Sovereignty and the Role of Government in Cyberspace

James A. Lewis
Senior Fellow
Center for Strategic and International Studies

“The first principle is that this will be an environment or a world where private actors lead, not governments.” - Ira Magaziner, May 1998

One of the central elements of thinking about internet policy was that the role of government in this new domain should be minimal, both because this was the best thing to do and because many obstacles prevent national governments from extending sovereign control into cyberspace. This belief had profound and ultimately damaging implications for security. A reexamination of these beliefs suggests that they are best seen as a product of their time rather than immutable characteristics of cyberspace. Ideology, culture, and business practices help explain the initial understanding of cyberspace and government’s role in it.

Many of the assertions produced to support a limited role for government do not hold up to scrutiny. The belief that the internet had initiated a period of rapid, fundamental economic change was taken as implying that “the digital economy moves too quickly and requires too much flexibility for the processes of government to be, in most cases, successful in relating to it.” This conflates evolving business models with fundamental change. The argument that technology evolves too rapidly to be regulated is true only if we lack perspective. The flood of new applications and devices can appear bewildering and overwhelming, but the speed of technological change has been overstated. There have been four technological epochs in the last forty years: the mainframe era, the advent of the PC, the internet, and now a move into mobile and what is often called “cloud computing.” This is a rapid rate of change when compared...
to earlier technologies, but it is not blinding or impossible to describe and manage.

Similarly, the concept of cyberspace being a global commons due to its supposed lack of borders is best seen as a wish rather than a description. This concept undercuts both national and international security and is increasingly unsustainable as other governments seek technological and policy solutions to extend their control in cyberspace. The culture of the net pioneers, combined with a larger U.S. preference for limited government and a reliance on markets, helps to explain both the rejection of sovereignty and the approach taken by the U.S. government to cybersecurity. But the policies that grew from this wish now face challenges in the new conditions of the twenty-first century, in which the internet is no longer a U.S. artifact, but rather an arena in which states contend.

The concept of cyberspace being a global commons due to its supposed lack of borders is best seen as a wish rather than a description.

The internet began as a U.S. government enterprise, created for defense and research purposes. The steps taken by the Federal Government in the early 1990s in opening this government-controlled network of networks to private activity profoundly affected internet governance. The U.S. government opened the internet to the public in a period of substantial political change, shaped by the triumph of market economies during the cold war and reinforced by the trend in many industrialized nations towards deregulation, particularly in telecommunications.2 The policy decisions made in this larger political context were reinforced by the general anti-authoritarian, non-hierarchical and anti-government beliefs held by many internet pioneers. The result was a conscious decision in the United States to minimize government role, as “private-sector action is preferable to government control.”3

The growth of the internet also coincided with (and was intimately involved in) the growth of a global economy. National borders became less relevant (and national policies less effective) in this new economic environment. The erosion of sovereignty and the possible demise of the Westphalian state system brought on by globalization strongly affected views on internet governance held by policy makers, technophiles, and the internet community.

The decision by the U.S. government to turn over most governance functions to the private sector were also shaped by the assumptions of the dot-com era, when internet pioneers proclaimed repetitively that the internet and the World Wide Web were new phenomena; old rules did not apply because it is untrammeled, borderless, and without need for traditional government.4 Such pronouncements affected policy makers in many countries, who feared that government intrusion would damage adoption of the new technology and condemn them to a secondary economic status.
Sovereignty and the Role of Government in Cyberspace

The debate in the United States and in its European allies over the control of encryption products reinforced the emphasis on private sector leadership. Other industrial nations mirrored U.S. efforts to impose a single encryption technology and to create a national regulatory scheme for the use of encryption, which led to technological dead-ends and won little public support. The effort to mandate use of the clipper chip was (and remains) a powerful argument for minimizing the government’s role in prescribing technological solutions.

The conceptual gap between internet security and commercialization in U.S. policy-making was so large that the Clinton White House set up two separate working groups: one on security led by John Deutsche, the Director of Central Intelligence and one on commercialization led by Ira Magaziner, Clinton’s advisor on health care. Coordination between the two groups was often patchy and at times was marked by a degree of hostility and competition.

Assertions about sovereignty and the role of government in cyberspace have taken on new importance in recent years. Some reflect a growing awareness of threats and vulnerabilities, but most of it stems from the realization that the internet has become a vital component of economic activity and national security. This dependence has brought growth and greater efficiency in business, research and government.

The United States has woven computer networks into so many of its economic activities and military operations, perhaps becoming more reliant on the Internet than any other nation. Networks reinforced existing trends of military thought on the importance of intangible factors—greater knowledge, faster decision-making, and increased certainty—that would increase combat effectiveness. Leaving its organization of the internet to voluntary efforts may have been tolerable when it was still a gadget or a toy, but not for something that has become an essential global infrastructure.

The internet was not designed to be a global infrastructure upon which hundreds of millions of people would depend. It was never designed to be secure. Like other past innovations—airplanes, cars, and steam engines—the appeal and the benefits are so great that we have rushed to adopt the internet despite serious safety problems. The global connectivity of the new infrastructure amplifies these problems, as the speed of internet connections means that geographical distance provides little in the way of protection. For earlier technologies, safety came about through innovation driven by government mandates, and by agreements among states. The same process of maturation is necessary to secure cyberspace, but this will require shedding some of our old ideas about its nature. There is a reluctance to acknowledge the ideological blinders that shape our views on the nature of the internet, the role of government, and the limits of sovereignty. The early architects and thinkers of cyberspace in the first flush of commercialization downplayed the role of government. Their vision was that cyberspace would be a
global commons led and shaped by private action, where a self-organizing community could invent and create. This ideology of a self-organizing global commons has shaped internet architecture and policy, but we must now recognize its inadequacy.\(^\text{10}\)

There are two reasons for this inadequacy. First, sophisticated intelligence and military services will overwhelm private efforts to secure networks. Cybercriminals, sometimes supported by their national governments, may have similar advantages. The private sector does not have the capability to defeat the intelligence and military services of an advanced opponent like Russia or China (and other nations would add the United States and the United Kingdom), organizations that invest hundreds of millions of dollars and employ thousands of people to defeat any security measure. Just as we do not expect airlines to defend our airspace against MiGs, we should not expect private companies to defend cyberspace against foreign governments.

Second, in the absence of government intervention, adequate security will not be provided.\(^\text{11}\) Cybersecurity is a public good, goods are those that benefit all of society but whose returns are difficult for any individual to capture. The private sector does not adequately fund public goods because returns to the individual investor may be inadequate, even though the returns to society are great; we can add cybersecurity to this list of public goods. The combination of unplanned global access, porous technologies, and weak governance makes this newly critical infrastructure exceptionally vulnerable. As the United States’s reliance on the internet increases, so does its vulnerability to remote exploitations and attacks. That the technologies designed in the early 1970s have worked so well and have so cleanly scaled to support more than a billion users is an amazing triumph, but at the price that anyone with malicious intent can easily exploit these networks.

Beliefs shape actions and understanding. For the internet, these beliefs were a mixture of libertarianism, anti-authoritarianism, and belief in a New Economy, strongly supported by business interests who sought to limit regulation and liability.\(^\text{12}\) The resulting “architecture” for cyberspace reflects these beliefs and is now under challenge. Perhaps more importantly, they limit our ability to define both problems and solutions. An approach to governance constructed on this foundation was not inevitable, but a matter of choice. Those choices, made largely by U.S. citizens, can be undone, especially as other nations gain influence in shaping cyberspace.
“Personal computers and the PC industry were created by young iconoclasts who had seen the LSD revolution fizzle, the political revolution fail. Computers for the people was the latest battle in the same campaign.” – Howard Rheingold

An uptake of new network technologies made great advances in numbers and in geographic spread in the 1990s. The culture that shaped this uptake was largely American; a blend of science and engineering cultures with a strong dose of West Coast libertarianism contributed to this culture. While this image and mindset is appealing, it is also fading. The modern internet architecture, standards, and protocols originate from the United States and date back to the 1990s. As manufacturing spreads to other countries with political objectives that are less dominated by free market doctrine, the ability of U.S. citizens to “build in” their beliefs into the technology is diminished. Other states often also are less retrained about government intervention and industrial policy, as they see the risk of an unregulated infrastructure as unacceptable.

The designers and theorists of the internet built the network to reflect their values: the internet was open and non-hierarchical, as well as somewhat antiauthoritarian and anti-government. Theorists such as Kevin Kelly, Howard Rheingold, and John Perry Barlow saw the new digital network technology as enabling a new kind of community and a new approach to make organization flat, non-hierarchical and collective. Their conclusions pointed to replacing some sphere of government with a self-organizing community.

As Steven Levy described, “the engineers and programmers who loved computers and had become politicized during the anti-war movement were thinking of combining the two activities.” Their ideas were influential and, to a degree, shared by officials in the Clinton administration responsible for commercializing the internet. Given the central role of the United States in the 1990s in shaping cyberspace, these ideas helped determine the future path of internet governance. The outcome was a conscious decision by the United States to minimize government’s role, as “private-sector action is preferable to government control.”

Certainly, in some instances, such as the Internet Engineering Task Force (IETF) or the Open Source Software Movement, this vision of an open, nonhierarchical community has worked exceptionally well. This open, non-governmental approach likely accelerated creativity and the adoption of the technology, but the amorphous and, at times, anonymous global collective of millions of individuals has overwhelmed the capacity for self-governance.

The anti-authoritarian aspects of internet culture were strengthened by the con-
cept of a New Economy, which seemed to reinforce the point that old structures were inappropriate for cyberspace. In the New Economy, old economic rules seemed to no longer apply as economic activity in the 1990s transitioned, supposedly, to an economy based on the exchange of ideas and information. A commonly held view in Silicon Valley was that Washington was largely irrelevant to this new world.

The strength and influence of these ideas in shaping internet governance rests on linkages among the beliefs and perceptions held by internet pioneers. These linkages have not yet been fully explored. The beliefs held by the individuals who made internet policy were based on their political experiences in previous decades. In this case, the original governance bodies of the internet, such as the IETF, were formed along the lines of self-organizing communities or non-governmental entities, such as the Internet Corporation for Assigned Names and Numbers (ICANN) in accordance with the “New Economy” mindset.

Additionally, some of the crucial figures establishing the governance framework for cyberspace were themselves college radicals or were closely linked to politics of the 1960s. One of the most important of these was Ira Magaziner. Magaziner directed the Clinton administration’s planning to commercialize the internet, and was himself once a college activist. Magaziner’s views are complex and nuanced, but his preference was for a “market driven approach . . . [that] was a bottoms up kind of medium that should not be over-regulated.” As he put it, “I think a model of industry self-regulation and of industry codes of conduct and decentralized governance fits better for the Internet age...That is part of the new model that we think will govern in the digital age.”

**Voluntary Regulation and Self-Governance**

“The Federal Government should recognize the unique qualities of the Internet including its decentralized nature and its tradition of bottom-up governance. Existing laws and regulations that may hinder electronic commerce should be revised or eliminated consistent with the unique nature of the Internet.” -White House Memorandum on Electronic Commerce, July 1997

The commercialization of the Internet came to a head during the high tide of deregulation. The experience of central governments in using Keynesian tools to manage their economies led to the recognition that control ran counter to economic growth. Regulated industries were often inefficient in their use of resources and in their delivery of goods and services. The long cycle of deregulation in the telecommunications industry was particularly important in shaping the views of internet pioneers. Deregulated telecom companies performed better than government owned firms, and it is not surprising
that this conclusion should have carried over to the Internet. Telecom deregulation, however, was an inadequate model for the Internet, as it was concerned with ownership and the introduction of market forces into the supply of telecom services within a larger regulatory context that sought to ensure security and quality of service.

Voluntary self-regulation has strong roots in U.S. political culture. As the United States evolved into an urban, industrial society, reformers found the concept of highly trained professionals exercising stewardship over public policy and transforming public policy issues into scientific, technical and managerial problems more attractive than the dubious electoral politics of the 1900s. The approach emphasizes “engineering efficiency” over “inefficient” democracy and a dependence on private sector initiatives to meet public needs, on the grounds that small groups of experts, accountable to scientific principles rather than the broad public, are more likely to arrive at effective solutions. The center of this philosophy was Herbert Hoover’s Commerce Department, and there is some irony that 70 years later, it was the department he founded to encourage efficiency and private-led expertise that promoted the self-governance policies that shaped the commercial internet in its inception.

Three general principles for internet policy emerged from this culture. First, policy should be technology-neutral. Second, development of policy was to be industry-led, as part of a public private partnership where government’s role would be to provide a minimal, predictable legal and regulatory environment. Finally, policy solutions would need to work in a global marketplace. These principles remain broadly attractive, but in retrospect, it appears that the weakness of the policy process that led to self-regulation lies in a failure to distinguish between those activities where self-regulation is best and those where it is inadequate, where the market will fail to provide the best outcome.

Dealing with market failure is politically challenging, as it involves deferring individual interests to the larger societal good. This political difficulty has been true since the earliest days of the republic. Steam engines, although notoriously unsafe, had to wait 40 years until a series of savage accidents costing hundreds of lives led Congress to impose safety regulations. Automobile safety rules took more than half a century and faced strong opposition from manufacturers. Air safety regulations appeared more than 20 years after the first flight. A foundational belief for the United States is that “intellect and practical science,” as an early Congressional report explaining why regulation was unnecessary for steamboats stated, will lead to improvement via some automatic and self-correcting market process, without government intervention. The decision of the United States to take a minimalist approach to regulating the internet had considerable influence on other nations. In part, this reflects U.S. diplomatic efforts in multilateral fora to win support for policies that emphasized private sector control. These efforts were reinforced by the rapid growth of the U.S. economy in the 1990s, which made
other countries consider whether they were sufficiently attuned to the “the powerful language of laissez-faire” and the economic benefits of information technology.\textsuperscript{23}

**SOVEREIGNTY AND THE ILLUSION OF THE COMMONS**

The Organization for Economic Co-operation and Development (OECD) defines global commons as natural assets outside national jurisdiction such as the oceans, outer space and the Antarctic.\textsuperscript{24} Cyberspace is not a commons. Sovereignty completely covers cyberspace, even if nations have not always chosen to assert sovereign control (and the reasons for this may be a combination of poorly conceived ideology and concerns over liability and regulation). This is because cyberspace is an artificial creation which rests on a tangible, physical construct. There is no moment when bits moving from one computer to another are not on a network that someone owns and that is physically located in a sovereign state. The exceptions might be undersea cables or satellite transmissions, but the action still takes place on an owned facility were the owner is subject to some country and its laws. We can show ownership at any moment. Sometimes this is forensically challenging, but there are ways to reduce the forensic challenge to be able to assign sovereign responsibility.

Most of the interconnected networks that form cyberspace were created for commercial purposes, such that actions in cyberspace take place in a context defined by commercial law and business contracts. Under these “peering” agreements, traffic is allowed to pass from nation to nation without inspection or authentication. Nations currently assert few rules over in-transit traffic, in part because sovereign control may last only a few milliseconds as one network relays traffic to the next.

This legal construct accommodates commerce, but it also enables covertness and reinforces deniability. Sovereignty in cyberspace is not ambiguous, but the perception that it is so allows us to evade thorny issues. Western nations, as those currently most vulnerable to cyber attacks and those most constrained by law, might gain more than they would lose by changing these rules to allow nations to close their networks to traffic designed for criminal or offensive purposes. Cyberspace is a “pseudo commons,” more like a condominium or a shopping mall. It is a shared global infrastructure. Governance of this infrastructure is both weak and fragmented, but sovereign authority exists, even if it is not usually asserted or enforced. This “passive sovereignty” depends on political decisions by governments not to assert control and instead to rely on commercial agreements that create strong interconnections to provide a governance structure, but this decision could be changed at any time.

However, as new technologies increase the scope for monitoring and intervention in the flow of traffic, and as nations question the “hands-off” approach originally
taken by the United States, passive sovereignty is evolving into a more active assertion of the rights of national governments to exert control. Countries are beginning to assert sovereign control over their national cyberspace. The next steps will be to deploy technologies to let them enforce control and to create multilateral governance structures to legitimize these actions.\textsuperscript{25}

\textbf{Reconsidering the Role of Government}

Cyberspace is increasingly Hobbesian, and the belief of the pioneers that a “social contract” would emerge naturally from the self-organizing internet community without the intervention of the state has proven to be either wrong or moving at a pace so slow that threatens security. Beliefs about the nature of cyberspace have downplayed the role of formal governance and governments. Changing this assumption is part of the long-term process to adjust to the new environment created by technological change.

This is not unusual; when new technologies come along, they are either unregulated or efforts are made to regulate them with the old, antiquated rules. As the technologies mature and governments gain experience with them, they are brought into the ambit of societal control. However, unlike the 1990s, when most internet technology and users came from the United States, this process of reconsideration may now be led by other nations. The United States increasingly shares ownership and control of the internet with other nations. The beliefs that shaped the internet are now being challenged and the set of beliefs that guided the U.S.-led commercialization of the internet conflicts with the goals of states that seek to control information and resist U.S. hegemony. Governments are also being driven to take a more active role due to the failure of the self-organizing model to provide adequate security.

Governments will establish sovereignty in cyberspace, but it is yet an open question as to whether this extension will be consistent with Western values or it will lead to a fragmented, less open internet. Other nations will extend government control in ways that may not be to our liking.\textsuperscript{26} A failure to move from the beliefs of the internet pioneers could put democratic values at risk. The benefit of worldwide use of a U.S. internet architecture is that it reflects Western political values, such as openness for ideas and discourse, which are not universally esteemed by all governments. As innovation and manufacturing shift from the U.S. to the Pacific and as the equipment upon which cyberspace rests is built in countries with very different political ideals, we could easily see this openness contract. The result could be a cyberspace that would be open for business, but not to ideas.

The reasons for this are not readily apparent, but those who set the standards, manufacture the hardware and write the code have a deep degree of control. While
we debate the size and nature of the global commons, other nations may seize the opportunity to “rearchitect” cyberspace to better serve their political and commercial needs. The U.S. ideology and culture that shaped cyberspace is now subject to subtle changes as manufacturing spreads to Asia and as Americans no longer constitute the largest number of internet users.

The struggles over the Domain Name System (DNS) and ICANN, the battles over technology standards, and the problems at the International Telecommunications Union (ITU) are all symptoms of this reorientation of internet governance to reflect the increasing influence of other nations. Cyberspace is being reshaped. National governments, with all their resources and power, have entered cyberspace and we cannot dismiss their efforts to reshape the domain for economic and political advantage. Perhaps the United States still has enough influence to put forward a new vision for cyberspace to make it more secure and yet still amenable to our political values. Doing this will require rethinking the role of government and recognizing the scope of sovereignty. All of this leads us to the antithesis of the original view of the role of government in cyberspace. In this new phase of administering and securing the internet, governments will lead, not private actors.

Notes


2. Telecom deregulation, however, is an inadequate model for the Internet, as it is concerned with ownership and the introduction of competition into the supply of telecom services.


4. The most famous example is Gilder’s Declaration of Independence.

5. A government designed encryption module that could be inserted into computers and other network devices that made data inaccessible to all but Federal authorities.

6. The author was a member of the security group.


10. Protocols, contracts and national laws that determine what actions form the architecture of cyberspace and what relationships are permissible.


14. Kevin Kelly (who went on to found Wired and who preceded Rheingold as an editor of the Whole Earth Catalogue), Out of Control: The New Biology of Machines, Social Systems, and the Economic World
Sovereignty and the Role of Government in Cyberspace

19. Magaziner's full quote: “[M]arket driven approach to the development of the internet. We felt that it was a bottoms up kind of medium that should not be over-regulated, and we felt that we wanted to preserve the organic nature of the internet, but to set in motion a series of predictable rules that would allow commerce to take place because commerce requires a certain amount of predictability. So we advocated creation of uniform commercial code to govern transactions, market oriented approach to digital signatures; we opposed censorship of the internet, felt that that should be free content on the internet, that you wanted to evolve the government's mechanism to one that would gain global acceptance but that would still be market-driven and not heavy regulation. We advocated not having taxes on the internet, getting agreement for internet commerce to be free of tariffs across borders, and also to avoid internet taxation. At that time there were proposals floating around to tax bits. We proposed leaving, not having the FCC or ITU regulate the internet the way they did telecom, to keep the packet-switch networks out of FCC regulation. We advocated a degree of protection of intellectual property that would allow copyrights and patents to be protected and a variety of other measures like that that set a framework.” *Internet Governance Raw Footage: Ira Magaziner, Carl Malamud*, (2006), http://www.archive.org/details/igover-nance_rawfootage_Ira_Magaziner.
21. Robert Kahn, one of the creators of the Internet (he led the DARPA project) said, for example: “There are many areas where we could have made a lot more progress if there had been an organized effort to create new types of infrastructure. Some of the most vigorous opposition actually comes from the private sector - not usually in terms of overt actions, but by just not wanting to see change happen in areas that would dramatically affect them.” http://www.gcn.com/Articles/2009/05/18/GCN-Interview-with-Robert-Kahn.aspx.
START A TRIAL SUBSCRIPTION TODAY—GET ONE FREE ISSUE

Provocative, lucid and engaging  |  Pioneering future debate

Undaunted and uncompromising  |  Critical analysis of government policy

The INDEPENDENT REVIEW
A Journal of Political Economy

For even greater savings, subscribe online and pay now to receive 2 free issues. That’s 6 issues for the price of 4.

www.twitter.com/IndependentInst
www.facebook.com/IndependentInstitute

www.independentreview.org • review@independent.org
100 Swan Way, Oakland, CA 94621-1428 • 800-927-8733 • 510-568-6040 (fax)