VIEWPOINT: BETWEEN A ROCK AND A HARD-DRIVE: EXPORT CONTROLS ON SUPERCOMPUTERS

by John Arquilla

In an era in which information has emerged as an increasingly important dimension of national power, U.S. export control policy toward trade in supercomputers[1] has recently turned away from traditional (i.e., Cold War-era) restrictive strategies, favoring instead an approach that will foster the wide diffusion of this technology. In the economic realm, the shift toward openness will have salutary effects upon the supercomputer industry, helping U.S. companies to maintain and extend their dominance of the market, and to rack up handsome profits.[2] However, in the security sphere, concerns will necessarily arise regarding the possibility that other nations, or even some non-state actors, might use the vast power of these computational engines to enable them to develop and secretly test a wide range of weapons. While the use of supercomputers in support of nuclear proliferation activities remains a paramount concern, the ability to design and produce very advanced conventional weapons—and to engage in some forms of "information warfare"—also flows from the acquisition of high performance computing (HPC) capabilities. Thus, in the area of supercomputers, proliferation concerns are growing in diversity and complexity.

Despite the fact that the new "open" policy has already received presidential approval (on October 6, 1995), after only a very limited public (or private) debate, the built-in requirements for annual review allow considerable room for continuing reappraisal. Also, the 1984 bilateral agreement between the United States and Japan to coordinate policies on the sale of technological systems with military applications requires Japanese assent to the new HPC policy. In this case, the Japanese government did not provide input prior to the October announcement and still has not granted its approval. Finally, in addition to these other reasons for review of the presidential decision, the very seriousness of the issue, which highlights a growing tension between commercial and security interests, should encourage a careful examination of the merits of the various strategies that might govern this particular export control policy.

With these considerations in mind, this essay first discusses the details of the new export control policy toward supercomputers. Then it considers the range of plausible strategies that might apply in this issue area, on a spectrum that has complete openness at one end and exclusion at the other, with hybrid approaches in between. A few historical analogies illustrate the timelessness of the problem of controlling information flows and help in developing an analytic framework. Evaluation of the relative merits of the differing export control strategies follows. This essay concludes by drawing some implications for further clarifying and amending the existing policy. It suggests that this issue's importance to U.S. national security may require the inclusion of legislative branch input on a continuing basis, and perhaps some decisionmaking authority, rather than continuing to keep these export controls solely under the authority of the executive branch of government.

THE POLICY

If one could describe the range of possible export control strategies as a spectrum of choices, ranging from a preclusive, closed stance at one end, to complete openness at the other, the Clinton policy falls squarely in the middle. On the more proprietary side, the policy prohibits sales of *any* supercomputers to countries that pose national security concerns to the United States. These include such "usual suspects" as Iran, Iraq, Libya, and North Korea. Cuba, already excluded from such purchases by virtue of the overall U.S. economic embargo, fills out the membership roster of this "pariahs club." At the other end of the spectrum, Western Europe, Ja-

Dr. John Arquilla is Associate Professor of National Security Affairs at the U.S. Naval Postgraduate School. The views expressed are his alone, and do not represent the position of the Navy or the U.S. government.

pan, Canada, Mexico, Australia, and New Zealand have no limits whatsoever (in terms of U.S. governmental review) on their purchases.

Between the extremes lie two middle layers. The more open one allows sales of machines capable of 10 billion theoretical operations per second (TOPS), with only record-keeping requirements, to all South American countries, most of the former Soviet satellites, South Korea, and South Africa. Individual licensees must support their purchases above this level. Above 20 billion TOPS, members of this group would possibly have to allow end-user site safeguards.

The last class of purchasers includes former Cold War adversaries Russia, China, Vietnam, and Syria; states of the Middle East, the Maghreb, and South Asia also fall in this more preclusive range of the spectrum. All may purchase computational engines without any regulation up to two billion TOPS, a figure that clearly crosses the threshold of high performance (set since 1993 at 1.5 billion TOPS). Purchases between two to 10 billion TOPS require the granting of individual licenses, with record keeping by the exporter or, in cases between seven to 10 billion, as required by the U.S. government. Above 10 billion TOPS, the policy states only that "additional safeguards *may* be required at the end-user location."[3] Typically, precautions against diversion to military uses extend to having U.S. technicians in the employ of the manufacturer operate the supercomputer in a segregated facility. Such a site must prove sufficiently secure to prevent access or control by the purchaser, who enjoys only the outputs of the computational engine. However, the new HPC export control policy articulates no mandatory requirement to take such precautionary measures, even concerning sales of the most advanced machines.

This hybrid strategy toward the diffusion of information has clear antecedents in the ancient and medieval eras, as well as in more recent times. For example, Hippocrates took the view that medical science should spread, but very carefully. Thus, the Hippocratic Oath requires, among other things, keeping knowledge of the healing arts away from "strangers." Medieval guilds followed a similar strategy; but this approach no doubt reached its zenith in the alliance between commerce and state during Venice's golden age in the 14th and 15th centuries. The various guilds and the Venetian government decided, in the interest of commercial competitiveness, overseas production, and profit maximization, to allow skilled artisans to emigrate. However, Venetian secret police would monitor their activities, and those who breached agreements to keep the inner workings of their crafts safe from foreigners found themselves kidnapped back to Venice.[4]

In the 20th century, two well-known examples of the hybrid approach include efforts to control the spread of nuclear and missile technologies. The first has attempted to allow the spread of peaceful nuclear power as an energy source while precluding its use for the creation of weapons of mass destruction. In the second case, the principally military uses of missiles have led to a somewhat more proprietary Missile Technology Control Regime (MTCR), although "friendly" states clearly have substantial access to this technology. The new HPC export control strategy flows from these two cases, drawing upon both the need to allow peaceful uses while discouraging military applications, and fostering the creation of classes of "tame" and "rogue" states to help in identifying the appropriate customer base.

The foregoing examples of hybrid export control strategies all have varying degrees of commercial ramifications, with the Venetian case representing the most substantially market-driven calculus of strategic decision. The HPC situation has a similarly robust economic dimension. The possibility thus arises that the current hybrid export control strategy might have emerged from the effort to balance American commercial and security interests, with political leaders shaping policy in response to pressure exerted by domestic interest groups, both corporate and individual.

With regard to President Clinton, for example, one might hypothesize that his loosening of HPC export controls reflected a response to direct or indirect pressures. Campaign finance records, however, indicate that the computer industry's contributions to him in 1992 fell near the bottom of the list of financial support shown on an industrial sector-by-sector basis. Further, scant evidence appears to suggest that indirect pressure might come from a Congress influenced by the computer industry. In the last Congressional election cycle (1994), for example, total contributions from computer companies and trade associations amounted to only $720,000, whereas the agriculture industry contributed $15.5 million.[5] Thus, the possibility that high-tech interest groups have "captured" either the president or Congress on the HPC issue seems extremely unlikely. This conclusion does not, however, rule out the possibility that the president might take actions in favor of computer industry interests, in the hope of gaining their support in the

1996 election, especially since Silicon Valley lies in electoral-vote-rich California.

An understanding of the origins, nature, and scope of the current HPC export control policy, though useful, does not by itself allow for thoughtful evaluation of the path chosen. For this purpose, the key alternative strategies must come under some scrutiny as well. Only then might a better sense of the most appropriate policy emerge, or of the conditions under which a shift in strategy might grow necessary. Further, one must also consider the prospects for control and the related goals. Fortunately, the rapidly advancing frontier of HPC "TOPS capability" guarantees future opportunities for control, both in terms of the rate of advance and regarding specific states.

ALTERNATE STRATEGIES

With regard to the spectrum of HPC policies that lie on either side of the hybrid approach, the major alternatives consist of the adoption of either preclusive or inclusive strategies. Attempting to prevent the spread of advanced technology or knowledge has long proven a very attractive option. In the military realm, the Byzantine Empire strove for centuries to keep the secret of its incendiary naval weapon, "Greek fire." During this same period, Christendom in general sought to keep military technology regarding heavy artillery out of Muslim hands. In the 19th century, the British Royal Navy attempted to keep its technological innovations secret until it grew clear that competitors would soon begin production of the device in question.[6] Finally, in the 20th century, a veil of secrecy, of the most preclusive sort, has remained over stealth technology,

While the tendency toward proprietary strategies in the military realm has remained fairly constant, with some notable exceptions mentioned below, civilian technologies and intellectual properties have seemed to move more toward openness since the dawn of the industrial age. Thus, in the preindustrial 15th century, Prince Henry of Portugal maintained tight control over navigation science (a truly dual-use discipline), and the Roman Catholic Church sought to prevent the publication of the Bible into the various vernaculars. With the coming of mass production and mass global markets in the 18th century, however, the commercial value of exclusion seems to have dropped. Technologies became more interconnected, and industrial advances worldwide meant not only more competition, but more markets for sophisticated manufactured goods, and enormous demand for manufacturing equipment. Clearly, the 19th century Manchester creed, which holds that there exists a system-wide harmony of economic interests, signaled the onset of a serious tension between the benefits of technological diffusion for trade and its risks in the security sphere.

If commercial concerns form the paramount interests of a state, it would seem appropriate to pursue a strategy of openness toward technological innovations. As mentioned above, this approach has proven common in the more than two centuries since the beginning of the industrial revolution, even in the area of military technology. An excellent example of laissez-faire attitudes toward even the most cutting-edge technologies arises in the case of the submarine. Robert Fulton, the American inventor, spent much of his time during the Napoleonic Wars trying to market his submarine (which actually worked and even sank an enemy ship in a "combat experiment") to both the British and the French. The Royal Navy rejected him out of hand, no doubt because of fears for the future of sailing fleets. Napoleon simply could not believe that this weapon would overturn the naval balance.[7]

The understandable apprehensions of both Britain and France notwithstanding, Fulton was able to hawk his wares wherever he wanted. This lax policy remains puzzling and has present-day analogs. Current diesel submarine design has arrived at air independent propulsion and at acoustic superiority to nuclear vessels, posing serious potential threats to the freedom of the seas. Nevertheless, the trade in these boats goes on in the almost complete absence of regulation, allowing the emergence of a new kind of regional naval arms racing.[8]

EVALUATING THE STRATEGIES

Clearly, the various security and economic consequences of adopting one of the above mentioned export control strategies must figure significantly in any comparative evaluation of alternatives. In the military sphere, concerns should extend to potential shifts in relative power, the effects on weapons (nuclear and advanced conventional) proliferation and war-marking capabilities, and the prospects for arms racing. Analysis of commercial effects should revolve around notions of short-term market share outcomes and longer-term concerns about industry viability and competitiveness.

Finally, some sense of the evolutionary pace of the HPC industry and the practical prospects for controlling the diffusion of this information technology must also form a part of the analysis.

With these factors in mind, one may quickly note that, to the extent allowable by the state of the technology, a preclusive strategy maximizes security while paying little heed to commercial effects. Conversely, an open strategy fosters the greatest degree of commercial competitiveness, but may have deleterious consequences in the security sphere. A hybrid approach, however, offers some hope of serving both security and business interests. This last strategy also accommodates itself well to an industry which, by all accounts, appears poised for a period of explosive growth in terms of the TOPS-capabilities of the best machines.

If one accepts the notion that each year, the level of "uncontrollable" advance in HPC technology will rise, as will the maximum performance of the leading computational engines, then one might find it reasonable to allow unrestricted sales, at the very least, to the "control" threshold, and perhaps a bit beyond. While attractive in theory, in that it addresses both security and economic concerns, how does this notion relate to the evaluation criteria?

Clearly, the hybrid approach fosters a very robust commercial environment for the HPC industry and, unlike the purely "open" strategy, does not contribute to the erosion of relative power advantages. Or does it? The answer to this question depends both upon the setting of the control threshold and the policy toward sales to specific countries. The government-sponsored analysis of the HPC issue develops a comprehensive methodology for identifying the appropriate thresholds on a class-by-class basis, but avoids discussion of factors such as the risks entailed in vending supercomputers to potential politico-military rivals.[9] In this regard, then, one must note that the current HPC export control policy derives principally from notions of technological determinism,[10] with a lesser degree of care shown to the consequences for shifts in relative power. Herein lie some problems.

Concerns about the risks of a too open policy should revolve around its effects on nonproliferation and counterproliferation policy, both in the nuclear and advanced conventional sphere. With this in mind, the currently formulated HPC policy will contribute less to adding new nuclear proliferators,[11] but may allow those with some weapons to increase production and refine capabilities quite significantly, and to do so without detection. For example, Gary Milhollin, of the Wisconsin Project on Arms Control, has observed that "Russia and China will be able to develop their nuclear arsenals [further] without having to conduct underground tests and we will not be able to monitor them."[12] This possibility could foster both qualitative and quantitative arms racing. As nettlesome as the prospect of the increasing opacity of nuclear development seems, though, this problem could ease if the U.S. government emphasized other nonproliferation policies, ranging from the control of very advanced communications technology to the imposition of serious penalties for detected violations of existing nonproliferation and arms control agreements.

The greater proliferation risk engendered by the HPC agreement lies in the risk that potential adversaries will now have the ability to bring their militaries into the information age. High performance computing capabilities will allow them to develop the complex communications battle management systems needed to fight in the future, nonlinear battlespace. Currently, the sensors and image analysis capabilities needed to wage "cyberwar" fall in a range from one to eight billion TOPS. However, even in this area, one may note important nuances. For example, advances in the design of composite and/or explosive reactive armor rely upon HPC capabilities well above eight billion TOPS, all the way to 21 billion. Similarly, the requirements for the most advanced antisubmarine sensing devices begin at the eight billion TOPS level, and extend to the 20 billion level.[13] Much still remains at the farthest reaches of HPC.

However, the frontiers of HPC expand further every several months, putting even the 20 billion TOPS level in sight by the year 2000.[14] This progression implies a need to monitor closely the threshold of "controllability," and to inquire as to whether the current level of controls might provide potential rivals with easy opportunities to enhance their military capabilities greatly. Further, even if a particular TOPS level becomes "uncontrollable," the issue of whether to sell the technology or assist its development requires consideration. Why make an information proliferator's path to the design and production of very advanced conventional weaponry easier? Britain asked this question during its mid-19th century naval rivalry with France, when ships converted from sail to steam, concluding that controlling the export of steam engines raised French costs by over 35 percent. France, however, viewed the development of its own steam engine industry as a *sine qua non* of great power, and took up the cudgels to compete with Britain.[15]

The foregoing raises the possibilities that tighter controls may help to maintain relative advantages over potential competitors, but also that more preclusive approaches might encourage or require development of indigenous design and production capabilities. With this in mind, one may see that both major potential rivals to the United States, Russia and China, both currently topping out at the 1.5 billion TOPS level, have barely reached the minimum level of high performance computing. The 1995 HPC guideline will allow them to advance, rapidly and cost effectively, even though they fall into the more preclusive range of the new policy. On the other hand, India, toward which HPC policy has long followed a very preclusive course, has developed capabilities of its own of around three billion TOPS. This development confirms the point that exclusion may breed internal efforts at information proliferation.[16] Thus, short-term efforts to protect relative power advantages may improve others' long-term prospects.

In summary, this discussion of the strategic and commercial factors, which forms the basis for strategy evaluation, describes two tensions. First, efforts to safeguard national power advantages over others, associated with exclusion, engender commercial costs in terms of lost market share. Similarly, openness fosters economic competitiveness, while tending to erode advantages in relative power over actual and potential rival states. The second tension lies *within* the realm of security concerns, in that attempts to preserve power advantages through exclusion may have beneficial short-term effects, but may encourage competitors to engage in an HPC "information arms race" that will have negative long-term effects.

Reconciling these tensions, to the extent possible, and selecting an appropriate export control strategy demands knowledge of two types. First, a reasonably precise sense of the degree of HPC technical controllability must inform preclusive efforts. As the United States does not hold a monopoly over HPC technology, a completely closed strategy will prove infeasible. However, to the extent to which the rate of advance follows predictable patterns, a "moving preclusive limit" on HPC exports could emerge.

The other quantifiable factor that should guide strategic decisionmaking lies in the area of economic impact. Currently, the entire HPC export market has annual sales of roughly $35 billion,[17] of which the United States holds a roughly 80 percent share. Presumably, a preclusive strategy would exert downward pressure on U.S. market share, while openness would help to maintain this overwhelmingly dominant position. Also, closed approaches would hinder general growth of the market's size, while openness could enlarge it considerably. However, economic considerations and forecasts of possible outcomes regarding market size and share always have an element of uncertainty. Therefore, the negative effects of exclusion could actually prove modest, as could the positive results from openness.

Given the somewhat uncontrollable nature of technical progress in HPC, and the uncertainties about economic effects, a hybrid strategy seems best suited to the needs of the situation. Pure exclusion lies beyond the realm of possibility, but a guarded approach, calibrated in terms of the rate of technological advance, can work. With regard to impacts on market size and share, one cannot know now what will happen. One can, however, measure results from year to year, resetting limits based on market data, and keeping in mind the changing threshold of technological controllability. For these tasks, the hybrid approach, which combines preclusive and open elements, appears optimal. The Clinton HPC strategy clearly falls in this category, although there remains a number of security issues. The correct resolution of these issues will determine the success of this HPC export control venture. Since advances in operational warfighting, as well as in command and control systems, depend upon HPC capabilities, they have become an essential element of national power in the information age.

IMPLICATIONS FOR POLICY

The preceding analysis has identified the strategies available for approaching the issue of export controls on supercomputers, and has supported the notion that a hybrid policy, mixing open and closed elements, has the best chance to foster commercial competitiveness without unduly compromising the national security. In this regard, the recently elucidated Clinton plan for HPC export controls appears sensible. However, this policy will have consequences in a number of areas, each of which bears significantly upon security issues and requires careful attention.

First, to deal with the likelihood of increasing "opacity" on the part of potential rivals or non-aligned existing nuclear states that may wish to improve their arsenals (e.g., Russia, China, India, Pakistan, and possibly North Korea), steps should commence to ensure their compliance with existing arms control and nonproliferation agreements and to sharpen the penalties for noncompliance. Further, counterproliferation efforts should focus increasingly on the monitoring of improvements in sophisticated satellite and other communications and control systems. Finally, the problem of "downstreaming" HPC capabilities to pariahs or rogue states requires very close after-sale relations, accompanied by stiff sanctions for violations. Indeed, HPC monitoring of this sort may have to become a major intelligence function.

The same will certainly hold true in the area of advanced conventional arms, where the undue spread of HPC capabilities may undermine the American advantage in relative power that has emerged in the immediate post-Cold War era. Indeed, the likely shape of conflict in the information age suggests that HPC will have ever increasing military applications. This implies, quite possibly, the need for bi- and multilateral arms control agreements on advanced conventional weapons. At a minimum, though, the prospect of the spread of HPC-driven arsenals requires careful, continuing net assessments of others' HPC capabilities on a very frequent, at least annual, basis.

This concern should also act as a spur to pursue the formation of an international governmental organization for dealing with the problem of "information technology proliferation," perhaps analogous to the International Atomic Energy Agency (IAEA). If the generally successful multilateral efforts to stem the spread of nuclear weapons represent a reliable indicator, then the prospects for similar success in the HPC area appear quite good. However, the worldwide diffusion of HPC knowledge and capabilities is much greater than nuclear weapon technologies. This difference suggests that, because of ease of access to this information, the political problems with achieving multilateral controls could prove quite substantial, if not insurmountable.

This raises the second key policy issue: Japan's role in any HPC export control regime. Without Japanese cooperation, the preclusive elements of U.S. strategy will grow problematic, as Japan constitutes a second major source of supply for HPC. In this regard, the United States should involve Japan more deeply in the setting of controls, as called for by the 1984 bilateral agreement. More to the point, though, the HPC issue may now assume a significant place in U.S.-Japanese relations. For, example, one might expect Japan to seek a lessening of pressure to open its markets to American goods in return for full compliance with the HPC regime. This bargaining strategy would make calculations of U.S. economic costs more complex, as fractiousness over trade could cost both HPC sales worldwide, and hurt the marketing of other U.S. products in Japan. On the other hand, Japan remains heavily reliant upon American markets for its goods, and U.S. forces will likely increase in value as a counterweight to rising Chinese power in the years ahead. The issue has many dimensions and should form an area of careful focus in the formation of future U.S. foreign policy. At a minimum, though, Japanese cooperation forms a necessary condition for the mounting of broader, multilateral efforts to manage the diffusion of HPC technology.

A third issue arises if limiting the spread of very powerful computational engines proves problematic over the long-term, with the threshold of controllability constantly driven higher. If this occurs, as this and other analyses suggest it will, then perhaps a more nuanced approach to HPC strategy can develop, one centered on the idea of controlling the dissemination of software rather than hardware. Indeed, analyst suggested that the urgent need "to safeguard critical software...may be more important than the [HPC] computers themselves."[18]

This notion suggests that the definition of "high performance" has qualitative as well as quantitative aspects. Unfortunately, the current HPC policy considers only the latter. This lesser attentiveness to the more qualitative side of HPC has led to some near accidents, such as the recent initiative to allow China access to advanced U.S. military simulation software. This policy only collapsed after heated internal debate, some of which became public.[19] The inclusion of the qualitative dimension of HPC makes good sense and may also lessen the impact of the increasing inability of states to control the diffusion of hardware technology. Software may even prove, as *The New York Times* has suggested, more important than brute force calculating capabilities. For, in the words of Claude Shannon, the "founding father" of modern information science, overemphasizing the quantitative side of computing will lead to the creation of machines that "see far but notice little; that remember everything, but know nothing."

The final implication for policy raised by the foregoing analysis concerns executive powers. Since the late

1930s, when U.S. technological export controls began, the president has controlled this issue area completely. In the case of the current HPC policy, President Clinton acted in this tradition, without Congressional approval. Given the profound economic and military ramifications of this policy, however, a strong *prima facie* case for involving the legislative branch emerges. The issue of HPC, while complex, remains quite open to understanding, particularly by expert congressional staff members. Finally, the potentially serious consequences of missteps demand a more protracted, comprehensive debate on the issue, particularly with regard to sales to potential adversaries, risks of "downstreaming," and the need to maintain U.S. advantages in power relative to others. Therefore, hearings on the HPC issue should begin soon to address the complex questions that we are only beginning to understand—but ignore at our peril.

[1] Since 1993, supercomputers have consisted of that class of computational engines capable of 1.5 billion theoretical operations per second (TOPS). For ease of reference, and to recognize the vast and rapid increase in computing power, this article does not use the older term "MTOPS," which stands for *millions* of theoretical operations per second.

[2] A government estimate of the immediate effects of the new policy suggests that computer exports could grow by nearly an additional 10 percent annually. As President Clinton noted, "[i]t is good for U.S. workers and U.S. business." See the "Statement by the President," October 6, 1995.

[3] Emphasis added. For further details about the classes of purchasers and the various levels of monitoring, see the Presidential Press Release entitled "Export Controls on Computers," October 6, 1995.

[4] Norbert Wiener, *The Human Use of Human Beings* (New York: Doubleday, 1950), p. 112, notes also that the secret police did some killing to prevent the diffusion of commercial information.

[5] *Report of the Federal Election Commission* (Washington: Government Printing Office, 1995); and David J. Lynch, "Industry now must plug in to political game," *USA Today,* January 16, 1996, pp. 1-2.

[6] Bernard Brodie, *Sea Power in the Machine Age* (Princeton: Princeton University Press, 1943), see especially p. 44.

[7] W.B. Parsons, *Robert Fulton and the Submarine* (New York: Dodd, Mead, 1922) provides a detailed account of Fulton's efforts to gain acceptance of his submarine. See also Brodie, pp. 264-7.

[8] Jonathan Landay, "The Arms Race Under the Sea," *The Christian Science Monitor,* September 27, 1995, pp. 1, 10-11, discusses the latest developments in this area.

[9] Seymour Goodman, Peter Wolcott, and Grey Burkhart, "Building on Basics: An Examination of High-Performance Computing Export Control Policy in the 1990s" (Stanford: Center for International Security and Arms Control, 1995), p. 14, notes, on this point: "This consideration is beyond the scope of this study." The Assistant Secretary of Commerce for Export Administration and the Assistant Secretary of Defense for Counterproliferation Policy sponsored the study.

[10] As Bill Archey, president of the American Electronics Association has put the matter, "it may be difficult to restrict the export of a high performance computer, [but] it is virtually impossible to restrict the export of high performance computing." Cited in Gary H. Anthes, "Restrictions Lifted on Export of High Performance Computers," *Computerworld,* October 16, 1995, p. 32. William Reinsch, Commerce Undersecretary for Export Administration, has argued along the same lines, about the problematic nature of control efforts: "This is not a happy reality, but it is the technological reality." From Pat Cooper and Theresa Hitchens, "New U.S. Computer Export Rules Spark Optimism, Arms Control Fear," *Defense News,* October 22, 1995, p. 26.

[11] Brian Deagon, "Why Tech Export Curbs may be a Futile Exercise," *Investor's Business Daily,* October 23, 1995, p. A8, notes succinctly, citing a 1990 Los Alamos National Laboratory study, that "the U.S. nuclear arsenal in the 1960s was designed using computing power equal to today's hand calculator."

[12] Cited in Jonathan S. Landay, "Easier High-Tech Controls Reopen Proliferation Debate," *Christian Science Monitor,* October 16, 1995.

[13] For details on the HPC requirements for these and many other military systems, see Goodman *et al.*, pp. 44-58. Other key military applications include cryptography and ballistic missile defensive systems.

[14] *Ibid.*, p. 27 projects the likely progress of HPC through the turn of the century.

[15] See Brodie, p. 39.

[16] For details on Russia, China and India, See Goodman *et al*., pp. 17-21.

[17] See Deagon, p. A8.

[18] "Computers Worth Protecting," *The New York Times,* editorial, October 7, 1995, p. 18.

[19] For a thorough presentation of both sides' positions in this debate, see Barbara Opall, "China Sinks U.S. in Simulated War," *Defense News,* February 5, 1995, pp. 1, 26.