Conclusion

The United States now faces complex challenges in a world that has changed significantly since the 1980s. Regional conflicts, terrorism, and the proliferation of weapons of mass destruction threaten U.S. national interests. A global economy and the spread of information and technology throughout an increasingly competitive world marketplace create new challenges for U.S. national security.

Research and manufacturing capabilities for information technology are now global. Access to technology and technical capabilities has spread widely and continues to spread in a global market. Barriers to entry for new competitors in information technology tend to be economic rather than technological. The United States leads in many technologies, but it does not have a monopoly. [1]

The current system of computer export controls derive from an era when U.S. strategy was to deny the Soviet Union access to technology. Limited communications, allied cooperation, and the real threat posed by the Soviets made this effective. Now, MTOPS-based hardware controls are increasingly irrelevant, given the lack of multilateral cooperation, the spread of technology, increases in computing power with more capable microprocessors, and the development of alternative sources of supercomputing like clustering and network computing. Computing power is becoming ubiquitous, as more devices contain processing power equal to what was once considered a supercomputer. Access to computational power continues to expand with technological advances and the spread of the Internet.

Consensus between the United States and its allies on threats and technology transfer has eroded. Multilateral cooperation for controlling information technologies is at a low ebb. The Wassenaar Arrangement, which controls general-purpose computers, has been decontrolling information technology since its inception. Wassenaar computer controls are set at a level far above what military applications need, and Wassenaar members will not embargo civil technology to countries like China or India. The absence of a common security threat and the emergence of a competitive global market mean that there is no support for Cold War controls on computers.

Computing power is not itself a chokepoint for military and proliferation activities. Computers of 500 to 1000 MTOPS are sufficient for military and proliferation purposes. Specially developed software codes, extensive databases, and the manufacturing and integration skills necessary for modern weaponry are more important. Military power today depends not only on the tools of the industrial age but on the tools of the information age as well. Potential opponents will seek to exploit U.S. vulnerabilities with the new technologies. The United States will need to find ways to use advanced commercial technologies to improve military capabilities and work with the private sector to enhance U.S. security. For the United States, information technology, properly integrated into battlefield operations, can provide the margin of victory.

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.

All of these developments will erode U.S. national security unless the United States takes steps to adjust its policies to the new situation. Denying access to computing power, although strategically important in the 1980s, is now ineffective and even counterproductive. The issue must now be recast. The new administration and the new Congress have the opportunity to take the bold, necessary steps needed to advance U.S. national security.

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.

From *Computer Exports and National Security in a Global Era - New Tools for a New Century* CSIS Panel Report, June 2001.