

# The Net: Power and Policy in the 21st Century

*Leslie David Simon*

*... a new form of state is being born: the virtual nation, a nation based on mobile capital, labor, and information.*  
— Richard Rosecrance  
The Rise of the Virtual State

The rapid growth of the so-called Net—the vast interconnected global system of communications networks, computers, software, content, and people linked together by the Internet<sup>1</sup>—is changing human institutions ranging from government to health care to education to banking and industry. It is fostering globalization, creating enormous wealth, shifting traditional patterns of power, and generating new political concerns (for example, security and censorship). Governments everywhere are giving it their full and often nervous attention. Most welcome its promise of rapid economic growth and promote it, even as they attempt to cope with its darker effects—the potential loss of privacy or the threat of cyberwarfare, for example. Dictatorships fear the freedom it offers and restrict its use. Some countries, such as China, try to do both, simultaneously attempting to foster electronic commerce while limiting electronic freedoms.

The United States leads the digital age because American political and economic freedoms provide unusually fertile ground for development of the Net. Its early success, however, will not be assured until we develop comprehensive, long-range national policies to promote the Net and to confront the challenges to national sovereignty posed by its remarkable growth and diffusion. What is needed is a policy framework that the United States and other countries might use to maximize their power while reducing future threats.

This policy framework would be based on principles reflecting an expansion of American freedoms. It would include such steps as ending telecommunications regulation, phasing out traditional export controls on high technology, focusing the foreign policy community on Net development abroad, and automatically granting U.S.

---

*Leslie David Simon is a senior policy scholar at The Woodrow Wilson International Center for Scholars. He previously served as director of public affairs in Washington and as vice president for external affairs in Paris for IBM Corporation. Mr. Simon is the author of Net Policy.Com: Public Agenda for a Digital World.*

citizenship to foreign citizens with American high-technology Ph.D.s. Such efforts would not only bolster American power, but they would also provide a challenge to the rest of the world: follow us, or fall further behind! Thus, democracies in general would become more efficient and powerful in many fields as their use of the Net matured, while totalitarian regimes would tend to fall further behind.

The notion that U.S. national power could be amplified by its mastery of the Net is only a few years old. Barely 4 years ago, Samuel Huntington wrote, “. . . for most of history, China had the world’s largest economy. The diffusion of technology and the economic development of non-Western societies . . . (is) now producing a return to the historical pattern. . . . The two-hundred year Western ‘blip’ on the world economy will be over.”<sup>2</sup> His assertion was based on an obsolete view of power that failed to realize how power would be strengthened many orders of magnitude by the digital technologies, themselves nurtured by Western democracy. More recently, Seymour Martin Lipset wrote, “At the dawn of the new century, the United States finds itself in a position of surprising dominance around the world. It has been a triumph of ideas and values perhaps even more than of power.”<sup>3</sup> Lipset is correct. While enormous numbers of people around the world still harbor the ethnic, religious, ideological, and racial hatreds that can drive nations to war, and while dictators still repress their people and commit aggression against neighbors, their numbers and power will weaken and decline in the face of growing democratic power, backed by American vigilance and strength.

The new economic phenomenon of globalization is also inherently dependent on the Net. Federal Reserve Chairman Alan Greenspan said recently, “. . . information technologies have begun to alter the manner in which we do business and create value, often in ways not readily foreseeable even 5 years ago.”<sup>4</sup> But the Net is also increasingly important to nations and governments in and of itself, as a source of power and influence on the one hand, and as a potential challenge to sovereignty and the existing political order on the other.

Democratic governments around the world, with near unanimity in fact, have concluded that development of the Net—guided by open market forces—is crucial to economic growth, as well as to the healthy development of government services, education, health care, criminal justice, and other social services. To some extent, those nations that are most successful in developing the Net also become most vulnerable to it and face cyberthreats from old sources such as other nations, terrorists, and criminals, as well as from new ones such as the Y2K bug. A RAND Corporation study for the Pentagon recognized the issue as early as 1995:

The United States has substantial information-based resources, including complex management systems and infrastructures involving the control of electric power, money flow, air traffic, oil and gas and other information-dependent systems. . . . Consequently, if and when potential adversaries attempt to damage these systems using IW [information warfare] techniques, information warfare inevitably takes on a strategic aspect. . . . There is no “front line.”<sup>5</sup>

However, the greatest threat to governments from the Net may come from a more subtle and diffuse source: their own citizens, who become ever more empowered by

the Net even as government regulations and controls weaken, for a variety of reasons. The global reach of the Net—that is, its technological indifference to political borders—is only one of the effects of the Net that weakens sovereign national control. The greatest threat posed by the Net is clearly to authoritarian governments that attempt to maintain closed societies in the face of the digital avalanche. An illuminating example of the conflict can be seen in Iran, where clerics clash over whether to use the power of the Net to export their interpretations of the Koran. A far more important one can be seen in China, where bureaucracies battle over the sharply conflicting goals of expanding use of the electronic commerce to drive economic growth and create jobs, while strictly controlling the content and transaction capabilities of the internal Chinese Net to maintain Communist Party control.

Thus, we live today in a world where nations believe that they have no choice but to develop their own information infrastructures and to increase their use of electronic commerce, even as they come to understand that the digital age can dilute their sovereignty and increase the threats to their traditional national existence and the cultures that define it. As a result, they will need to develop policies that reduce the threats, prepare themselves for conflict and competition, and balance the seemingly contradictory needs for openness and protection of technologies.

## **Net Growth and Diffusion: Definitions and Trends**

While there has been sharp debate in the past about the specific economic effects of the Net, there is no longer serious debate about its remarkable growth and extremely rapid diffusion throughout most sectors of the economy and society. According to the Department of Commerce (DOC),<sup>6</sup> it took radio broadcasting 38 years to reach 50 million people, and 13 years for television to do the same. Once opened to commercial use by the National Science Foundation in 1992, it took the Internet only 4 years. Used by more than 300 million people by March 2000,<sup>7</sup> the Internet is expected to reach over a half-billion people worldwide by 2002. While about half of all Internet users are now in the United States and Canada, the number in the rest of the world is growing at a much faster pace. Finland is now the world's most wired country, followed by nations such as Australia, Singapore, Britain, Germany, and Israel. Although overall penetration in countries such as China and India is low because of their extremely large populations, the Net is flourishing in those countries among the educated elites. Two out of three of all large European companies now use the Internet for business.

The economic impact of the Net has been staggering and positive. In the United States, the use of information technology plays a major role in propelling the "New Economy." According to the most recent DOC statistics,<sup>8</sup> information technology reduced American inflation by 0.7 percentage point over the period 1996–1998 and contributed 35 percent of American economic growth over the period 1995–1998, and productivity in information technology-using industries increased by 2.4 percent annually. Reports by the Organization for Economic Cooperation and Development (OECD) show similar results in other countries, as do individual country studies. Moreover, we are still in the very early stages of electronic commerce. The online

sale of goods and services in the United States doubled from 1997 to 1998,<sup>9</sup> and the Department of Commerce estimates that the total value of all electronic commerce will reach \$1.4 trillion by 2003.<sup>10</sup>

The digital phenomenon is also improving the working lives of millions of people. In 1999, 4.3 million people were employed in the United States in information technology occupations, and they earned an average of \$53,000 per year, compared with an average of \$28,000 per year for other private sector workers. OECD has also reported that in 1998 there were 600,000 unfilled information technology jobs worldwide, half of them in the United States alone.<sup>11</sup> No government or political party should ignore these economic facts, and few are. Since the G-7 Ministerial Conference on the Information Society in Brussels in February 1995, the governments of the United States, Canada, the European Union countries, and Japan all have accepted the powerful job-creating impact of the Net, rejecting earlier decades-long debates about the potentially negative employment effects of technology. In most of these nations, concern about developing the Net is so high that government policy is set at the highest possible levels, usually presidential or prime ministerial.

The diffusion of the Net is also changing economic and social institutions at a rapid pace. The phenomenon of *convergence*, once used only to describe the technological merging of the computer and communications industries, has now spread to a wide range of sectors from entertainment to financial services to education to manufacturing to retailing. Banking and financial services institutions, for example, facing an explosion in global electronic transactions caused by globalization and the steady replacement of cash transactions by electronic ones, are replacing their physical assets with virtual ones as quickly as they can in order to control costs. One result is a shift in economic power from traditional regulated banks to unregulated institutions such as software firms and network providers. Another is the rapid growth of global competition, since virtual financial transactions can be done in Singapore or Switzerland as easily and cost-efficiently as on Main Street. Still another is a breakdown of the 1930s regulatory system that controlled and supervised banking institutions. This broad phenomenon of convergence is thus undermining regulatory and legal frameworks that have been in place for many decades and that were based on very different industrial and social structures.

The Net also is revolutionizing government services, as waiting in line in government offices is being replaced by instant clicks on a Web site at any hour of the day or night, any day of the week, for everything from renewing vehicle registrations to applying for jobs to getting food stamps. Federal, state, and local governments are beginning to save money and provide better services to citizens by offering their services on the Net. Moreover, by replacing human assets—civil servants—with virtual ones, governments also make themselves more transparent in ways that empower citizens. A wealth of government information is becoming easily available online—without bureaucratic intervention.

Perhaps most important, the Net is blurring the lines between government agencies and challenging the existing organization of government. For example, President Clinton signed an Executive memorandum on December 17, 1999, directing, among other things, that government agencies “promote access to government information

organized not by agency but by the type of service or information that people might be seeking.”<sup>12</sup> In the future, the Net may further challenge national governments. As part of the phenomenon of globalization, it is shifting more power into the hands of international organizations, especially in the economic and legal fields, thus potentially diminishing the sovereignty of national and even local governments—a trend that is generating political opposition from the right and the left.

Similar changes are taking place in health care and other public institutions. A proliferation of health care Web sites is changing the practice of medicine by providing patients with more information than they had ever had at their disposal—and giving them new leverage with physicians. Education, retailing, manufacturing, entertainment, and other fields are being similarly transformed by the Net. In particular, the old seasonal and pedagogical model of elementary and secondary education is beginning to be revolutionized by the new networked technologies, hopefully to help provide the human capital that is necessary to raise living standards and sustain the digital age.

Governments around the world, having observed the surge of technology and the powerful economic turbocharge provided by the Net, as well as its transformative effects on so many critical sectors, are moving to develop and implement policies to promote its growth and use. These policies have been in place in some countries and regions—such as the United States, the European Union, Singapore—for a number of years, while other countries—for example, India, Estonia, the Philippines—have adopted them more recently. What is particularly remarkable is the almost unanimous view that market forces and competition should play the leading role in development of the Net, and that the government’s role should be secondary—as an enabler that removes regulatory obstacles and deals with negative effects such as the exposure of children to objectionable content, and as a leading-edge user of the new technologies.

This role for the private sector empowers it as a policymaker in areas such as the protection of individual privacy, the provision of universal access to the Net, and the security of the Net. Thus, the private sector worldwide becomes an important new actor with which most governments will have to deal on a new basis. This provides a national advantage for the United States, which is exceptional in its acceptance of private power.

## **Government Policies: An Overview of the Key Players**

The United States was the earliest believer in the ability of the new information infrastructure to build national economic power. The Federal Government played an early, key role in Net development. While much of the basic technology underlying the Internet was derived from research done by the Department of Defense Advanced Research Projects Agency—research that created the Advanced Research Projects Agency Network—civilian agencies such as the National Science Foundation and the National Bureau of Standards (now the National Institute of Standards and Technology [NIST]) also played an important early role. By the 1980s, as the importance of the new technologies became more obvious, and in spite of a political debate about “industrial policy,” the Bush administration, with backing from key Democrats such

as then-Senator Albert Gore, established the High Performance Computing Program and the Advanced Technology Program to fund key research in the field. The Federal Government currently is spending about \$1.7 billion on such research, which involves many partnerships between government agencies, corporations, and universities. The administration's fiscal year 2001 budget calls for spending of \$2.3 billion, with the largest increase of 56 percent for the Department of Defense. Projects include advanced research on encryption, ubiquitous computing, broadband optical networks, data storage filters, and mining and wireless networks.

The importance with which this policy is viewed is underscored by its bipartisan support. In fact, all of the candidates in the 2000 Presidential race supported it. As *The Wall Street Journal* recently reported, "All the candidates recognize technology as central to the current boom. Mr. Gore and advisors to Mr. Bush say they believe that the economic gains from computer technology today echo the way electrical technology lifted the American economy a century ago."<sup>13</sup> The *Journal* story went on to point out that both Vice President Gore and Senator John McCain favor increasing spending on research. In fact, a recent report by the President's Information Technology Advisory Committee raised the alarm that the Nation might fall behind unless the feedstock of research that is supplying the Internet boom is replenished: ". . . the current boom in information technology is built on basic research in computer science carried out more than a decade ago. There is an urgent need to replenish the knowledge base."<sup>14</sup>

Government support for Net research, however, is only the tip of the policy iceberg. In fact, by January 2000, it was a rather small part. The main body of Federal Net policy was spelled out in *A Framework for Global Electronic Commerce*,<sup>15</sup> a document announced in the White House by President Clinton and Vice President Gore before an audience of Net users and creators. Clinton summed up the document's content: "Government can have a profound effect on the growth of commerce over the Internet. . . . Knowing when to act—and at least as important—when not to act—will be crucial." The basic thrust of the document is that development of the new information infrastructure and electronic commerce should be the responsibility of the private sector and be driven by market forces and competition. Government's role should be to deregulate, modernize government, and help create a level playing field internationally.

Key actions of the administration based on the policy framework and other initiatives have included deregulating telecommunications, relaxing export controls on encryption and supercomputers, offering electronic government services, "jawboning" the private sector to deal with issues such as privacy and objectionable content, modernizing copyright law, providing funding for Internet access for schools and hospitals, and negotiating a series of critical international agreements. Among the key international agreements and negotiations have been the Global Agreement on Basic Telecommunications, the World Trade Organization agreement to a moratorium on duties on electronic transactions, the International Technology Agreement, the World Intellectual Property Organization agreement on digital copyright, negotiations on the tax treatment of electronic transactions, and a series of bilateral and multilateral agreements articulating the principles of the framework document.

To a surprisingly large extent, the U.S. framework principles and the idea of government support for research have generally been accepted by governments—at least in principle—with varying ideological roots, political frameworks, and economic systems. Although it is impossible in this paper to adequately cover a substantial number of national policies in any detail, what follows is a snapshot of some key countries.

The Canadian position on the Net is best summarized in the government report *Convergence Policy Statement*<sup>16</sup> and in the 1997 report of the Information Highway Advisory Council,<sup>17</sup> which call for liberalizing and deregulating telecommunications and cable services, relying on competition and the market, ensuring universal access, and protecting Canadian culture. Canada's budget for 1997 initiated a 5-year, \$800-million program, principally for the national research and academic network.

Japanese views on the Net are expressed well in the Ministry of International Trade and Industry (MITI) paper *Toward the Age of the Digital Economy*. . . .<sup>18</sup> This paper recognizes the primacy of the private sector and the marketplace and the role of competition in developing the Net. While MITI has pushed for faster liberalization, other ministries, such as the Ministry of Posts and Telecommunications, have slowed the pace of telecommunications liberalization. Japan has also committed public funding for research on advanced computing and communications. An interagency committee directed by the Prime Minister's office coordinates policy.

South Korea's vision for the Net is similar to Japan's and is spelled out in *Cyber Korea 21*,<sup>19</sup> which aims to create one million new jobs.

The Philippines is an example of a developing country that has embraced the Net as a strategic and economic asset for the Nation's future. Its report, *IT21: Action Agenda for the 21st Century*,<sup>20</sup> calls for a new sound regulatory environment for electronic commerce, the use of education and training for the development of human capital, liberalization of foreign investment laws, and the creation of "cyberparks," or high-technology industrial parks.

Malaysia and Singapore have also embraced the Net as an economic tool, as outlined in their respective policies, *The Way Forward—Vision 2020*<sup>21</sup> and *IT 2000—A Vision of an Intelligent Island*.<sup>22</sup> Both papers portray the Net as crucial to national aspirations and provide for substantial government funding and incentives for investment in computing and communications. Singapore's authoritarian style of government and its view that its national culture is fragile have led the government to take strict measures, however, to regulate the use of the Net, including the licensing of Web sites. Malaysia has more recently taken similar steps.

China has invested heavily in the development of its backbone research and academic network, China Education and Research Network (CERNET), and has even moved to deregulate telecommunications to some extent and to liberalize foreign investment in Internet projects. The region around Tsinghua University, where CERNET is based, has become a magnet for high-technology ventures. The Chinese government is also setting up Internet ventures, such as the 21 Dragon News Network, eastday.com.cn, and CCIDnet.com, to promulgate its own views and ideology.

But despite the Chinese government recognition of the key strategic importance of electronic commerce, it has also cracked down on Internet use. Beginning in February 1996, China required registration of all intranets within the country and also

required connections only through the Ministry of Posts and Telecommunications. During the subsequent years, China has toughened its rules, going so far as to sentence a programmer to 2 years in prison in 1999 for supplying a list of email addresses to a prodemocracy movement.<sup>23</sup> By early 2000, China's internal security forces were trying to require companies using encryption to use locally developed products and register their use, for obvious reasons. Ministries more interested in attracting foreign investment, on the other hand, were ignoring the rules.

However, as David Gompert, a former Deputy Under Secretary of State for Political Affairs and Special Assistant to the President for European and Eurasian Affairs, has pointed out, "Beijing will not be able to forestall a national information revolution. . . . Different as China might be . . . an authoritarian regime will be unable to withstand pressure for both political and economic freedom if it is to achieve technological success."<sup>24</sup>

India's experience proves that the power of the private sector in developing the Net is such that a country can succeed in spite of outmoded government policy. As two Indian economists have observed, "For the NII [national information infrastructure] to have its full impact upon the economy, a clean break with conventional ideas in India's telecomm sector is called for."<sup>25</sup> Regulatory changes are exceedingly slow in India. The nation enjoys so much software talent and individual entrepreneurship, however, that India now employs more than 40,000 software engineers in an industry that is growing at 40 percent per year. Two-thirds of Indian software exports go to the United States, served both through high-speed satellite uplinks and the movement of people between the two countries.

Driven by concerns about U.S. strategic dominance in the fields of computing, communications, and microelectronics, the European Union began its European Strategic Program for Research and Development as early as 1982. Its specific program for development of the Net began in earnest in 1994 and culminated in 1997 with the publication of *A European Initiative in Electronic Commerce*.<sup>26</sup> The Initiative stated that the "expansion of electronic commerce would be market driven," and that there would be "no regulation for regulation's sake." It also recognized that "electronic commerce is inherently a global activity," but stressed the need to rely on the World Trade Organization (WTO) and other international forums—an acceptable substitute for U.S. dominance.

However, the European Initiative left considerably more room for government action to support the development of the Net than did its U.S. counterpart. In a major speech on the Net in 1997 that reflected the French government's digital *dirigisme*, French Prime Minister Jospin said, "In reality, despite a certain discourse on the seemingly unavoidable withdrawal of the State, throughout the world, public powers are actively assisting in the development of new technologies and services. . . ."<sup>27</sup> Thus, while Europe moved ahead in principle with the deregulation of telecommunications and agreed to such initiatives as the duty-free treatment of electronic transactions, some of its governments were ready to intervene whenever they thought it was in their interest to do so.

The tradition of private sector leadership was strongest in the United Kingdom, and telecommunications had been liberalized there in 1984. By 1997, the United

Kingdom led the nations of the European Union in Internet access for business and home, as well as in the use of electronic commerce.<sup>28</sup> The United Kingdom has moved quickly to shift government services onto the Net and is also a leader in the use of self-regulation by industry to deal with issues such as objectionable content.

France made an early but misguided start on the Information Age with the government-funded Minitel project of the mid-1980s; its videotext system was soon obsolete. Nevertheless, the French government could not rid itself of government control. Said a 1998 French government report, "France's entry into the information society represents an issue of decisive importance for our future. . . . That is why the government is offering the people of France a project and a political vision of information and communications technology. . . ."<sup>29</sup>

Virtually every other European government has a high-level plan to achieve Net superiority, lying somewhere on the scale between the United Kingdom's liberal approach and the French statist view. Finland, for example—the world leader in Internet usage—aspires to jump ahead and become the first "Wireless Information Society." Finland is already the nation with the highest penetration of Internet hosts and cellular telephones and the leading Internet banking nation.<sup>30</sup> While the vital presence of the Nokia Corporation is one reason for this development, another is the Finnish government's conscious decision in 1995, as the Soviet Union broke up, to develop a brand new strategic thrust for the future.<sup>31</sup>

Across the Baltic Sea, Estonia has followed the Finnish lead and is well on its own way toward Net maturity, with Internet hosts for every 54 citizens, ranking just behind Finland and the United States.

Beyond North America, Europe, and Asia, in both the industrial and the developing worlds, governments are doing much the same. From Australia to Egypt to Brazil, building and using a robust Net and integrating it into national institutions are high on the agendas of every government, often involving the President or Prime Minister personally. Under the auspices of the Organization of African Unity and the United Nations, for example, a plan has even been developed for Africa—the least developed part of the world in terms of telecommunications usage—for an African Information Society Initiative.<sup>32</sup>

Thus, a substantial number of the world's governments—industrial and developed, democratic and authoritarian—have accepted the notion of the centrality of the Net to their future economic and political power. All are engaged in developing policies to develop the Net and encourage its use as quickly as possible. The democratic nations—especially the United States, with its robust private sector and values of free expression—enjoy the largest advantage.

In many cases in the past, national competitions like this often led automatically to international conflict. Colonialism and mercantilism, for example, were in large part zero-sum games with winners and losers. The physical resources that were the object of the game—land, sea-lanes, natural resources—were limited. But the digital world, with its infinite supply of virtual content and wealth, is a win-win game. Everyone who plays can win. The more who play, the more who win. The only sure losers will be those who do not play at all.

This suggests that some of the major causes of domestic and international conflict should ease, since virtual wealth—as opposed to physical wealth—is infinitely expandable, and nations will have less need to fight over scarce resources. Nevertheless, those nations that are the most skillful in expanding their virtual power may well use their new power to export old ideologies or to redress ancient ethnic or national grievances. Since countries such as France and Canada have already proclaimed their intentions of using the Net to propagate their cultures, there is no reason why other governments should not attempt to use the Net for more belligerent and less peaceful purposes. North Korea, Iraq, and Iran are among the governments that could use the Net to enflame ideological and religious hatreds. Chinese officials have threatened Taiwan with cyberwarfare. Cuba, for example, used Web sites such as that of *Granma*, its news agency, to propagandize the case of Elián González. More seriously, of course, they and other countries could target the electronic commerce and digital government activities of the United States and other democracies for cyberwarfare—the darker side of the Net for which the United States must be prepared.

Just as the rise of maritime power required the development of new international laws to deal with conflicts on the high seas, the rise of virtual power establishes the need to develop international norms and laws as we colonize cyberspace. But maritime law took centuries to develop. Even negotiation of the Law of the Sea Treaty took more than a decade. There are other interesting analogies to the development of maritime law. For one thing, just as piracy on the high seas stimulated the growth of a new legal framework, so too piracy in cyberspace—notably, the theft of copyrighted material such as software—is pushing the limits of global intellectual property law. While the bulk of such piracy is committed by private entities, governments are also involved, sometimes through the outright sanctioning of digital privateers, and sometimes by attempting to weaken the international copyright framework.

In addition, just as the rise of naval power resulted in a growth in the importance of coastal cities and regions, the growth of the digital world is creating cybercoasts and regions. In the United States, for example, Internet penetration is highest in San Francisco, San Diego, Chicago, Seattle, Portland, New York, Los Angeles, Boston, and Washington, almost all coastal cities.<sup>33</sup> The Australian government is concerned about the difficulties in pushing Net penetration beyond its coastal regions and into the interior of the country.

With the Net and its challenges growing daily and exponentially across borders, there is an urgent need for governments to move beyond their national policies and work for new international agreements on everything from taxation to consumer protection to the use of cryptography.

Moreover, almost all new laws for cyberspace, whether developed at the national, state, or provincial level, must pass international muster, given the borderless nature of virtual transactions and electronic commerce. In fact, these negotiations are ongoing in such forums as OECD, the UN Conference on International Trade Law, the WTO, the Wassenaar Agreement, and numerous regional and bilateral negotiations and agreements. By entering into these international discussions, however, nations have already acknowledged the potential of cyberspace, given its borderless nature and other key characteristics, to weaken the nation-state and its subunits and chal-

lenge governments everywhere. The most serious challenge to governments from the Net over the long term is not from international conflict but from internal challenges from their own people and from new forms of political, social, and economic organization made possible by the Net.

## Challenges to Government Power

*The traditional powers of the nation-state will suffer somewhat as a result of the information revolution . . . nation-states will increasingly find their powers curtailed by the availability of information to those who reside both within and outside their borders; and those powers that remain will increasingly have to contend with nonstate actors who are acquiring power.*  
— John Arquilla and David Ronfeldt<sup>34</sup>

Perhaps the greatest irony of the digital phenomenon is that while governments everywhere embrace it, they also face serious challenges from it, many of which they are just beginning to understand. The most advanced democratic nations certainly understand their vulnerability to technical disasters, and their methodical and successful preparation for the Y2K problem illustrated that. (It also proved that with careful planning, nations could deal successfully with difficult technical security issues.) Most nations also understand the potential threats of cyberwarfare, cyberterrorism, and cybercrime, although they have not yet developed comprehensive measures to deal with them.

The United States has commissioned a variety of studies on these subjects and is implementing a wide variety of measures to deal with these threats.<sup>35</sup> These encompass the White House; the Departments of Defense, Justice, and Treasury; agencies such as the Securities and Exchange Commission and the Federal Trade Commission; the intelligence community; and state and local law enforcement. As Dorothy Denning at Georgetown University has pointed out, cyberwarfare is a particularly difficult challenge:

Modern information technology has created many new possibilities for information warfare. Operations can take place in an instant and come from anywhere in the world. They can be orchestrated from the comfort of a home or office. . . . The number of targets that potentially could be reached is staggering. . . . The cost to the perpetrators might be negligible, the losses to the victims immeasurable.<sup>36</sup>

The subject of information warfare and the related matters of cyberterrorism and cybercrime are important subjects in and of themselves, but threats to the overall security and thus stability of governments are much more compelling.

If technical security has been the major Net concern of the major democratic powers, communist and totalitarian states have had an additional and much more serious preoccupation with the Net—its uncanny ability to empower individuals and groups. For example, in January 2000, the Chinese government announced new regulations requiring firms to use only encryption technology developed in China, to reg-

ister the type of encryption they use, and to provide details about employees who use encryption. According to *The Wall Street Journal*, the new rules are aimed at stopping Internet use by groups such as Falun Dafa. The Chinese government organization that enforces the new rules reports to the State Council and is staffed by the Ministry of State Security.<sup>37</sup>

China is certainly not alone. While its regime is more benign, Singapore has moved aggressively to control use of the Internet by its population even as it has encouraged the growth of electronic commerce. As one observer noted, “. . . the government has embarked on an ambitious attempt to superimpose strict . . . censorship on the medium. Other authoritarian regimes in Asia have been inspired by this model of regulation.”<sup>38</sup> Singapore and China are right to fear the power of the Net. If wealth and power in the 21st century are increasingly based on the possession not of territory or physical resources, but of information and knowledge, then the growth of the Net will spread both wealth and power, threatening those whose power is more limited physically.

Daniel Bell foresaw this in 1973 when he wrote, “If capital and labor are the major structural features of industrial society, information and knowledge are those of the post-industrial society.”<sup>39</sup> Communist Party ideologists in Moscow derided Bell’s views when he published them, but a decade later, the Soviet policy of *glasnost*, or permitting a freer flow of information from news media, began to wash their system away. By 1989, it was gone. That was even before the rise of the Net.

What are the specific characteristics of the Net that pose such a challenge to national power and sovereignty, especially for authoritarian and totalitarian nations? The most important is the Net’s pulverization of borders. Electronic bits ignore political and physical boundaries as they speed along fiber-optic cables or over satellite transmission bandwidths, and the use of packet switching breaks intelligent messages into pieces that move over almost random pathways: “Information . . . moves around the world on the wings of energy too small to be sensed without instruments. . . . Information is diffusive; it leaks like a universal solvent despite great and continuing efforts to contain or restrict its spread.”<sup>40</sup>

This digital disregard for borders has a number of effects. First, it simply reduces the overall power of governments to control their citizens. As Lawrence Lessig of Harvard Law School has pointed out, in explaining how in the past governments used borders to make it more expensive to escape their control, “Borders keep people in and hence governments could regulate. Cyberspace undermines this balance . . . escape from regulation becomes easier. The shift is away from the power of government to regulate, and toward the power of individuals to escape government regulation.”<sup>41</sup>

Second, cyberspace blurs the normal powers of government. Who has the right to collect taxes on a transaction when goods are produced in one country, warehoused and shipped from a second, ordered from a server in a third, and shipped to a customer in a fourth? Whose intellectual property laws apply to copyrighted material in cyberspace? Whose consumer protection laws apply, and whose courts hold jurisdiction? Indeed, does virtual information have any standing in national courts? Does the private sector “usurp” government power when it creates privacy “law” by developing software to protect individual privacy?

Moreover, who really controls cyberspace when even governments proclaim that the private sector plays the leadership role? It is difficult to cite any historical instance of a government relinquishing control over such a pervasive development as the Net. Whether it was the initiation of closed and recorded boundaries for real property in Tudor England, or government ownership or regulation of basic industries such as electric power generation or telecommunications in the early part of the 20th century, governments have always attempted to maintain control over key economic and technological developments. In the case of the Net, thanks to strong U.S. leadership, most have acknowledged the primary role of the market and competition. Although this was the right choice, it does not favor the growth or even maintenance of government power in a future in which most institutions are organized and run around the Net. Not only will governments face new difficulties in dealing with strengthened, legitimate private institutions such as banks and corporations, but also they will face greater threats from illegitimate ones such as criminal organizations and terrorist groups.

Third, cyberspace is developing too fast for most governments to deal with in an orderly manner. Democracies usually make wise choices, but only because they divide and separate powers and take a long time to pass new laws. The colonization of cyberspace may be proceeding too quickly for them to deal with in a rational way; its outlines may be complete before the political systems have a chance to shape them. Authoritarian regimes, on the other hand, can move quickly but generally make bad decisions. China's rules on encryption may help control its citizens for a brief time, but, more importantly, they will retard Chinese economic development, which may be an even greater long-term threat to the regime in Beijing. China's encryption rules are only one example of China's need to restrict the free expression of ideas that is one of the prerequisites for development of the Net.

An excellent example of the difficulty that governments face in keeping up with the velocity of information technology developments lies in the area of export controls. According to the Computer Systems Policy Project, 75 percent of computer company revenues in 1998 came from products that did not exist just 2 years before.<sup>42</sup> The implication of this for governments is that computers that are controlled for export and defined as *supercomputers* by the government have been commoditized and are already being sold in huge numbers, even before the government can move to control them. In testimony before the House Armed Services Committee, a representative of the industry commented on the government's move in July 1999 to raise the threshold for export control purposes from computers performing 2,000 million theoretical operations per second (MTOPS) to 6,500 MTOPS:<sup>43</sup> "Computers that will perform up to 6500 MTOPS are now widely available from U.S. and foreign manufacturers, as are the components and know-how to manufacture such computers."<sup>44</sup> Moreover, the worldwide proliferation of multiprocessor systems, based on chipsets such as the Pentium III, and the ability to manufacture them, is exploding. The Gartner Group points out that by 1999, factories in such countries as Taiwan, Hong Kong, China, Korea, and Malaysia, as well as many in Europe and the Americas, could build multiprocessors exceeding 2,000 MTOPS. Said Gartner, ". . . infor-

mation needed to build such systems from components or subsystems is readily available on the Internet."<sup>45</sup>

While the new supercomputer export control thresholds of 6,500 MTOPS in July 1999 was seen at the time as a hard-won victory for high-technology industry, it was totally obsolete within a mere 6 months! On February 1, 2000, President Clinton raised the threshold to 12,300 MTOPS, while still maintaining the complex licensing system. Moreover, in January 2000, the administration also moved significantly toward lifting the export licensing requirement on encryption, allowing all retail encryption programs to be sold overseas. Rapid advances in strong encryption technology, coupled with the important need to protect security on the Net, forced the change.

A December 1999 report of the Defense Science Board<sup>46</sup> examined the impact of information technology and globalization on the effectiveness of export controls. It concluded the following:

. . . the utility of export controls as a tool for maintaining the United States' global military advantage is diminishing as the number of U.S.-controllable militarily useful technologies shrinks. . . . Clinging to a failing policy of export controls has undesirable consequences beyond self-delusion. It can limit the special influence the United States might otherwise accrue as a global provider and supporter of military equipment and services . . . shutting U.S. companies out of markets served instead by foreign firms will weaken the U.S. commercial advanced technology and defense sectors upon which U.S. economic security and military-technical advantage depend.

Export controls, however, are only one example of government's difficulties in keeping up with the software engineers and venture capitalists. The Net is nurturing globalism and revolutionizing institutions far faster than cumbersome 19th-century government structures can move. This speed, combined with the Net's other characteristics—its borderless nature and its blurring of government power—is, on the whole, a large advantage for the industrial democracies. While they must still deal with issues such as privacy, telecommunications regulation, access, and even sovereignty, their existence itself is not threatened by the Net, even though their governments' power, in the old sense, is weakened.

On the other hand, the Net seriously threatens the existence of authoritarian and totalitarian regimes. The diffusion of knowledge and the openness of information simply cannot be tolerated by governments like China, Iran, or Iraq, and it even needs to be limited by more moderate but still authoritarian governments such as Singapore and Malaysia. This basic assertion about the Net—that it threatens non-democratic governments—gives rise to some fundamental thoughts about a framework for U.S. policy.

## **A Framework for Policy Choices**

As we have seen, the industrial nations, as well as most others, have concluded that the development and use of the Net will be an important component of their national strength—perhaps the single most important—in the 21st century. Most nations are implementing a variety of policies to facilitate this development and use by

the private sector as well as by government. These policies require the free interchange of goods, ideas, technology, capital, and people across borders, and the deregulation of national economies.

On the other hand, nations are apprehensive about the Net. All are concerned with their security as they become more dependent on cyberspace, and the non-democratic ones are most fearful and worry about their ability to maintain control over their populations in this global electronic village. Thus, most governments are moving to defend their critical infrastructures, and some are trying to control the use of the Net by their own people.

The United States arrives at this juncture in a position of enormous strength. It dominates the Net technologically, economically, and even culturally. Not only is English the Net's language, but also the Net's very "coolness," its antitraditional style, is quintessentially American. As Don Heath, president of the Internet Society says, "If the United States government had tried to come up with a scheme to spread its brand of capitalism and its emphasis on political liberalism around the world, it couldn't have invented a better model than the Internet."<sup>47</sup>

Both the private and public sectors deserve credit for American success. While private entrepreneurs have built the Net, the government has followed a policy for almost two decades of deregulating and letting the market take the lead. The Reagan, Bush, and Clinton administrations all deserve credit. Europe, on the other hand, the also-ran in the Internet race, is behind. As Thomas Middelhoff, Chief Executive Officer of Bertelsmann AG, says, "Europe just doesn't get the message. Governments . . . don't seem to understand that the best way to deal with high unemployment is to put money into developing new technologies, not preserving old ones."<sup>48</sup> Other contenders, such as Japan and China, also lag far behind as they agonize over relinquishing control over such a powerful and central phenomenon.

Yet the American success in dominating the digital world—and its early successes in formulating digital policy—is not yet matched by a comprehensive, long-range foreign policy response to the worldwide challenges posed by the Net. To quote David Rothkopf, former Deputy Under Secretary of Commerce, "For the U.S. Government, the challenges of formulating foreign policy in this environment are myriad. Our institutions are not suited to it. They are designed to relate to other government entities and are ill-equipped to deal with a world in which nonstate actors are of vital importance . . . they lack even the apparatus to analyze the trends shaping this new period much less their consequences."<sup>49</sup>

To further enhance its own substantial technological and economic Net strength, the United States should institute a principled policy focused on facilitating global access to, and use of, the Net. On the whole, widespread use of the Net by people and their institutions around the world will serve U.S. interests in two ways. First, the more people and institutions that use the Net, the more important it becomes, thus further enhancing the U.S. position. Second, global use of the Net will weaken both actually and potentially hostile nations—the nondemocratic world. Those who resist the Net's imperative will weaken their own economies and reduce their own future influence and power. Five basic principles warrant consideration: accelerating de-

regulation, providing more openness, offering global leadership, maintaining security, and developing human potential.

### *Accelerating Deregulation*

While the United States has deregulated many industries during the past decade, the process is far from over. With regard to the Net, there are two categories of deregulatory policies that should be implemented. The first category deals with telecommunications; the second, with other industries and the public sector.

As policymakers have focused on the phenomenon of convergence, they have tended to think of deregulation narrowly, in terms of the jurisdiction of the Federal Communications Commission and the Telecommunications Act. Thus, in 1996, Congress amended that Act, in its view deregulating further the telecommunications markets by opening up to competition not only long-distance service but also local telephone service as well. The problem is that not only did lobbying by the key players make the Act so complex that it is taking years even to achieve its own narrow purposes, but also the Act barely took notice of the Internet. In fact, the only references to the Internet in the Act are the Communications Decency Act, an attempt to censor content on the Net, which was stuck down by the Supreme Court, and new government support for connecting schools and hospitals to the Net, a worthy goal but one that was flawed by adding a new but hidden telecommunications tax.

What is needed is a much broader leap of the imagination: terminating the Federal Communications Commission altogether as an organization and making a much more substantive move to allow market forces and competition in technology to deal with the issues of wired and wireless telephony, cable, broadcasting, and their relation to the Internet. Natural monopolies in communications simply do not exist anymore, and it is foolish to pretend that they do. Internet telephony is growing rapidly. Radio stations broadcast worldwide on the Internet. Cable, telephone, satellite, and cellular modes all compete with each other. Lingering regulatory needs in areas such as allocating spectrum or overseeing amateur radio could be administered by Commerce Department agencies, including the National Telecommunications and Information Administration and NIST. The Department of Justice and the Federal Trade Commission both oversee the Sherman Act and other monopoly concerns. They have vigorously executed their mandates, prosecuting Microsoft, investigating Intel, and overseeing such proposed mergers as those of American Telephone and Telegraph with MediaOne, and Bell Atlantic with New York Network Exchange. Such a move would not only free up and speed new technologies and ventures in the United States, but it also would help force other nations to deregulate more quickly.

More broadly, the Nation needs to continue to deregulate other industries and work for their deregulation around the world in the WTO and other forums. Moreover, areas such as education and health care need attention. The monopoly that exists in K-12 public education has stifled true reform. Mechanisms that provide more competition from the private sector, even on an experimental basis, would help force the kind of revolutionary change that is needed to prepare children for the digital age. In health care, burgeoning public programs are adding layers of regulation and bureaucracy. Programs that bolster competition should be tried here.

Those who fear that a further loosening of the Federal reins would engender more digital crime and exploit consumers should examine the development of the privacy issue. The Clinton administration promoted self-regulation—with a big stick: the threat of new legislation. The Federal Trade Commission is ready and has already taken numerous actions to protect privacy on the Net. New laws in the most sensitive sectors—medical and financial privacy—have passed or are pending. But industry has also moved quickly to develop a variety of technological means as well as self-policed codes of conduct to protect privacy. The jury is still out on the final results, but the interim report card is encouraging—although still not quite a passing grade.

### *Providing More Openness*

The Net thrives in open societies and withers in closed ones. Moreover, as David Gompert has pointed out, “. . . military and other forums of power depend increasingly on knowledge and thus on the openness and global integration that spawn and sustain information technology.”<sup>50</sup> The free flow of ideas, goods, services, and people are the basic building blocks of the Net. Government should strengthen all of them. Nineteenth-century ideas about government censorship or import barriers should be demolished. Twentieth-century ideas about controlling the export of technology or intellectual property also need to evolve.

Specifically, the government should continue to work to lower trade barriers, particularly in the area of high technology. The so-called International Technology Agreement II, which would broaden the duty-free treatment of high-technology goods, should be pushed hard at the World Trade Organization. Barriers to technology flows should also come down with a WTO agreement on streamlining the international testing system for high-technology goods. The government should also stop its practice of placing international restrictions on the use of intellectual property in research and development contracts with high-technology firms. This becomes increasingly important as the number of public and private research projects in advanced computing and communications grows.

Most important, the cumbersome system of export controls developed during the Cold War needs to be ended. With a few important exceptions, the use of technology by other countries will strengthen the U.S. position, not threaten it. Even Richard Perle, Assistant Secretary of Defense with responsibility for export controls under President Reagan, has said, “We no longer live in a world where it is vitally important that advanced technologies be tightly controlled. . . . I don’t think we can effectively control raw computing power.”<sup>51</sup>

Export controls still involve four “tiers” of countries, nine major Federal Government agencies or departments, and at least five different major international agreements. Export reviews can take so long that they outlast the life cycle of the product. For example, while the government has doubled the supercomputing threshold in 6 months, as we have seen, to over 12,000 MTOPS, IBM is building “Blue Gene,” a *petaflop* supercomputer capable of a thousand trillion floating point operations per second! Blue Gene will be 500 times faster than the two fastest supercomputers operating today—at Lawrence Livermore and Los Alamos National Laboratories. While Moore’s Law dictates that such a speed would take 15 years to

achieve, IBM plans to build Blue Gene in only 5 years. Its initial purpose will be civilian—to understand protein folding in genes—and more civilian applications will undoubtedly follow very quickly.

Moreover, as we have seen, foreign competition is ubiquitous. Products providing strong encryption, for example, are available from numerous other countries—for example, Germany, Russia, and Israel. What is needed is a much more streamlined and targeted system—a sniper's rifle, not a sawed-off shotgun. Such a system would restrict controls to what have been called "chokepoint" products and technologies, or those needed specifically to produce weapons of mass destruction—nuclear, biological, and chemical. It would not attempt to control mass-market products and technologies or those available in foreign countries outside the multilateral control regime. It would target bad actors, both governmental and private, and focus resources on preventing them from acquiring advanced technology.

Specifically, the U.S. Government should implement the recommendations in the Defense Science Board report, which calls for shifting from a policy of technology protection to one of essential capability preservation. This would include establishing a continuously evolving list of essential military capabilities and developing strategies for preserving each. It would abandon the protection of capabilities and technologies available on the world market.<sup>52</sup> Such a policy would also treat more harshly those who deal with the few "Tier IV" or terrorist nations, establishing tougher criminal penalties and other civil penalties for companies that are found to have violated the rules on dealing with them.

Perhaps the most difficult export control issue is that of encryption. Encryption is used in the digital world not only to encode information but also to authenticate transactions and for other security and legal purposes. It is a prerequisite for electronic commerce. It should also be fundamentally decontrolled, with the exception of sales to terrorist states. At the same time, however, the Government needs to clarify domestic law related to the Wiretap Act, permitting the Federal Bureau of Investigation (FBI) and other law enforcement agencies legal access to plaintext under a court order. Continued increases in funding for encryption research by the FBI and intelligence agencies are also needed.

### ***Offering Global Leadership***

The United States can provide global leadership mainly through implementation of the other four principles, but it can also move beyond this. The foreign policy community should set as a major priority the impact of the Net on our foreign policymaking processes and priorities. For example, the United States has been leading the movement among international organizations to deal with the positive and negative effects of the Net. But we should be asking ourselves if the current international organization framework is suitable to begin with. Is the diffusion of the Net important enough to merit a new international organization, much as new trade and investment needs after World War II created a need for the General Agreement on Tariffs and Trade, the International Monetary Fund, OECD, and the World Bank? Moreover, are our own foreign policymaking institutions up to the task? For example, are they

leading-edge users of the Net themselves? In most cases, the answer is no. A high-level study is needed of these issues.

Moreover, the United States should set as a major foreign policy priority making the rest of the world—especially the developing countries—Net-ready. We have already taken major steps to that end, such as the elimination of tariffs on most high-technology goods, the global agreement to deregulate basic telecommunications, and the numerous bilateral agreements on electronic commerce. Another step might be to focus on a single region. Latin America would be the best candidate. Although the region is of great economic and strategic importance to the United States and has made democratic progress, there are crises of democracy in a number of countries. Rapid deployment of the Net would boost economic development and help cement ties to the United States. Additionally, the United States should develop a single yardstick by which nations—especially developing ones—can measure their progress in creating a benign policy environment.

A number of such yardsticks are available now. Among the most important are the Asia-Pacific Economic Cooperation Group's Readiness Assessment Tool,<sup>53</sup> and the guide for developing countries, *Readiness for the Networked World*, developed at Harvard University.<sup>54</sup> Both of these create measurements based on a number of categories such as basic infrastructure and technology, access to services, current Internet penetration, human resources policies, use of electronic commerce by business and government, and the creation of a sound legal framework, privacy laws, tax regulations, and the like.

Organizations like the Agency for International Development, the National Telecommunications and Information Agency, and the National Science Foundation could provide training for developing country officials based on these guides. Industry support could also be solicited. While the private sector will lead the global diffusion of the Net, government can help clear away the policy underbrush. In fact, the private sector has already begun to size up Net business prospects around the world. Legg Mason has published *The Building Blocks of Growth in the "New Economy,"* which ranks countries on their overall Net policies. Not surprisingly, democracies like the United States, Canada, the United Kingdom, Denmark, and Finland score highest, while China and Russia score the worst.<sup>55</sup>

### ***Maintaining Security***

Because digital competence and infrastructure are key pillars on which national power rests, national security resides in the protection of both. Digital competence can be nurtured with the measures already discussed. The Government has begun to take measures to protect the infrastructure but needs to go further. The recommendations of the President's Commission on Protecting Critical Infrastructure have begun to be implemented through a series of Presidential directives and Executive orders. Most importantly, focal points have been established on the National Security Council staff and at the FBI, and funding is being provided for research. The new National Center for Critical Infrastructure Protection should be the focal point for both public and private research in the area. In addition, more cooperation is needed with industry, and while government should avoid mandating standards for security, more re-

search is needed on standards. The National Security Telecommunications Advisory Committee is one forum for achieving this, but it is too narrow.

Moreover, the Armed Forces need to focus on both defensive and offensive measures for information warfare. The December 1999 Defense Science Board Report on Globalization and Security contains a list of detailed recommendations dealing with defensive measures that should be implemented, including an Essential Systems Software Assurance Program, software certification systems, research at the Defense Advanced Research Projects Agency and NIST, and the use of red teams to test defense security.<sup>56</sup> Congress must also provide adequate funding and a means for the services to attract talented personnel. The legal issues surrounding the use of offensive information warfare must be carefully studied and debated, so that clear and quick decisions are possible if such measures have to be used at some point in the future.

### ***Developing Human Potential***

The Net will continue to develop most quickly in those nations that afford their populations the best environment to develop their full potential, including their work skills. Specifically, U.S. policy should be aimed at three areas. First, we need to achieve 100 percent access to the Net for all of our people. This should be achieved not by the 19th-century model of “universal service” but by encouraging market forces and providing government support for access to public places such as schools, post offices, libraries, and public information kiosks. These programs should be supported from general revenues, not by new taxes on telecommunications or Internet services, the very areas we are trying to stimulate. Countries that do not provide universal access will generate a “digital divide” and encourage future economic and social conflict within their borders.

Second, we need to encourage immigration of the brightest people from around the world to narrow our talent gap. We should automatically grant U.S. citizenship to those who acquire a Ph.D. in engineering or science in the United States, encouraging them to stay here. They will help us maintain our lead, but they will also establish strong connections with their home countries, generating growth there. The Indian immigrants to the United States are a good example.

Third, we need a revolution in K–12 education and lifelong worker training focusing on technology and the use of the Net. Advanced teacher training would be a good place to start, followed by community school networks, allowing teachers, parents, students, and administrators to communicate easily. All school districts shall have in place broad technology plans, involving not only Internet access for students and teachers but also integrating the Net totally into curricula and operations. Similarly, the application of the Net to lifelong education will call for cooperation by industry, labor unions, and government agencies, including the military.

## **Conclusions**

The United States arrives in the era of the Net and the virtual state with an enormous advantage: the values and political traditions that were written into the Consti-

tution by the Founding Fathers and strengthened over the course of the Nation's history. Among the ones that are key to building the global information infrastructure are freedom of speech and expression; respect for the private sector and markets, as opposed to government ownership and control; meritocracy and respect for education and the work ethic, as opposed to hierarchical social strata that perpetuate ignorance; and a love for change and a desire to challenge the status quo, as opposed to living under the tyranny of history and tradition.

The United States has all the right ingredients in place to increase its lead in building the Net and electronic commerce. The challenge will be to open society further to new ideas, people, and technology, as well as to physical goods and investment. In an era when globalization and the novelty of the Net are upsetting to people such as those who protested the World Trade Organization in Seattle and the World Bank in Washington, the United States must resist the temptation to turn back to protectionism, nativism, and opposition to the free expression of ideas.

The Net will not usher in a utopia, however. Citizens in countries such as those in sub-Saharan Africa, where the spread of infectious diseases such as HIV/AIDS alone threatens the total breakdown of civil society, will not be touched by the Net, except in the most remote ways. Nor will the Net erase centuries of hatred, intolerance, and aggression. The United States and its military forces will still have to deal with hostile nations and other threats, some of which may be strengthened temporarily by the new technologies. On the other hand, China and other such nondemocratic countries arrive at this era with enormous handicaps. The weight of its chaotic history hangs heavy over China, and the government's fear of individual freedom is so strong that it continues to adopt policies that so restrict individuals and the private sector that the creation of an effective information society becomes impossible. Two paths are open to China and other totalitarian and authoritarian countries: reform, become more open and democratic, and take great strides forward in advancing their economies and national power; or resist change, fall further behind in the new virtual democratic world, and become less powerful relative to the democracies.

The United States will remain more powerful for the foreseeable future in either event, but let us hope that China and other countries like it choose the path of openness and democratization. Such a development would mean much more than 1.5 billion customers for American high-technology industry. It would mean a more peaceful and prosperous world for everyone. 🌐

## Notes

<sup>1</sup> For an excellent and nontechnical discussion of the components of the Net, or global information infrastructure, see the Web site of the Computer Systems Policy Project (CSPP) at <<http://www.cspp.org>> for a series of papers. CSPP work had a major impact on the Clinton administration's approach to the issue.

<sup>2</sup> Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York: Simon and Schuster, 1996), 88.

<sup>3</sup> Seymour Martin Lipset, "Still the Exceptional Nation?" *The Wilson Quarterly* (Winter 2000), 31.

<sup>4</sup> Alan Greenspan, speech to Federal Reserve Bank of Chicago, May 1999.

<sup>5</sup> Roger C. Molander, Andrew S. Riddile, and Peter A. Wilson, *Strategic Information Warfare: A New Face of War* (Santa Monica, CA: RAND Corporation, 1996), xiii.

<sup>6</sup> U.S. Department of Commerce, *The Emerging Digital Economy* (Washington, DC: Department of Commerce, June 1998).

<sup>7</sup> Nua Internet Surveys, <<http://www.nua.ie/surveys>>. Nua, an Internet survey firm, offers on its Web site a wealth of global Internet usage information.

<sup>8</sup> U.S. Department of Commerce, *The Emerging Digital Economy II* (Washington, DC: Department of Commerce, June 1999).

<sup>9</sup> Forrester Research, Inc., as reported in *Business Week*, June 22, 1998.

<sup>10</sup> U.S. Department of Commerce, *The Emerging Digital Economy II*, 5.

<sup>11</sup> *Ibid.*, 38.

<sup>12</sup> William J. Clinton, "Electronic Government," memorandum to the Heads of Executive Departments and Agencies, The White House, December 17, 1999.

<sup>13</sup> "Campaigners Are Cautious on Economy," *The Wall Street Journal*, January 17, 2000, A8.

<sup>14</sup> President's Information Technology Advisory Committee, report (Washington, DC: Government Printing Office, February 1999). Interestingly, the Republicans not only agreed with the report but also tried to outdo the administration in June 1999 when Congressman Sensenbrenner (R-WI) introduced his own larger increases in spending.

<sup>15</sup> The White House, *A Framework for Global Electronic Commerce* (Washington, DC: Government Printing Office, July 3, 1997).

<sup>16</sup> Government of Canada, Convergence Policy Statement (Ottawa: August 6, 1996).

<sup>17</sup> Industry Canada, *Preparing Canada for a Digital World: Final Report of the Information Highway Advisory Council* (Ottawa: October 8, 1997).

<sup>18</sup> Ministry of International Trade and Industry, Government of Japan, *Toward the Age of the Digital Economy: For Rapid Progress in the Japanese Economy and World Economic Growth in the 21st Century* (Tokyo: May 1997).

<sup>19</sup> Ministry of Information and Communications, Government of Korea, *Cyber Korea 21: Korea's Vision for a Knowledge-Based Information Society* (March 1999).

<sup>20</sup> National Information Technology Council, Government of the Philippines, *IT21 Philippines: Action Agenda for the 21st Century* (October 1997).

<sup>21</sup> Mahatir Mohamed, Prime Minister's Office, Government of Malaysia, *The Way Forward—Vision 2020* (Kuala Lumpur: 1996).

<sup>22</sup> National Computer Board, Government of Singapore, *IT 2000—A Vision of an Intelligent Island* (1992).

<sup>23</sup> For an excellent (but now dated) study of China's bifurcated policy, see John H. Taylor III, "The Internet in China: Embarking on the Information Superhighway with One Hand on the Wheel and the Other Hand on the Plug," *Dickinson Journal of International Law* 15, no. 3 (Spring 1997).

<sup>24</sup> David C. Gompert, *Right Makes Might: Freedom and Power in the Information Age*, McNair Paper 59 (Washington, DC: National Defense University Press, May 1998), 37.

<sup>25</sup> Ajay Shah and Shuvam Misra, "Designing India's National Information Infrastructure," *Economic and Political Weekly* (November 8, 1997), 2880.

<sup>26</sup> A European Initiative in Electronic Commerce, communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, Brussels, April 12, 1997.

<sup>27</sup> Lionel Jospin, "Preparing France's Entry into the Information Society," speech at Hourtin University of Communications, August 25, 1997.

- <sup>28</sup> Department of Trade and Industry, Government of the United Kingdom, *Moving into the Information Society: An International Benchmarking Study* (London: Department of Trade and Industry, July 1997).
- <sup>29</sup> Prime Minister's Office, Government of France, *Preparing France's Entry into the Society: Government Action Programme* (Paris: January 16, 1998).
- <sup>30</sup> Erkki Ormala, remarks at The Digital Economy in International Perspective Conference, Willard Hotel, Washington, DC, May 27, 1999.
- <sup>31</sup> Ministry of Finance, Government of Finland, *Finland Toward the Information Society—A National Strategy* (January 18, 1995).
- <sup>32</sup> Economic Commission for Africa, United Nations, *Building Africa's Information Highway: Africa's Information Society Initiative* (Addis Ababa: March 16, 1996).
- <sup>33</sup> Nua Internet Surveys, <[www.nua.ie/survey/?+=VS&art\\_id](http://www.nua.ie/survey/?+=VS&art_id)>.
- <sup>34</sup> John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND Corporation, 1997), 303.
- <sup>35</sup> For a complete discussion of the threats from these sources, see Robert T. Marsh, *Report of the President's Commission on Critical Infrastructure Protection* (Washington, DC: Government Printing Office, October 13, 1997). See also President's Working Group on Unlawful Conduct on the Internet, *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet*, March 2000, <[www.usdoj.gov/criminal/cybercrime/unlawful](http://www.usdoj.gov/criminal/cybercrime/unlawful)>.
- <sup>36</sup> Dorothy E. Denning, *Information Warfare and Security* (New York: Addison-Wesley, 1999), 17. Denning's book provides complete coverage of this subject.
- <sup>37</sup> Matt Forney, "China to Issue New Rule on Software for Foreign Firms: Government's Move Could Slow Internet Growth," *The Wall Street Journal*, January 25, 2000, A10–A13.
- <sup>38</sup> Garry Rodan, "The Internet and Political Control in Singapore," *Political Science Quarterly* (Spring 1998), 65.
- <sup>39</sup> Daniel Bell, *The Coming of Post-Industrial Society* (New York: Basic Books, 1973).
- <sup>40</sup> Brian Nichiporuk and Carl F. Builder, "Societal Implications," in *In Athena's Camp: Preparing for Conflict in the Information Age*, 296.
- <sup>41</sup> Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), 207.
- <sup>42</sup> Computer Systems Policy Project, *Freedom to Grow* (Washington, DC: n.p., 1998).
- <sup>43</sup> An *MTOP* is millions of theoretical operations per second, a measurement used only by the government to give it some standard benchmark for judging what is a supercomputer.
- <sup>44</sup> Dan Hoydysh, testimony before the House Armed Services Committee, October 28, 1999.
- <sup>45</sup> The Gartner Group report on U.S. and foreign high-performance computer industries, published in 1999 by Gartner, a high-technology consulting firm in Stamford, Connecticut, shows vividly the worldwide spread of the computing technologies underlying the current performance of the Net, as well as its future direction. It highlights the impossibility of the government's keeping pace with developments in its attempts to control exports.
- <sup>46</sup> Office of the Under Secretary of Defense for Acquisition and Technology, *Final Report of the Defense Science Board Task Force on Globalization and Security* (Washington, DC: Government Printing Office, December 1999), vii.
- <sup>47</sup> Steve Lohr, "Welcome to the Internet, the First Global Colony," *The New York Times*, January 9, 2000, section 4, 1.
- <sup>48</sup> William Drozdiak, "Europe Can't Match U.S. Techno-Boom," *The Washington Post*, January 15, 2000, A1.

<sup>49</sup> David Rothkopf, "Cyberpolitik: The Changing Nature of Power in the Information Age," *Journal of International Affairs* 51, no. 2 (Spring 1998), 358.

<sup>50</sup> Gompert, *Right Makes Might*, 6.

<sup>51</sup> Richard Perle, address on export controls at the American Enterprise Institute, December 1, 1999, <<http://www.ccre.net>>.

<sup>52</sup> For a fuller discussion of the Defense Science Board proposals for modernizing export controls and technology transfer, see Office of the Under Secretary of Defense for Acquisitions and Technology, *Final Report*, 55–67.

<sup>53</sup> Electronic Commerce Steering Group, Auckland, *APEC Electronic Commerce: Readiness Assessment Tool* (June 1999).

<sup>54</sup> Center for International Development, *Readiness for the Networked World: A Guide for Developing Countries* (Cambridge, MA: Harvard University Press, 1999).

<sup>55</sup> Rudy Baca, *The Building Blocks of Growth in the "New Economy"* (Legg Mason Precursor Group, Spring 2000), 29.

<sup>56</sup> Office of the Under Secretary of Defense for Acquisitions and Technology, *Final Report*, 44–46, 83–93.