. DOD should share with industry the savings from cost-cutting, facility closings, and other efficiencies. On most current defense contracts, higher costs lead to higher profits, giving industry an incentive not to cut costs. If the government does not share the returns on investment, industry managers will not invest in new factory equipment or make other cost-cutting investments. DOD should take steps to reverse this perverse incentive.

DOD should allow higher profits when industry performs successfully in terms of cost, schedule, and performance. Under current procurement rules, poorly performing companies too often enjoy the same profits as those that deliver superior value.

DOD should (with the approval of Congress) expand use of multi-year contracts. Multi-year contracting is common practice in commercial industry, with the period of the contract adjusted by the customer to enhance value to itself. Congress has begun to permit exceptions to its general requirement of annual reauthorization of budget authority; this should be expanded. Such exceptions can result in enhanced program stability, lower costs, efficiencies due to load-leveling of employment, and greater capital investment by industry.

DOD should adjust "progress payment" practices for both contractors and their subcontractors, with the goal of having their cash flows match defense industry historical levels and more closely approximate related industry standards. DOD reimburses contractors for costs of operation through progress payments. Historically, these progress payment rates were in the range of 80–85 percent, but in the past decade they have declined to 70–75 percent. As a result, industry must borrow or cut internal investment in innovation to make up for the reduction in cash flow, neither of which serves the government's interest.

DOD should educate program managers and acquisition policymakers in commercial management and finance practices, not just the Federal Acquisition Regulations, so they can better align their management practices with market forces. It is not surprising that managers who have spent their careers mastering the government's unique business practices are sometimes not familiar with commercial best practices. They are therefore not able to advocate changes in regulations that would increase value to the government, nor to apply better practices when existing regulations would permit them. In recent years training in commercial practices has been made more available to the acquisition workforce through courses in DOD institutions such as the Defense Acquisition University, the Industrial College of the Armed Forces, and the National Defense University, as well as civilian business schools and distance learning.[24] These programs should be expanded, and tailored instruction should be made available at the

24. See Testimony of Under Secretary of Defense for Acquisitions, Technology, and Logistics Jacques Gansler before the Readiness and Management Support Subcommittee, Senate Armed Services Committee, April 26, 2000. Examples of curriculum descriptions can be seen at <www.ndu.edu/ndu/icaf/curriculum9.html>.

highest levels of the acquisition system, where the need and potential benefits are greatest.

The Secretary of Defense should provide an annual statement to Congress on the state of the defense industry and technology base and its ability to support the offset strategy. Preserving the offset strategy through a market approach to the defense industry and technology base is a shared responsibility of the Secretary of Defense and Congress. A dialogue between the two branches on such matters as contracting policy would acquaint senior policymakers on both sides with the issues and would foster joint solutions. The personal delivery by the Secretary of Defense of an annual statement on the "industrial force structure" to the relevant committees of Congress would provide a focus for policy thinking and action on both sides of the Potomac River.

Acquisition Practices Should Foster the Health of the Second and Third Tiers of the Defense Industry

Second and third-tier companies, more often than the primes, combine both commercial and defense businesses; they thus are an important conduit by which commercial technology can find its way into defense systems. A number of steps could be taken to help ensure their continuing good health.

First, DOD should encourage lower-tier companies serving both defense and commercial marketplaces to remain in the defense business. This objective can be attained by reducing the administrative barriers to selling to the government, and by encouraging the primes to manage their subsystem suppliers in the best practices of commercial supply-chain management.

DOD should encourage continued consolidation of firms in the lower tiers, including units spun off from primes. DOD should make clear that it encourages consolidation in the cause of greater efficiency at the second and third tiers, and should provide clear guidance on issues of competition, anti-trust, and security policy to companies pursuing consolidation.

Program managers should encourage prime contractors to buy rather than make subsystems themselves, when better value could be obtained by buying from a lower-tier company. The large primes created in the consolidation wave of the 1990s sometimes have internal incentives to buy subsystems from their own business divisions rather than from second-tier companies specializing in these subsystems. DOD pro-

gram managers should monitor these "make-or-buy" decisions to ensure that they are made on the basis of best value to the government.

DOD should give important subsystems the status of full procurements, funding their R&D separately. The value, both military and economic, of military platforms increasingly inheres in their electronic subsystems. These systems are becoming complex, integrated, and expensive. They should be treated as systems in their own right and not merely as subsystems tacked on to the platform.

U.S. Government Policy Should Encourage Robust Trans-Atlantic Defense Industry Linkages

Trans-Atlantic defense linkages reinforce alliance solidarity and, over the long run, will provide efficiencies to all allied militaries arising from the benefits of free trade. Several steps could promote this goal. At the level of the primes, DOD should remove barriers to joint ventures, strategic partnering, and teaming arrangements as well as mergers and acquisitions. DOD should expect and encourage further mergers and acquisitions at the lower tiers. It should support recent reforms in export controls policy favorable to trans-Atlantic linkages, and should initiate further reforms (described in more detail below).

REMAIN THE WORLD'S FASTEST INTEGRATOR OF COMMERCIAL TECHNOLOGY INTO DEFENSE SYSTEMS ("RUNNING FASTEST")

Military advantage in the future will be conferred upon defense establishments that are able to mine the globalized, commercialized technology base the fastest, keeping ahead of competitors who will be able to draw from much of the same base. It is crucial to U.S. military advantage that it be a faster adopter and adapter of technology, since it can no longer hope to be technology's exclusive owner.

Crucial steps to help achieve this would include implementation of the recommendations of Chapter 7 on the "Revolution in Business Affairs" that encourage use of commercial buying practices and commercial systems in defense procurement, because the single most powerful mechanism to make defense a smart buyer of technology is to reduce the artificial barriers that separate defense businesses from commercial businesses. Also critical to success in technology integration are civil service reforms that strengthen the quality of DOD managers who oversee relations with the commercial sector. DOD

cannot be successful in these endeavors unless it has well-trained executives.

Increase Front-end R&D Spending

DOD should increase front-end R&D spending — the categories of basic and applied research and exploratory development — as a percentage of overall investment spending (R&D plus procurement). While DOD R&D will not be as large a contributor to the store of technology available to defense as it was during the Cold War, DOD's investments are still important for three reasons. First, commercial investments, while large, focus on relatively near-term and incremental improvements to existing technology. The government still has a role in promoting long-term, high-risk, high-payoff technology. Second, R&D sponsorship is one mechanism by which DOD can attract the interest and involvement of commercial industry in defense problems. Third, by participating in its own R&D programs, DOD retains the technical proficiency and currency needed to be an efficient consumer of commercial technology — to run faster.

Do More to Make R&D Investments by Defense Companies Profitable

Defense companies must be given reasonable financial incentives to ensure that they continue to invest in R&D, both to generate new technology and to be better absorbers of new technology.

Reduce the use of fixed-price R&D contracts. Fixed-price R&D contracts reflect the illusion that the cost of genuine exploration and innovation can be planned in advance. In the past, this fiction was indulged by industry and government because companies could expect to cover their losses from R&D contracts through the long production runs characteristic of the Cold War. Today, however, R&D is too often a losing proposition for defense companies, and they decline to perform it, or perform it poorly. This trend must be reversed, by a reduction in DOD's use of fixed-price R&D contracts.

Increase independent R&D, especially at lower tiers. Since not all good ideas originate in the government, it is important that industry have the option to make investments in innovation that its own scientists and engineers conceive. Such investigator-initiated independent R&D (IR&D) is also a key inducement to technical personnel to remain in the defense industry. DOD should increase its contributions to IR&D, with special attention to the lower tiers of the defense in-

dustry, and should refrain from dictating the content of IR&D projects, allowing them to be truly independent.

Resist budget pressures to cut investment in prototypes and technology demonstrations. Budget shortages affecting major acquisitions create pressure to cut funding for such projects. But prototypes and technology demonstrations are critical vehicles for technology development and for retaining systems engineering expertise. Thus DOD should resist budget pressures to cut investments in prototypes and technology demonstrations.

Improve Ties between DOD and the Biotechnology Industry

Biowarfare defense (BWD) technology needs will require stronger ties between DOD and the biotechnology industry. Thus, DOD should support and increase investments by the Defense Advanced Research Projects Agency (DARPA), the Defense Threat Reduction Agency (DTRA), the services, and the military medical system in biotechnology research performed in commercial companies. This is a way of introducing these companies to defense needs and acquainting defense technology managers with a relatively unfamiliar, yet increasingly crucial, industry. DOD should make corresponding adjustments in its treatment of contracting, intellectual property, and indemnification, to align with practices in the biotech industry.

Interagency technical linkages should be strengthened between DOD's BWD efforts and related U.S. government efforts in the National Institutes of Health, the Centers for Disease Control and Prevention, the Food and Drug Administration, and the Department of Agriculture. These agencies have a longer association with the biotech industry, and can help DOD to become more familiar with them.

DOD should establish and fund a new not-for-profit research and development center dedicated to BWD, and associated with a major biomedical research university. In the past, when faced with revolutionary technologies of military significance, the government founded not-for-profit research centers to perform independent scientific and technological work in the public interest. These institutions were able to attract and retain technical talent that the government could not. The Los Alamos and Livermore national laboratories for nuclear weapons, the Aerospace Corporation for space technology, and the MITRE Corporation for information technology are examples of institutions devoted to technical excellence in the

service of the government. As the biotech era dawns, an institution devoted to BWD is necessary and appropriate.

The Secretary of Defense should also establish a standing BWD Science Board composed of eminent bioscientists and biotech industry leaders, within the framework of the existing Defense Science Board, to advise the Secretary of Defense on BWD technology.

Information Technology Requires Targeted DOD Action to Keep Pace with Commercial Developments

DOD should require developers of information technology–intensive military-related systems and subsystems to *plan for continuous incremental upgrade, rather than periodic block upgrade*, and this requirement must be incorporated in the system design. DOD should also insist that system design incorporate commercial, open-system architectures. These steps will make it easier for DOD development programs to benefit from the rapid improvements in commercial technology.

DOD should continue to fund high-risk, high-payoff R&D in the information technology field. Notwithstanding its position as a niche player in the overall information technology revolution, DOD has good reason to continue to fund IT R&D. Whereas industry work is frequently focused on near-term developments, DOD needs to encourage fundamental advances. DOD support should include design, production, testing, security, and privacy tools. Investment in these tools will promote DOD's goal of continuing to have an open window into the rapidly changing commercial technology.

DEVELOP AN IMMUNE SYSTEM TO PROTECT SECRETS

A growing amount of important technology is non-defense and non-American, because of increasing commercialization and globalization. Attempting to maintain a hermetic seal around the U.S. defense technology base will therefore not protect security, and could even impede the objective of "running faster." New technology brings with it new categories of threats with which the system of personnel and industrial security must contend. In the face of these changes, current export controls and security systems are increasingly ineffective, as bureaucratic and rule-laden regulatory systems administer simpleminded and outdated hermetic seals. What is needed is a system that measures risk and reacts proportionally to it: an immune system. Some of the rec-

ommendations below deal with the basic efficiency of the export controls system, which would be needed even if the world were not changing so rapidly around it. But other recommendations begin the process of continual adaptation that corresponds to the immune system model.

Support the Defense Trade Security Initiative

The aim of the U.S. government's recently adopted Defense Trade Security Initiative is to streamline and rationalize some aspects of export controls administration where the security risks are low.[25] It provides for blanket exemptions of licensing restriction for allied countries that meet specified standards of security controls, flexible one-stop licensing vehicles, and some streamlining (including computerization) of defense-related licensing processes. The new administration should support this Initiative.

Seek Fundamental Change in the Statutory Basis of Export Controls

The new administration should establish a consultative process with the leadership of the new Congress, with the aim of fundamentally altering the statutory basis of U.S. export controls. The new basis should eliminate the statutory and regulatory distinction between munitions and dual-use items, and establish a single, unified licensing system with interagency policy direction.[26] The munitions and dual-use systems share common functions, and harmonizing the two processes, to the extent feasible, is in both the economic and the security interests of the United States. Such efforts would go far in eliminating public and industry confusion due to a welter of export regulations; they would streamline the processes to enhance U.S. competitiveness on the global market, encourage information shar-

25. Fact sheets detailing the Defense Trade Security Initiative released by the Bureau of Political-Military Affairs, U.S. Department of State and the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, U.S. Department of Defense, Washington, D.C., May 24, 2000, can be found at <secretary.state.gov/www/briefings/statements/2000/ps000524d.html#fs>.

26. While "the end of the Cold War brought about the elimination of parallel export control systems in most nations … the United States has continued to maintain a robust [dual] system of dual-use and munitions controls." Report of the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction, "Combating Proliferation of Weapons of Mass Destruction," July 14, 1999, p. 41.

ing, and enhance intelligence among the controlling agencies.[27] Meanwhile, agency overhead costs would also be reduced by greater coordination and shared resources.

Centralize Export Controls Licensing, but not Policymaking, in a Single Entity

The new administration should centralize all administrative, training, and technical support to export controls licensing in a single entity. This entity should comprise 90 percent of all U.S. government positions devoted to export controls administration. It should have a full-time administrative director and a well-funded annual training program for its staff. The new licensing entity should be required to develop performance metrics for the export controls regulatory system, to assess timeliness of response to license applications, technical training of the licensing workforce, promotion rates of the licensing workforce compared to their agency peers, the cost to the economy of licenses denied, the reduction of foreign threat through controls, and the costs to the economy and increased threat attributable to different allied export controls practices.

The agency should report these measures regularly to Congress. It is not recommended, however, that the administration attempt to create a central export controls policymaking organization distinct from State, Commerce, and Defense: these agencies would only re-register their legitimate concerns at the cabinet level, wasting time and energy for all. The new central licensing agency should be funded jointly by State, Commerce, and Defense, with the contribution of each agency proportional to its overall budget.

Create a Combined Automated Licensing, Intelligence, and Enforcement Information System and Database

The centralized licensing entity should create a combined State-Commerce-Defense automated licensing, intelligence, and enforcement information system and database. It should be funded in proportion to the total budgets of these agencies, with ample annual funding to maintain and upgrade the system. The combined system should be implemented and managed by the new central licensing organization.

27. "Since proliferators purchase both dual-use goods and munitions items, a single system would allow licensing officers to communicate more regarding end-users of concern." Ibid., p. 42.

Develop a Regulatory Policy toward Systems Engineering

The new administration should task the National Security Council working group on export controls to develop a regulatory policy toward systems engineering. Systems engineering represents the lasting American strength in military technology and the attribute most difficult for potential opponents to replicate. It therefore is most deserving of protection through controls. A systems engineering approach should supplement, and to a certain extent supersede, the current lists of "militarily critical" underlying technologies.

Develop a Strategy for Enhanced Use of End-use Controls

The National Security Council working group on export controls should also be tasked to develop a strategy for the enhanced use of end-use controls. End-use controls ensure that items licensed for sale to a civil customer are not diverted to military use. They represent an effective adaptive response if administered properly. Most importantly, end-use controls allow the export controls system to target users rather than entire countries. The strategy should cover both policy and implementation, including funding and personnel to conduct inspections.

Increase Intelligence Support for Export Controls

The new administration should increase funding for intelligence support to the export controls process, including national intelligence, for assessments of security threats both from wider availability of technology and from foreign availability. The immune system concept depends on intelligence that assesses threats and the effectiveness of various responses. Today the intelligence community is too often asked to determine whether export controls rules are being obeyed, rather than illuminating how they can be made more effective.

Seek International Agreement on Export Controls Standards

The Secretary of State should continue to give high diplomatic priority to seeking international agreement on export controls standards and performance metrics for national export controls regulatory systems. When the United States applies controls where others do not, both security and economic objectives are sacrificed.

Increase Support for the Export Controls Systems of Non-allied Nations

The United States should increase its support to non-allied nations for strengthening their export controls systems. States that wish to cooperate with U.S. export controls policy are sometimes frustrated by the absence of effective legal and enforcement mechanisms. They could be assisted through the expansion of such cooperative international programs as the Nunn-Lugar Cooperative Threat Reduction program, the Bureau of Export Administration's Nonproliferation and Export Control Cooperation, and the joint DOD–Customs Service Counterproliferation Program. These initiatives provide expertise, training, and equipment to strengthen the export controls systems of foreign governments in an attempt to head off proliferation of weapons of mass destruction (WMD). However, both are largely limited to the states of the former Soviet Union. Their mandate and scope should be expanded to allow for greater multilateral initiatives that build on current cooperation and program development in other regions of U.S. interest.

Create an Interagency Security Policy Task Force to Develop Policy for New Security Problems Posed by Technological Change

An interagency security policy task force should be created and tasked to develop policy guidance covering the new problems to industrial and personnel security posed by technological change. This guidance should address such issues as problems relating to the increased density of storage media; network security; and the integrity of software, including embedded software, from non-U.S. commercial sources.

Develop a Policy on Risk of Compromise from High Operations Tempo

The new administration should task the Secretary of Defense, with the advice of the Chairman of the Joint Chiefs of Staff, to develop a policy on the risk of compromise of operational security resulting from the high operations tempo increasingly characteristic of U.S. military operations, and the consequent risks of revelation of U.S. capabilities.

Widen Use of Commercial Techniques of Security, Privacy, Technical Monitoring, and Human Resources Management

DOD should apply commercial techniques of security, privacy, technical monitoring, and human resources management to DOD personnel

and industrial security. Competitive commercial industries spend a great deal of effort and money on security, and they apply an immune system approach rather than a rule-based bureaucratic system to identify real threats and provide the most effective and least disruptive protection. DOD security managers could benefit from experience gained in industry.

Closing

Technology is a national strength of the United States. Its culture and institutions are well-suited to the rapid creation and adoption of new technology. These national characteristics can continue to infuse national defense if steps are taken to preserve DOD's technological edge in the commercialized, globalized world that is emerging.