CHAPTER 21

Internet Governance

Harold Kwalwasser

INTERNET GOVERNANCE: the concept is a challenge to understand. No single body dominates collective decisionmaking about the Internet. No one type of decision process repeats itself in different venues. As a result, cyberpower— in the sense of having the power to influence collective decisionmaking about the Internet—is easy neither to exercise nor to describe.

Two predominant and related facts define this subject. First, governments exercise relatively little control over the Internet, even though it has a tremendous impact on society. Second, the key forums for Internet governance are evolving, not fixed. One of the impulses driving the forums' evolution is the tension between their legitimacy and the pressure by some governments to increase their roles; the pressure—and the likelihood that it will yield some success—will become greater if the current structures' legitimacy ever declines or disappears. Conversely, the pressure will diminish only if and when the structures' legitimacy becomes firmly and permanently established.

Internet governance is complex, with collective decisionmaking distributed among various organizations that have different structures. Few aspects of the Internet's operations are subject to typical government or even inter- governmental decisionmaking. Instead, in many of the key forums, particularly those related to the standards process that is fundamental to the Internet, private parties dominate and governments play only a subordinate role.

The structure of each of these organizations and the scope of its jurisdiction generally came about by a combination of short-term decisions and historical accident. Power, or the ability to influence particular policies, arises not from the sovereign might of states, but rather from the persistence of participants—entities and individuals—and their technical expertise, alliance-building among operators and users, and sheer financial capability to participate in multiple forums around the world.

Further complicating this picture is the fact that some of the most important organizations are new and their rules and working procedures are still evolving. The Internet Corporation for Assigned Names and Numbers (ICANN), which oversees the Domain Name System (DNS), was organized as a nonprofit corporation in 1998.[1] The original predecessor to the organization now known as the Internet Engineering Task Force (IETF), which resolves key standards for the operation of the core of the Internet, dates only from 1979.

Governments other than that of the United States have realized how little they can control what happens in and around the Internet. As it has grown into a powerful engine of economic growth and political speech, Internet issues have taken on a significance they did not have just a few years ago. What were once considered technical questions to be left to scientists and engineers have become matters of public policy that greatly interest large numbers of people who claim a stake in the decisions. It has been said that "'technical issues' become 'public policy' whenever voters think they should."[2] The Internet's great ability to foster globalized free market competition and free speech cuts across traditional geographic boundaries and challenges historic notions of national sovereignty. This transnational effect diminishes governments' control over the activities of their own people and their own economies, and some governments see this change as a challenge to their national sovereignty and domestic power.

Governmental control of the Internet is impeded, however, by the existing governance

structure, and therefore some governments have called for changes in that structure. Others, notably the United States, want the current system to remain largely in place, provided that they can deal with a limited number of pressing problems such as child pornography and cyber crime.

The main part of this chapter describes the components of Internet governance, what each governs, and how each is organized and governed internally. The first three sections describe the most prominent organizations involved in Internet governance. These organizations' agendas are significantly or exclusively focused on Internet-related questions. The first section describes ICANN and the management of the DNS. The second section addresses the IETF, the Internet Society, and the other bodies that it supports, and offers a brief review of the independent World Wide Web Consortium that oversees the Web. The third section examines the International Telecommunication Union (ITU), a specialized agency of the United Nations (UN) that predates the Internet but whose decisions particularly affect the telecommunications companies that carry Internet traffic.

The next three sections describe institutions whose focus is broader than the Internet but that nonetheless play significant roles in Internet-related decisionmaking. Because they have generally been established longer, they are less subject to issues of legitimacy and the kind of evolutionary pressure described above. The fourth section describes the role of international entities such as the Organization for Economic Co-operation and Development (OECD), the UN (other than the ITU), and the Council of Europe. The fifth section looks at the role of national governments, particularly the U.S. Government. The sixth section briefly describes other international standards-setting bodies whose decisions may affect the Internet, including the Institute of Electrical and Electronics Engineers, the International Electrotechnical Commission, and the International Organization for Standardization.

Table 21–1 summarizes the organizations and their subject matter concerns.

The Internet Corporation for Assigned Names and Numbers

For a variety of reasons, many people see ICANN as the governance body for the Internet, but this view is a misperception. ICANN oversees the DNS and operates the Internet Assigned Numbers Authority (IANA). These are important Internet-related functions, but other institutions are just as vital to other equally significant decisionmaking. Nonetheless, ICANN has been the center of the international political debate about Internet governance, most likely because of the existence of three agreements with the U.S. Government that affect its operations. ICANN is, therefore, an appropriate place to begin.

ICANN coordinates the allocation and assignment of three sets of unique identifiers for the Internet: domain names, Internet Protocol (IP) addresses, and protocol port and parameter numbers.[3] ICANN also "coordinates the operation and evolution of the DNS root name server system; [and] coordinates policy development . . . related to these technical functions."[4]

The DNS is the addressing function of the Internet, translating a typical uniform resource locator, such as <www.aol.com> or <www.ndu.edu>, into the unique numeric IP address that is actually used to route messages. "Each domain name is made up of a series of character strings (called 'labels') separated by dots. The right-most label in a domain name is referred to as its 'top-level domain' (TLD),"[5] such as *.org* or *.com*. "Most TLDs with three or more characters are referred to as 'generic' TLDs, or 'gTLDs,"; these also include *.edu*, *.int*, *.mil*, *.net*, and *.org*.[6] TLDs also include country-code TLDs (ccTLDs); these generally have two letters, such as *.uk* for the United Kingdom or *.cn* for China.[7] ICANN has the right to

authorize new gTLDs and ccTLDs and to review changes to the domains' registries, which operate them.

Table 12-1 Internet Governance Organizations

Organization	Subject Matter
Internet Corporation for Assigned Names and Numbers, which includes functions referred to as the Internet Assigned Numbers Authority	Supervises the Domain Name System, allocates Internet protocol address space, and oversees the root zone servers that provide basic finding information for Internet traffic
Internet Society and related organizations: Internet Engineering Task Force, Internet Engineering Steering Group, and Internet Architecture Board	Develops standards for operation of Internet and its overall architecture
World Wide Web Consortium	Develops standards for the World Wide Web
International Telecommunication Union	Develops standards for telecommunications, including interface of Internet and telecommunications systems
Organization for Economic Co-operation and Development, European Union, Council of Europe, United Nations agencies	Ad hoc policy development on issues of critical interest to members
National governments acting individually or through joint agreements	Ad hoc policy development chiefly related to cyber crime, use, and commercial regulatory issues
Institute of Electrical and Electronics Engineers, International Electrotechnical Commission, International Organization for Standardization	Standards for products and for manufacturing and testing processes (operations of these entities relate only peripherally to the operation of the Internet itself)

The Internet Assigned Numbers Authority was originally created by the Defense Information Systems Agency (DISA) in the early days of the Internet to assign addresses to Internet users, meaning that it significantly predates ICANN. Much of that work has now devolved elsewhere, but IANA still deals with the policy-related functions of TLD and address block management. Its most prominent function—and its most politically charged one—is to make changes to the master root zone file.[8] The Internet Architecture Board also designated IANA to carry out the technical registration functions associated with IETF protocol parameters and other technical assignments. Currently, "the IANA function," which ICANN performs under a no-cost contract with the U.S. Department of Commerce (DOC), represents primarily administrative or book- keeping functions. The three most important of these are coordination of the assignment of technical protocol parameters; administrative functions associated with root management; and allocation of IP address blocks.[9]

ICANN and IANA issues

The kinds of questions ICANN addresses provide a sense of what is at stake,

particularly the implications for the security and stability of the Internet itself.

One current issue is that of Domain Name System Security Extensions (DNSSec), a suite of IETF specifications for securing certain kinds of DNS information on IP networks. DNSSec is a set of extensions to DNS that provide for origin authentication and data integrity. When one types in an Internet address, one has to have faith that the message is going to the intended recipient or Web site and that the message received is actually from the person or organization identified as the sender. False addresses, improper routing instructions, or other disruption of Internet addressing and routing would undermine the faith of users in the accuracy of the system. The system faces significant threats from people with the capability to disrupt this process. Individual operators can apply DNSSec tools within their own systems, but promoting and coordinating the process of adoption of DNSSec over the entire system needs a central focus.

Another prominent ICANN issue is internationalized domain names. The DNS utilizes American Standard Code for Information Exchange, which relies on the Latin alphabet. If one reads only Chinese or Hindi or Arabic, using the Internet can be a challenge. If the Internet and the DNS are to be truly universal, other scripts must be incorporated into the DNS. Research and development is not complete, and the policy issues are nettlesome; for example, which of India's multiple scripts should the Internet use? If internationalized domain names are not successfully implemented, it could lead to the balkanization of the Internet and limit its universality.

A third issue involves information about IP address holders. The so-called WHOIS database is a publicly available source about those who hold IP addresses, designed to offer a means to find out who is accountable for each one. However, the WHOIS database has been challenged by privacy advocates. The resolution of these two goals must balance the interests of law enforcement and others who want the identifying information to be available against assertions of privacy rights in the information.

The list of issues is much longer, including the adoption of a new addressing scheme, Internet Protocol version 6 (IPv6), and the creation of new gTLDs. Even without further elaboration, the point is clear: numerous significant issues are decided at ICANN.

ICANN Governance Structure

Prior to the formation of ICANN, the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation were responsible for managing critical parts of the Internet. By the mid 1990s, much of the operational responsibility had been contracted out to the University of Southern California's Information Sciences Institute. However, the U.S. Government wished to stop overseeing the growing commercialization of the Internet DNS, especially the burden of deciding when to authorize new TLDs during the "dot-com" boom or resolving disputes around "cyber-squatting" and other trade name and copyright problems. In a 1997 document called "Framework for Global Electronic Commerce," President Bill Clinton directed the DOC to privatize the DNS in a manner that would increase competition and facilitate international participation in its management.

The resulting Internet community discussions of management of the DNS considered both a private sector–lead model and an international treaty–based organization. The DOC proposed a transition to private sector management and sought public comment. However, the private sector model provoked considerable concern among foreign governments and others who were uncomfortable with the idea of an oversight function that was not controlled by a

governmental or intergovernmental entity. Nevertheless, in 1998, DOC called for transition to independent, private sector management, based on a new private sector entity, ICANN.[10] The Department of Commerce Memorandum of Understanding (MOU) with ICANN called for ICANN to develop a management scheme that reflected the principles of "stability," "competition," "private control," "bottom-up coordination," and "representation." The transition process would be overseen by the Department of Commerce.[11] The original 1998 agreement ran until 2000 but has been repeatedly extended; it is now called the Joint Project Agreement (JPA).

The issues related to trade name and copyright infringement, such as cyber- squatting, became a joint project of ICANN and the World Intellectual Property Organization. The latter organization eventually developed the Uniform Dispute Resolution Procedure, an alternative to traditional litigation that has been generally successful in handling these problems.

U.S. Government Contracts for DNS

There are now three major U.S. Government agreements with regard to Internet DNS: the DOC agreement with ICANN (the MOU/JPA), a procurement contract for IANA functions between DOC and ICANN, and a cooperative agreement with VeriSign, a publicly held corporation, which provides for maintaining and administering the root zone file, among other things.

The MOU/JPA with ICANN provides the framework of the transition to private sector management of the DNS.[12] It does not, however, give DOC any authority over ICANN's policymaking process.[13] Commerce's role is limited to oversight of development of the management and policy process.[14] The MOU/JPA contemplates that DOC will cease to have an oversight role once there is a stable governance arrangement that meets the goals stated in the MOU/JPA. As of 2007, DOC oversight of ICANN continued; even though the agreement has been extended and modified several times, the DOC role has not yet changed. At the time of the most recent extension in 2006, the administrator of DOC's National Telecommunication and Information Administration (NTIA), which administers the agreement, stated that the U.S. Government remained committed to an "independent" ICANN and suggested that it might allow the MOU/JPA to expire at the end of the current contract period in 2009.[15]

Another way in which the U.S. Government is involved with ICANN is through a procurement contract between DOC and ICANN for management of the IANA functions, such as assigning IP address space and processing requests for delegation and redelegation of management of TLDs.[16] After ICANN processes any proposed change to the root zone file, DOC must approve it before it is entered. A private company, VeriSign, then enters the change in the authoritative root zone file, which it maintains on a master root zone server, pursuant to a third U.S. Government agreement described below.

DOC reportedly intends to continue to contract for IANA services into the future (although leaving open the question of who might be its contracting partner), thereby maintaining U.S. Government oversight of changes to the master root zone file.[17]

Although DOC has generally not interfered with root zone changes, in 2005 the U.S. Government had to decide whether to concur in ICANN's tentative approval of a change in the root zone in order to create a new gTLD, *.xxx*, which would have hosted adult sites.[18] Rather than veto the proposed change itself, however, the Government and conservative interest groups worked successfully to have ICANN reverse its decision. The ICANN Board rejected *.xxx* in

May 2006[19] and again in March 2007.[20] The episode was proof to critics that the United States had excessive leverage over the ICANN process. However, there are no reported cases of actual DOC rejection of proposed changes, and critics generally complain about potential rather than actual abuse of power.

Under a cooperative agreement with Commerce, VeriSign (formerly Network Solutions, Inc. [NSI]) maintains and updates the authoritative root zone file.[21] When this cooperative agreement was initially executed in 1992, it included management of the *.com*, *.net*, *.org*, *.edu*, *.gov*, and *.us* domain names, giving the company a virtual monopoly in registry services. Upon the creation of ICANN, the cooperative agreement was revised.[22] VeriSign was required to separate its registry and registrar businesses, give up several of its registries, and enter into agreements with ICANN for management of its remaining registries.[23] DOC retained the right to review and approve any *.com* registry agreement between ICANN and VeriSign because of concerns over the importance of *.com* to the Internet and monopoly pricing due to *.com*'s extraordinary size and impact.[24] DOC also continues its oversight regarding any changes in the authoritative root zone file: "While NSI [now VeriSign] continues to operate the root zone server, it shall request written direction from an authorized U.S. government official before making or rejecting any modifications, additions or deletions to the root zone file."[25] The U.S. Government's agreement with VeriSign is expressly acknowledged in the provisions of the ICANN MOU/JPA and its amendments, which affords the Government a role in overseeing this particular TLD, *.com*, that it does not have with regard to any other private registry.[26] The agreement with VeriSign runs through 2012 and may be further renewed.

ICANN Internal Governance

The ICANN Board of Directors, with 15 voting members, is at the pinnacle of the organization's structure, which has now grown large and complex. ICANN has incorporated the Regional Internet Registries (RIRs), some of which existed prior to ICANN. The RIRs are essentially regional groupings of IP users, as well as others, that administer much of the system, particularly allocations of blocks of IP addresses. In many respects, they function independently of ICANN, as they did before ICANN's creation, but they have agreements with ICANN and must seek the board's approval for common policies. The RIRs, ccTLDs, and gTLDs have been organized into supporting organizations. Each of these three organizations selects two members of the Board. ICANN has also sought to provide a forum for a broader group of those involved with the Internet, such as Internet service providers, commercial and noncommercial users, and intellectual property interests. All participate with the gTLDs' registrars and registries in the Generic Number Support Organization (GNSO). An at-large advisory committee, which meets monthly, provides a way for individual users to participate. As of the fall of 2007, three board members were American.[27]

Governments have no direct voting role in ICANN. A governmental advisory committee (GAC), which advises the board, is open to any national government. The GAC has the right to advise the board on the public policy aspects of any decisions it considers. ICANN's bylaws require the board to explain any decision it takes contrary to the GAC's advice. Until recently, participation in the GAC was sparse and its influence weak. However, after calls for a new ICANN governance structure were turned aside at the meeting of the World Summit on the Information Society in 2005, both ICANN and many of the world's leading governments promised to reinvigorate the GAC process.[28] The GAC nominates a nonvoting member of the

board nominating committee, and there is a nonvoting GAC liaison on the board itself.

ICANN has become a robust political forum. Three 4-day board meetings are held every year around the world. Board committees and supporting and advisory organizations meet and also conduct work by email.

The ICANN structure represents an audacious attempt to incorporate the views of thousands of interested parties from around the world. The presumption underlying the MOU/JPA is that it can be done, but the evidence is thus far mixed. During the public comment period prior to the completion of the 2006 MOU/JPA between ICANN and the U.S. Department of Commerce, there was considerable criticism of ICANN for lack of transparency and accountability and other governance deficiencies (discussed further below).[29] As a result, the MOU/JPA pushed ICANN to do better on both fronts.

Who Has Power within ICANN?

Given this context, *power*—defined as the capacity to influence a particular decision or result—is difficult to quantify. For nations other than the United States, governments' power is constrained. Governments have no vote on ICANN's decisions. Their influence through the GAC has been weak. They may try to invigorate it, but that possibility remains an open question. Alternatively, they may be able to increase their influence by spending more time and effort participating in board committees or supporting organizations, although they would have no greater status than nongovernmental members. Whichever route they choose, their influence will have to come from the level of expertise and effort they put forward.

Governments can also attempt to exercise power or influence in two other ways. One is through the use of surrogates: the corporations, Internet providers, and registries that are active in ICANN affairs can, if they choose, carry the banner for governments' preferred policies. The practice has likely benefited the United States more than anyone else.

Local Internet societies[30] and ccTLD[31] registries may be more under the control of their respective national governments, and they may have less incentive than companies to act independently of their governments' interests in ICANN or other Internet governance forums. The United States has recognized the right of national governments to manage their own ccTLDs.[32] Over time, ccTLDs under control of their national governments may become, in essence, government representatives at ICANN.

A wedge between governments and their potential proxies or representatives is the effect of globalization. As companies become more citizens of the world than citizens of one country, it is more likely that narrow nationalist policies will be decreasingly consistent with companies' own goals. Governments may be less able to influence firms to support positions contrary to those goals.

Another way governments can exercise power is by threatening to create a separate DNS, essentially ignoring the ICANN regime. China has already exercised this option to some extent. By separating itself technically from the global Internet, it has achieved significant internal control over Internet access and content.

During the WSIS in 2005, Brazil, China, India, Iran, Russia, South Africa, and others denounced ICANN and IANA principally because of the contracts with the U.S. Government. Brazil, for example, complained that "on Internet governance, three words tend to come to mind: lack of legitimacy. In our digital world, only one nation decides for all of us."[33] They demanded that the Internet be truly internationalized, at least by ending the U.S. Government

agreements, and preferably by coming up with an entirely new governance structure in which governments would have a greater role. They played on anti-American feeling, elevated due to the Iraq War. Some threatened to go their own way, like China, creating their own separate Internets using their own rules.

While no government (other than China to some extent) carried through on the threat, and the proposals were defeated, the overall issue has not gone away. As part of the final compromise at the WSIS, there was an agreement to create an Internet Governance Forum, a multi-stakeholder body for discussion, not decisionmaking. At the first forum, in the fall of 2006 in Athens, there was some discussion about changing ICANN's structure, but it was not a major issue. At the second forum in Rio de Janiero in 2007, the issue was more prominent, but there was no consensus among the multi-stakeholder participants on a way forward. A Russian proposal made at the end of the conference to consider placing the Internet under some form of international structure did not draw significant attention.

Because the United States created ICANN, as well as the Internet, it has a distinct position among government actors. First, it holds the three contracts described above: the MOU/JPA with ICANN, the contract with ICANN for management of IANA functions, and the agreement with VeriSign regarding the root zone file. Through those contracts, the U.S. Government can influence ICANN's process. During the 2006 MOU/JPA renewal negotiations, the Government asked for comments about ICANN's performance. There were complaints about transparency and participation. ICANN's promises to improve were incorporated into the MOU/JPA.

The more fundamental question is whether or not the three contracts give the U.S. Government excessive leverage over policy decisions. Those who want to reshape ICANN's structure play upon such concerns. Whether evidence of such influence is genuinely important to the political debate, however, is open to question. The fierceness of the attack by governments (such as those of Russia and Brazil) and some academics seems to have less to do with actual malevolent use of influence than with the possibility of such influence.[34] The evidence of actual influence is meager: the *.xxx* episode, but little else.[35] The practical reality is that whatever influence the contracts give the U.S. Government is limited.

If it overreaches, there would be considerable damage to ICANN's legitimacy, making the cost likely greater than any benefit.

The U.S. Government's use of surrogates and its direct participation through individuals present a more complicated story. Its view is that the extensive deployment of a stable and secure Internet best advances its larger political and economic interests. Its philosophy, reflected in policies of the Clinton and George W. Bush administrations, is that a relatively unregulated atmosphere that relies on competition, open markets, and corporate self-interest best achieves that end. The corporate world can easily work under those assumptions. Nonetheless, there are potential differences. For example, in the discussion over the WHOIS database, a corporation's interest in assuring its customers of their privacy may be inconsistent with the desire of law enforcement to be able to identify IP address holders who hack or commit cyber crime.

U.S. Government employees from the National Institute of Standards and Technology, DOC, Department of Homeland Security, and DOD, among others, are involved in ICANN's committees and, to some degree, in the North American Regional Internet Registry (ARIN). Although identified as government employees, they have no particular status as such and participate generally as individuals. It is their expertise, which is often extensive, and their

long involvement in the process that affords them influence. However, it is somewhat difficult to evaluate the power associated with their participation. Is it the ongoing DOC–ICANN connection, the individuals' influence, or the significant continuing U.S. presence on the board—or some combination of those—that has helped resolve many recent issues in U.S. favor?

One question is whether the U.S. Government's influence can continue. Undoubtedly, its reluctance to terminate the MOU/JPA reflects the view that the contractual arrangement provides for U.S. guidance that might be lost or become subject to other influences if the agreement were to be terminated. However, there is considerable pressure, even from some European allies, to do so. It is also inevitable that with the retirement of U.S. individuals—the founders of the Internet and of ICANN—people from other countries will eventually have as much history and expertise as Americans. When that happens, the principal source of continuing U.S. influence may be through the Government's individual representatives and the U.S. companies who can act as Government surrogates. Unless they are extraordinarily vigorous, it would seem unlikely that the Government's distinct ability to influence outcomes can remain the same as it has been.

The power of nongovernmental participants in ICANN is also difficult to gauge. The 15 voting members of the board currently include 8 incumbents who are associated with businesses involved with the Internet. A former Australian government official and businessman sits on the board as the President of ICANN; the other board members are academics, researchers, lawyers, and a representative of a standards body. Only three of the members in the fall of 2007 were American; no other country had more than two.

The public comments prior to the 2006 MOU/JPA renegotiation suggest a measure of how well ICANN is meeting its goals. The board is generally seen as fair, or at least not dominated by one faction or another. ICANN's mechanisms to legitimize board selection seem to be successful. ICANN has published extensive ethics rules and has taken steps at the board level to manage conflicts of interest.[36] While concerns have been expressed that there may be undisclosed conflicts or that the nominating committee might fail to assure that all candidates have been thoroughly vetted, there is little evidence of any actual problem or of public concern.

The board itself sits atop a structure that has been frequently attacked. There have been complaints about financial reporting and the budget, about appeals from board decisions, and about the openness of the board's own meetings. Other challenges about issues such as transparency, accountability, and participatory decisionmaking figured prominently in comments directed to DOC during the MOU/JPA renewal discussions.

ICANN has not satisfied those who criticize its lack of transparency. In 2003, for example, VeriSign and ICANN became embroiled in an extended dispute about what services VeriSign, as the *.com* registry, could offer. The parties could not resolve the disagreement, and the case wound up in court. The settlement agreement was not popular with many groups active in ICANN.[37] Two lawsuits sought to stop the settlement, and a number of Internet registrars who rely upon the VeriSign registry actively criticized the board.[38] By approving the deal, albeit with some additional safeguards incorporated into the cooperative agreement, the

U.S. Government became a target of the settlement's opponents, who attacked it for endorsing "monopoly pricing."[39]

In response to criticism during the renewal discussions, the board com- missioned a nongovernmental organization (NGO) based in the United Kingdom, the One World Trust, to prepare a report on its efforts at transparency, accountability, and participation.[40] That report,

delivered in March 2007, suggested several improvements to ICANN's process, but gave ICANN relatively high marks for transparency.[41]

However, the unhappiness with ICANN over transparency continues. A posting on June 20, 2007, of responses to ICANN's request for public comments and dialogue on its performance reflected 14 comments. Even though the number was small, some responses were from significant ICANN participants, including GoDaddy (a registrar), the Internet Commerce Association, and the Canadian Internet Registration Authority, which "raised concerns over the transparency and accountability of governance at ICANN including how it conducts its public consultations."[42]

The key method of board consultation for a large number of issues is an online forum combined with formal and informal discussions. The electronic consultation process is open to all those who wish to submit views, and many people take a considerable amount of time to set out positions. As with all online forums, discussion can proceed through exchanges, but the structure is not optimal for getting consensus from initially disparate reviews. Nonetheless, ICANN's online forum on transparency and accountability operating principles had (as of July 2007) reflected no major complaints with the process for registering comments.[43]

ICANN created a policy development process (PDP) several years ago to investigate and articulate positions for consideration by the board affecting the interests of the gTLDs, ccTLDs, or regional registries.[44]

The PDP starts by request of the board, the Supporting Organization (SO) Council, or one of the SO's advisory groups. If either the GNSO (for gTLD registries and others) or the ccNSO (for ccTLD registries) initiates a PDP, an elaborate effort is made to solicit the views of SO constituent groups and the public, with a specific requirement for votes by the constituent groups on the recommendations. If the SOs propose a policy (by supermajority for the GNSO, by consensus or supermajority for the ccNSO), the board essentially is required to adopt it unless two-thirds oppose it.

In September 2006, the London School of Economics Public Policy Group published a study at the request of ICANN that reviewed the GNSO's representativeness, transparency, effectiveness, and compliance with ICANN's bylaws.[45] The report was mixed. Among several substantive negatives were that the "external visibility of the GNSO Council is poor" and that the "information costs [are high] for anyone who is not already a deep insider in ICANN." However, it concluded, "The processes and policy development exchanges of the GNSO Council are highly transparent, more so than most similar organizations," despite "some signs that Constituencies are hard to penetrate for newcomers and that baseline standards such as disclosure of interests are not adequately enforced." In addition, said the study, "Many PDPs take quite a long time to complete," and thus the "process of reaching 'consensus' on major policy issues is often arduous," while "current arrangements for voting introduce further complexities by assigning double-weight votes to two Constituencies (Registries and Registrars)."[46] The report prompted discussion of changes to the GNSO, but these remained inconclusive as of the fall of 2007.

Evaluating the PDP as it currently stands yields a complicated picture. The PDP is an attempt to balance pure participatory democracy against organizational coherence and efficiency. The procedure heightens the value of coalition- building and inclusive outreach; there has to be extensive vetting of ideas before each of the constituent elements of the SO; a public comment period provides an opportunity for individuals who are not involved in the SOs to speak; and deliberations by the constituent elements, seeking consensus or supermajority on the recommendations, are followed by consideration by the SO councils.

The process inhibits any one entity's ability to push a proposal forward unilaterally. In its attempt to reach out to any interested party, anywhere in the world, the PDP creates a lengthy, difficult process that is likely to founder in the face of any significant dissent. As a result, the system will work only if it can avoid problems that require immediate attention where no consensus is in place. However, business and Internet users share an overriding interest in pragmatic solutions that keep the system running. Any other interests they may have in the DNS are probably secondary to their fundamental commitment to a functional and constantly improving system. If, however, other players, such as governments, were introduced into the decisionmaking, their interests might not so consistently favor pragmatic technical solutions, and the PDP or some equivalent would be more prone to fail.

The One World Trust Report issued in March 2007 similarly called upon ICANN to make changes to increase its effectiveness and legitimacy, such as improving ways to publicize how the board makes its decisions, particularly its use of public and advisory input; improving availability of meeting agendas; and more consistent handling of public outreach during the PDP. ICANN has promised to implement some of the changes and to consider others.[47]

Any participant must have specific attributes if it intends to promote a particular policy or point of view within ICANN. An extraordinary commitment of time and effort is required to participate not just at the board level, but also at the board committee, supporting organization, and constituency levels. There has to be a willingness and an ability to go to meetings all over the world, draft papers, and otherwise take time to share ideas with the many participants whose consent is needed to move an issue forward. Corporations have understood the value of such expenditures, but few governments, apart from those of the United States, Australia, and New Zealand, have done so. Individual members of the European Union (EU), and the EU itself, have become more active, and other governments will almost inevitably reevaluate their level of activity as the Internet grows in importance in their home markets.

Effective participation also requires one to be an "insider." The process is so diffuse that those who have not built relationships and credibility are unlikely to have much influence in the decisionmaking. The organization may have aspirations of incorporating global views, but that it functions reasonably well is probably only because the same 200 to 250 people keep coming to the meetings and emailing each other.

Nontechnical issues pose a different challenge in decisionmaking, because they have no technical focus that could create convergence around a single answer. The security and stability of the DNS do not, for example, depend on whether a new gTLD is created (although the creation of a vast number might have an effect). Consensus is more difficult to achieve where there is no one technically best solution or even a technical framework on which to make such a judgment. In the absence of objective data, longstanding representatives who have built up relationships over time have an advantage in navigating the policy process. Even so, they have had to expend large sums over a long period, going to meetings and otherwise participating constantly, regardless of whether their employer or institution has a direct interest in a particular issue under consideration. Few companies or other institutions can support that level of activity, which winnows down the number of players.

The Value Structure Underlying ICANN Governance

A number of social forces and values influenced how ICANN took shape. Deregulation had a real impact on the current structure of ICANN, which also reflects the

broadening acceptance worldwide of participatory democracy. The 1990s were a time of spreading democracy and growing political commitment to direct public participation. The ICANN structure might not have been accepted if the significance of the Internet had been better understood. ICANN may also have benefited from timing. Had the Clinton or Bush administrations proposed ICANN just a few years later, when the power of the Internet had become clearer, other governments might have objected. Another influence on ICANN's structure was the U.S. Government's distinctive laissez-faire attitude toward the Internet. Although the Government, chiefly DARPA and the National Science Foundation, had paid for the initial research, development, and operation of the Internet, the Government refrained from seeking to control its evolution.

Another distinct influence is the power of academia. The Internet reflects the emergence of academics and researchers into an influential role in the "knowledge economy." In fact, the distinction between academia and corporate activity has been virtually erased. For example, whenever the history of Google is recited, it inevitably includes the comment that it was conceived by two graduate students at Stanford University.

A final distinction is the continuing influence of the U.S. Government— which, even if not exercised, may have forestalled the exercise of less benign control by others. During WSIS in 2005, the Government argued that ending its contracts and allowing other governments greater participation could be destabilizing. For a variety of countries—such as Africans nations who wanted to end the digital divide far more than they wanted to humble the United States—the point was persuasive.

The Internet Society and the World Wide Web Consortium

Most of the key organizations for collective decisionmaking about core technical standards and issues of the Internet are now grouped under the umbrella of the private, nonprofit Internet Society. They include the Internet Engineering Task Force (IETF), the Internet Engineering Steering Group (IESG), and the Internet Architecture Board (IAB).[48] Although it is a separate private, nonprofit organization, the World Wide Web Consortium (W3C), which sets standards for the Web (such as Hyper Text Markup Language [HTML], File Transfer Protocol [FTP], and Extensible Markup Language [XML]), is also discussed in this section, because of the Web's distinct and significant function as a principal Internet service.[49]

There are three main working elements of the Internet Society: the IETF, the IESG, and the IAB.

The IETF is an organization of designers, operators, vendors, researchers, and users that anyone may join; it has no formal membership and no membership requirements. All participants and leaders are volunteers, though their work is usually funded by their employers or sponsors. Its mission is to produce technical and engineering documents to help make the elements of the Internet work together better (in other words, to assure interoperability), including protocols, standards, and statements of best current practices. In particular, it develops the standards for the transmission control protocol and IP suite.

An area director oversees each subject area; the directors, together with the IETF chair, make up the IESG, which handles technical management of IETF activities and the Internet standards process. The IAB is responsible for defining the overall architecture of the Internet; it is both a committee of the IETF, providing it with guidance, and an advisory body to the Internet Society. The Internet Society was formed in 1992 to support these Internet

standards activities.

These organizations grew out of the Internet Configuration Control Board (ICCB), formed in 1979 by DARPA's Internet project manager.[50] The ICCB was filled with U.S. Government employees and their contractors. Over a quarter- century later, it has evolved into multiple related organizations that create the protocols and other standards and identify best practices in the Internet's operations.[51] There is close cooperation between these organizations and ICANN, ITU, and the other Internet governance organizations.

The Internet Engineering Task Force

The IETF is "a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet." Its mission is "to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better. These documents include protocol standards, best current practices, and informational documents of various kinds."[52]

The IETF has over 100 working groups in 8 broad subject areas.[53] Working groups address specific issues, mostly by telecommunicating. The IETF as a whole meets three times a year. The areas are overseen by the area directors, who are themselves volunteers, and a small secretariat.

The working groups of the IETF and its standards development process have been central to the evolution of the Internet's core functions. The documents produced by the IETF (known as requests for comment [RFCs]) cover practically every technical specification relevant to the operation of the Internet itself. Any change in the basic Internet protocols, whether relevant to security, capacity, or robustness, must come though the working groups.

The Internet Engineering Steering Group

The area directors of the IETF, together with its chair, form the IESG, which handles "technical management of IETF activities and the Internet standards process. . . . The IESG is directly responsible for the actions associated with entry into and movement along the Internet 'standards track,' including final approval of specifications as Internet Standards."[54] As of the summer of 2007, only one area director was a U.S. Government employee, but many of them were drawn from U.S. corporations.[55]

The Internet Architecture Board

The IAB, a committee of the IETF, is responsible for "defining the overall architecture of the Internet, providing guidance and broad direction to the IETF."[56] It does not focus on specific technical topics but develops documents on general technical principles to support the proper functioning of the Internet and its protocols or creates ad hoc panels to develop ideas in a particular area. The IAB can also convene a workshop or ad hoc panel outside the IETF's standards process.[57] The IAB handles editorial management and publication of the RFC series of publications; confirms the IETF chair and area directors from nominations provided by the IETF nominating committee; serves as the appeal board if there are complaints about improper execution of the standards process in a decision by the IESG; and selects the

chair of the Internet Research Task Force, which addresses long-term Internet-related research projects.[58]

The IAB has 13 members. Six are elected each year for 2-year terms based on nominations from the IETF nominating committee that have been approved by the Internet Society's Board of Trustees. The 13th member is the IETF chair. The board has had only two non-U.S. chairs since 1981; the most recent U.S. chair took office in March 2007. Eight of the IAB members as of mid-2007 were U.S. residents.

The Internet Society

When the IETF grew concerned about continuation of its U.S. Government funding, it created the Internet Society in 1992 to raise money to help support its operations and to handle administrative functions that the engineers viewed as a distraction from their primary focus on technical standards development.[59] As of 2007, the organization had an annual budget of approximately $9 million. In addition to supporting IETF, IESG, and IAB, it sustains a range of policy and education projects, focusing on national Internet organizations and operators. Most of its budget comes from the private sector, but DISA is a major contributor.[60]

Governance of the IETF and Related Bodies

The IETF's governance process is a mixture of straightforward direct participation and complicated policy development. On the one hand, it is broadly participatory: the IETF is open to anyone. As befits that open spirit, the introductory manual for new members is entitled "The Tao of the IETF."[61] However, influence requires continuous, high-quality, technically competent participation. Most of the area directors are senior officials with major corporations or senior researchers at government or academic institutions. The process of creating a new Internet standard has been characterized as arduous; it often takes years to go from IAB approval of a new working group charter to a final RFC that has been approved by the IESG.

The significant U.S. presence in the leadership of the IETF and the IAB provides some protection of U.S. interests. When working groups are so open and diffuse, the area directors and working group chairs derive influence from being able to direct the work and to shape, to some extent, the draft documents. They are probably most influential in determining which new questions will be studied and how the issues are framed. They also have some ability to resolve final outcomes. The adoption process requires only "rough consensus,"[62] which has been defined in many ways; "a simple version is that it means that strongly held objections must be debated until most people are satisfied that these objections are wrong."[63]

To the extent there is government participation, it is as technically oriented as other participation. The fact that any government proponent must present a case that will persuade technical experts who could deny a "rough consensus" makes political appeals not just useless, but counterproductive. As a consequence, when there were attacks on ICANN at WSIS, there was no similar pressure to change the working methods of the IETF. On the contrary, to the extent IETF was a subject of discussion, governments generally applauded its work.

Process at the IETF or other standards bodies is not pristine. It can matter a great deal to companies' competitive positions which standards are selected; that has led at times to accusations of unethical conduct. For example, Microsoft was accused in September 2007 of vote-buying in connection with a decision by the Swedish Standards Institute regarding a document

format known as Open Office XML.[64]

The World Wide Web Consortium

The Web is just one element of the Internet and it has its own standards structure, which is under the control of a much smaller number of participants than is the IETF. The W3C, not the IETF, sets standards for the World Wide Web, and W3C is not part of the Internet Society. However, the W3C involves some of the same people and corporate organizations as the IETF. They coordinate, but rarely need to collaborate, given their separate technological spheres. Governments are not particularly active in the W3C's deliberations, although DOC's National Institute for Standards and Technology and some government agencies from other countries are members of the W3C.

The Consortium was created in 1994 by Tim Berners-Lee (who developed original World Wide Web standards such as HTML, HTTP, and FTP) to promote the Web by creating guidelines and standards to facilitate its use.[65] Today, the consortium is jointly sponsored by the Massachusetts Institute of Technology, the European Research Consortium in Informatics and Mathematics, and Keio University in Japan. Membership is limited to organizations, many of which are academic institutions, consultants, and software companies. Over one-third of the members are from the United States.[66]

The W3C's working methods resemble those of the IETF, but there is more staff involvement and direction. A broad-based approval process relies on literal consensus. Working groups set up to address specific issues include consortium members, staff, and invited experts. The W3C uses member-donated funds to pay for a share of the research and development itself, while participating parties pay the rest. The groups work on a proposed recommendation until there is a consensus. The final version is put before the advisory committee, which has a representative from each member. If there is a consensus, the proposal is adopted as a new guideline.[67]

The International Telecommunication Union

The ITU was founded in 1865 and is now a UN agency.[68] Although the ITU allows private sector companies to participate in deliberations, it is unlike ICANN and the IETF in that only governments vote on final decisions. The distinction is one source of tension in the evolution of Internet governance.

The ITU's Telecommunication Standardization Sector (ITU–T) issues technical and operating standards for telecommunications networks and addresses tariff questions that can affect the Internet.[69] It does not address the technical issues integral to the internal operation of the Internet itself. Its Secretary-General and senior staff have speculated that the ITU could assume a larger role in Internet governance, perhaps taking over some of ICANN's functions.[70] Hence, both for what it does and what it might do, the ITU has a major role in Internet decisionmaking.

The worldwide telecommunications system depends upon the standards and tariff work in the ITU–T. The Internet has always been dependent on telecommunications networks for delivery, and the relationship between the two grows closer with the convergence of technologies, especially increasing use of voice over IP (VoIP) communications.

The range of questions under consideration in the ITU–T in mid-2007 demonstrated

the scope of its influence over the Internet. At least 20 questions before the ITU–T's 13 study groups directly would affect some aspect of Internet policy. Many more would have some collateral effect on the delivery or quality of Internet service.

ITU Collective Decisionmaking

The ITU operates differently from ICANN and the IETF, both because it is part of the UN and because it developed when telephone service was, in most of the world, a government-run function. Only governments vote in the ITU, making it a true intergovernmental organization.

That voting power creates a complicated process for the adoption of new standards. The practical reality is that private companies have the lead role in ITU deliberations, particularly in the ITU–T. The union has created "sector members," a membership category for nongovernmental entities that have an interest in the ITU's deliberations. These may be "recognized operating agencies" that operate a public correspondence or broadcasting service; scientific or industrial organizations that study telecommunications problems or that design or manufacture telecommunications equipment; other entities dealing with telecommunications matters; and regional and other international telecommunication, standardization, financial, or development organizations.[71] There are 191 national government administrations that are full members of the ITU and over 700 "sector members," including practically every major corporation with an interest in the telecommunication industry.

The ITU–T's method of doing business is worthy of close examination in this era of privatization and globalization. With the end of state-run telephone companies in most of the developed world, governments no longer have the expertise to provide much of the technical work that is the basis for the ITU's standards and other recommendations. They also have little direct incentive to participate, except insofar as the stability and security of their own national or intragovernmental networks are at issue.[72] The result is a need for close cooperation between the sector members, who do the actual investigation and drafting of the recommendations—and who have the economic interest in their passage—and the governments that vote on their adoption.[73]

Every 4 years, at the World Telecommunication Standardization Assembly (WTSA), all national administrations and the nonvoting sector members meet to define general policy and adopt working methods and procedures for the telecommunications sector. The WTSA determines many of the topics to be addressed by each study group; the study groups can identify additional matters. The study group chairs then develop work plans to address the questions posed under each topic. They take into account the directions of the WTSA and the recommendations of the Telecommunication Standardization Advisory Committee, which holds regular meetings of all government and sector members to advise the sector's bureau director.[74]

The chairs of the ITU study groups select the leaders of working parties, may appoint rapporteurs to investigate a particular issue, and may provide a report or draft text for a new recommendation. The study groups or the director of the Telecommunication Standardization Bureau may also create focus groups for the quick development of standards on specific subjects. According to the ITU–T, "the key difference between Study Groups and Focus Groups is the freedom that they have to organize and finance themselves."[75] The study group chairs have the power to appoint leaders of the subgroups and to determine the number and timing of meetings for each subject; this gives them considerable power to control the groups' work.

A sector member may submit contributions directly to a working party or propose instead that the submission be made in the name of its government. A government may submit a paper itself, or it may seek the endorsement of one of five regional groupings, such as the Inter-American Telecommunication Commission of the Organization of American States (*Comisión Interamericana de Telecomunicaciones,* or CITEL).

For example, in the United States, the formal interaction between sector members and the Department of State (which represents the United States at the ITU) occurs in the International Telecommunication Advisory Committee (ITAC), which is composed of interested private sector companies. However, because of the nature of the ITU–T's work, much of the public-private collaboration actually occurs at the Federal Communications Commission (FCC), whose International Bureau works closely with the State Department and private companies.[76] Following ITAC deliberations on a proposal, the U.S. Government reviews it in an all-government "national committee" that includes State, the NTIA, the FCC, and at times other agencies. If the proposal raises security and stability concerns that conflict with some other interest, the ITAC recommendation may go nowhere or be sent back for further negotiation. Although there is considerable one-to-one contact between company and government representatives during this process, rules of procedure under the Federal Advisory Committee Act slow down the ability to resolve issues.

The United States usually submits proposals to the ITU in its own name, but it has sometimes looked to CITEL for support. CITEL and the other four regional groupings have grown more active in recent years. They represent large blocs of votes, and thus a CITEL endorsement indicates wide support. However, the time and effort needed to win national and regional approval for a proposal may sometimes be impractical.

Whether a proposal comes from a private sector member or a government, after it has been considered in an ITU study group, a unanimous vote of the study group is required before final drafts of recommendations are adopted. The unanimous consent requirement gives nations leverage to negotiate even if, like the United States, they are not closely allied with a regional grouping. Unilateral vetoes have been rare.

In 2000, however, the WTSA adopted a rule for a fast-track alternative, called the Alternative Approval Process (AAP), for recommendations that were deemed not to have a regulatory or policy implication. A majority of Study Group activities appear to be on the AAP fast-track list.[77] WTSA later revised AAP to provide that proposals under fast-track consideration could be adopted despite the objection of a single national administration, but the United States strongly objected. The fast-track proposal was then further revised to allay concerns about loss of national sovereignty, effectively returning to the requirement of unanimity.[78]

The ITU–Radiocommunication Bureau (ITU–R), which deals with radio spectrum management, is not as central to issues related to Internet governance. However, broadband wireless communication is within its jurisdiction and is an important means of expanding the Internet's reach. The working methods of the ITU–R generally are similar to those of the ITU–T, but the relative power of the actors is somewhat different. Because national governments have significant interests in the radio spectrum, both for military and public safety uses, and they retain control over civilian spectrum allocation, they take a more active role in ITU–R deliberations. Their interests are more often at odds with the private sector, and ITU–R decisions reflect national security concerns more than in the ITU–T.

Although ICANN, IETF, and the ITU recognize each other and try to cooperate and

coordinate standards activity, there is inevitable overlap in some areas, particularly on hot-button issues such as stability, security, and internationalized domain names. That can lead to forum-shopping.[79]

Exercise of Power at the ITU

In the ITU–T, private sector companies, which draft and advocate most of the recommendations developed by the study groups, have the most influence. Power in the ITU is more of a mix of technical expertise, commercial pressures, and national political interests than in the IETF or ICANN. Political issues do not necessarily have primacy: governments with privatized phone service or a desire for a better system or wider Internet service will often do what is technically logical, although they may try to provide their corporate "national champions" with opportunities to capitalize on the standards.

The United States has done well over the years at the ITU. Both its national security interests and its commercial goals have been advanced. Success is generally attributed to the State Department's leadership of U.S. delegations and the active involvement of U.S. corporations in study group meetings. Here, as with the IETF, U.S. influence comes from its considerable presence among study group chairs.[80] Also as with the IETF, these bodies are dispersed globally, and thus those who control the work flow and the appointment of subordinate leadership have considerable power. Many of the U.S. chairs and cochairs will be stepping down in the near future; unless new U.S. leaders replace them, the U.S. ability to shape events will decline.

More significantly, there are considerable pressures to diminish U.S. influence by increasing the ITU's role in Internet governance. In early 2007, the new ITU secretary-general invited comment on Plenipotentiary Resolution 102, which instructed the secretary-general to "continue to take a significant role in international discussions and initiatives on the management of Internet domain names and addresses and other Internet resources within the mandate of the ITU."[81] Many responses came from countries that were also active at WSIS in calling for an overhaul of Internet governance.[82] For example, Brazil's response pressed for the ITU to assure that governments play a role "on equal footing" in Internet public policy issues. Iran drew attention to the fact that only the United States has more than an advisory role in Internet governance mechanisms. Saudi Arabia, too, argued for a greater ITU role in "worldwide coordination of technical and policy issues related to the management of Internet domain names and addresses."

A second force for change within the ITU was reflected in the WSIS Tunis Agenda for the Information Society (the Tunis Final Acts). It identifies various UN agencies to take the lead in coordinating specified Internet-related subject matters (called *action lines*), as originally described in the 2003 WSIS Action Plan.[83] Two action lines were assigned to the ITU: information and communication infrastructure, and building confidence and security in the use of Information and Communication Technologies.

In early 2007, the newly elected secretary-general announced initiatives for each of the WSIS Action Lines. The ITU, along with the World Bank and others, planned a "Connect Africa" conference in Rwanda for that year. The secretary-general also published the ITU Global Cyber-security Agenda to implement the cyber security action line.[84]

The question is whether these activities will eventually involve the ITU in decisionmaking now done elsewhere. At present, the ITU has a formal agreement with the IETF

intended to foster collaboration and prevent duplication of effort.[85] There are regular meetings between IETF and ITU–T leadership, and there have been joint workshops. The ITU is also active at ICANN but, except as noted, has not attempted to take over any of its functions.[86] Numerous ITU study group questions acknowledge work done at ICANN or IETF and promise not to duplicate their efforts. The secretary-general has repeatedly disclaimed any interest in changing the balance among the organizations.[87] However, projects such as the ITU's Global Cyber-security Agenda may eventually alter the division of labor.

A third force for change is the ITU's own staff. The former secretary-general and the director of the TSB have suggested that the ITU should take on additional Internet functions, such as running the IP addressing function.[88]

The U.S. Government, many other governments, and the overwhelming majority of ITU private sector members strongly opposed such ideas, and those proposals did not move forward. The secretary-general recognized that it was such a major issue for the United States that he had to address it directly during his campaign for office, but it remains to be seen whether he can honor that promise against pressure from some governments and ITU staff.

Other International Organizations

Discussion to this point has focused on agencies that set the Internet's common operating standards. However, the Internet has also created some issues and problems that have prompted action by governmental or international bodies. This section highlights what may be the most influential of these actions: the antispam toolkit developed by the Organization for Economic Co-operation and Development (OECD); the Council of Europe's Cybercrime Convention; and UN development activities.

OECD Spam Toolkit

The OECD is a 30-nation organization devoted to promoting sustainable economic growth and employment, economic expansion, and world trade. Information and communication technologies, electronic commerce, and the wider economic implications of the Internet have for many years been regular elements of the OECD work program. The organization regularly issues reports and other information about the Internet to support economic development. Because of the extraordinary burden on electronic commerce and communications created by unwanted Internet solicitations known as *spam*, OECD members decided to go further and to create a series of recommendations to governments about how to combat the problem, which they called the "Spam Toolkit."[89]

The toolkit reflects the fact that the Internet does not recognize national boundaries.[90] However, while it encourages international cooperation, it does not suggest any kind of international treaty or binding commitment by governments.[91] Instead, it focuses on suggestions for national legislation, regulations, and private sector initiatives. This reflects the limits of common action when, due to variations in views on commercial and political free speech, privacy, and consumer protection, governments are unable to arrive at a common definition of the actions they want to curb.

There has, however, been some progress toward shared goals in combating spam. For example, over two dozen antispam agencies and more industrial partners developed the London Action Plan, an initiative to promote international enforcement cooperation.[92] There is a similar

agreement among several European antispam enforcement agencies. Where adequate agreement to create a treaty is lacking, however, the OECD's toolkit encourages governments and industry to create more cross-border programs.

The Council of Europe Convention on Cybercrime

The Council of Europe is an organization of 47 European states that was created to promote democracy, human rights, and the rule of law in Europe. Although its focus is not the Internet, its antiterrorism, anticrime, and human rights efforts have led it to make proposals that affect Internet use and abuse. In particular is its Convention on Cybercrime, opened for signature in 2001.[93] As of December 2007, the convention had been signed by 43 countries and ratified by 21, including the United States. Its goal is to improve governments' ability to deal with cyber crime by harmonizing national laws and facilitating international cooperation against cross-border criminal acts. Parties to the convention agree to pass national legislation to outlaw specified cyber crimes, to take responsibility for crimes within their jurisdictions, and to authorize necessary investigative techniques. The convention also provides for assisting other nations' criminal investigations and the extradition of cyber criminals.

An example of the difficulty of drafting international legal rules for the Internet was a proposed provision to the convention, sought by many European nations, that would ban racist language. It was removed at the insistence of the United States, which saw it as an infringement on free speech guaranteed by the U.S. Constitution. There is now a separate protocol on racist language, which the United States has refused to sign.[94]

The convention has facilitated tracking down cyber criminals among signatories. However, cyber criminals will still have safe havens in countries such as North Korea or Yemen that do not sign the agreement.[95] Hence, while something like the convention is necessary to control international cyber crime activities against victims in the United States, it will never be totally effective because adversaries can evade it.

One recent high-profile example of the problem occurred in May 2007, when numerous denial-of-service attacks threatened to paralyze Estonia's economy. Estonia was able to identify several Russian IP addresses as the likely sources of the attacks, but the Russian government was unwilling to help track down the responsible individuals.[96] The Estonians had no choice but to shut down large parts of their networks temporarily in order to defend against the intruders.

The Council of Europe has several joint projects with the European Commission; some of these, such as privacy protection, affect the Internet.[97] The European Union's involvement in the Internet is considered below, but it should be noted here that the EU now participates in ICANN, and it has had a particular impact on the Internet through the enforcement of its privacy guidelines.[98]

UN Development Activities

The WSIS and the UN's Millennium Development Goals committed the organization to promoting the expansion of the Internet in the developing world.[99] In April 2007, the UN secretary-general reported on activities designed to follow up on the organization's WSIS commitments, which reflected the Millennium Development Goals for economic growth in the developing world.[100]

The report is a snapshot of a great many activities, but they have had far less effect

than market forces on Internet expansion. The WSIS had identified various action lines for the expansion of different aspects of the Internet in the developing world, specifying UN agencies for lead roles. As of the fall of 2007, however, the UN Department of Economic and Social Affairs had not gotten much beyond the consultation stage in its work on action lines. The one organization that had made real progress was the ITU.

Although the UN has laudably embraced an information technology development agenda, it is not likely to play a pivotal role in the actual expansion of the Internet. The UN's work may ultimately yield real benefits, especially in capacity-building and information-sharing, but those efforts will be dwarfed by competitive market forces

The UN's Internet activities are not exclusively focused on development. The UN Commission on International Trade Law has devoted extensive efforts to electronic commerce and has in particular spent several years working on a draft convention.[101] The challenge to the successful completion of the document is finding common ground among different legal systems for activities that may have a pervasive effect in local economies.

There is one other UN-related organization whose activities are worth noting: the World Intellectual Property Organization (WIPO). While its attempts to resolve intellectual property protections for material on the Internet are not fundamental enough to the functioning of the Internet to justify extensive discussion in this chapter, WIPO's deliberations have a vast impact on content providers who place materials on the Internet for use or sale. For any entity interested in influencing the economic results of using the Internet, the ability to achieve results at WIPO is extraordinarily important.

This discussion of intergovernmental organizations' activities is illustrative rather than exhaustive. It does suggest three significant points.

First, there may be political pressure to take action, even where no consensus exists. Intergovernmental agencies have adapted by finding ways to move forward without calling for mandatory regulation. Second, governments still have considerable power based on their national sovereignty, and they can exercise it to frustrate the ability of others to control aspects of the Internet within their own territory. Third, the private sector and users are quickly deploying the Internet, for which they need an "enabling environment" from government. That is, they need to be able to operate without undue regulation in a free market and be supported by adequate infrastructure such as the power grid. Although governments seek to support deployment of the Internet, their more significant role in Internet governance may be in constraining some aspects of its use rather than in promoting it.

National Governments

Where can national governments have impact on the Internet? How, and how much, can they influence the exercise of cyberpower by others? Governments have not always acknowledged the logic of the globalized nature of the Internet. They have acted based on their longstanding notions of national sovereignty, with varying degrees of success.

For example, the NTIA has pushed U.S. registrars to limit the practice of "tasting," which allows someone to use a domain name for a brief period at no cost. Although the practice is sanctioned by ICANN, it has become an attractive device to cyber criminals as a way to avoid being identified.

The suppression of free speech is another contentious issue. The U.S. Government's position on free speech led it to oppose the ban on racist language proposed in the Convention on

Cybercrime. At the same time, it has adopted antipornography laws to shield children from adult content. While Americans can reconcile those positions, others see contradictions.

The U.S. Government, the press, civil rights advocates, and other free-speech proponents have attacked the Chinese government for attempting to filter out words such as *democracy* from Web sites.[102] Chinese authorities have defended the practice, claiming the need to protect civil order, and have cracked down on Web sites containing what they consider politically troublesome content. Some U.S. companies have acceded to Chinese requests to eliminate the troublesome words and to reveal the identities of the Web site operators. Recently, Burma used an even heavier hand, shutting down its international Internet connections entirely during civil unrest in the fall of 2007.[103]

In other areas, governmental capability to control the Internet remains unclear. For example, debate in Congress on the issue of "net neutrality" leaves open the question of whether national legislation will work on a problem that is really Internet-wide. Some Internet service providers have raised the possibility of creating tiers of service, prioritizing some packets over others. Opponents call for net neutrality. So-called net-neutrality legislation has been proposed that would ban or limit tiered service. However, any prioritization program would only work if adopted worldwide, or at least broadly enough to allow faster delivery of priority traffic.[104] Eventually, U.S. activity around this issue may be a test of how far a nation can push its own policies without degrading the worldwide standards necessary for the system to function.

Other Standards Organizations

The Institute of Electrical and Electronics Engineers (IEEE), the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC) are involved in standards work on a broad range of issues, not just the Internet.[105] Each of these organizations encompasses specific concentrations on standards for devices, hardware, and software related to the Internet. The IEEE, for example, developed the 802 standard for wireless device connections to the Internet and has a focus on Internet best practices. The three organizations work closely with each other. A Joint Technical Committee on Information Technology combines the IEC's work on hardware with ISO's work on software. Each has a memorandum of understanding with the ITU. The ISO and IEC have agreed upon a common patent policy with the ITU to address how to deal with patented technology in standards.[106] While the three organizations have somewhat different processes for standards development, influence in each requires technical competence, as well as continuous and long-term participation.

The IEEE is a professional organization that develops industrial standards in a broad range of disciplines, including electric power and energy, biomedical technology and health care, information technology, information assurance, telecommunications, consumer electronics, transportation, aero-space, and nanotechnology. Open to anyone (although full membership requires attainment of specified educational standards), it has over 300,000 members and 10 technical divisions. The IEEE's Standards Association has 20,000 members who can join the standards process and participate in the standards coordinating committees. Their consensus recommendations are reviewed by a review committee and then by the association's standards board.

The ISO is an international standards-setting body that acts as a consortium of various national standards associations. Countries are represented by national committees; the American

National Standards Institute (ANSI) is the U.S. member.[107] Within ISO, national committees propose standards that are negotiated and then voted upon. Two-thirds of the ISO members that have participated actively in the standards development process must approve the standard; if so, and if 75 percent of all members that vote approve it, the standard becomes an ISO standard.

The IEC is a not-for-profit, nongovernmental international standards organization that sets standards for electrical, electronic, and related technologies, such as power generation, home appliances, semiconductors, batteries, and marine energy. Its members are called national committees, and each represents its nation's interests in the IEC. The U.S. committee operates through ANSI. Approximately 10,000 people working through 179 technical committees and 700 project teams develop standards that are then voted upon by the national committees. The IEC publishes standards with the IEEE and develops standards jointly with the ISO as well as the ITU.

These three organizations coordinate their activities to reduce subject matter overlap. ISO is less specialized than IEEE or IEC, but because of the closeness of their subject matters, ISO and IEC set up a Joint Technical Committee on Information Technology a quarter-century ago.

The significance of these standards is commercial; they have much less impact on national cyberpower than do the decisions of ICANN or IETF. The similarities in their processes underscore the difficulty and expense of participation in standards-making decisions, which may limit a participant's ability to manipulate the process to particular advantage.

Conclusion

All of the collective international decisionmaking processes that affect the Internet share some traits:

- they are not speedy, and swift decisionmaking is unlikely
- they stress technical competence and a long-term commitment to the process, and while political considerations are not unknown, outside the ITU, they are not generally influential
- they are worldwide processes, designed to incorporate a range of views
- all the standards bodies except ISO and the ICANN Board require unanimity, or close to it, for adoption of policies
- private, chiefly commercial, interests dominate the processes, even the ITU's standards process
- governments participate on equal footing with others, except within the ITU where governments formally dominate
- decisionmaking processes are fairly transparent, but leaders have considerable discretionary power, and it is not always apparent how that power has been exercised
- overlap of subject matters creates some incentive to forum-shop.

The process of Internet governance has worked reasonably well. The Internet has rapidly expanded around the world and, at least at the technical level, there is good reason to believe that the current collective decisionmaking processes can accommodate additional incremental changes. Internet governance should receive good marks on several measures: openness, democracy, transparency, dynamism, adaptability, accountability, efficiency, and effectiveness.

However, a fair assessment would also identify some problems that could eventually erode its overall legitimacy. Both positives and negatives are reviewed in this concluding section.

What Internet Governance Is

Open. Overall, the Internet governance process is remarkably open. IETF and ICANN both have formal outreach mechanisms to encourage individuals and entities to join and participate in the decisionmaking process. The ITU and the other organizations are not as open, but any motivated business, organizational, or academic interest can participate in ITU, IEEE, ISO, or IEC deliberations.

Generally democratic in spirit, if somewhat less so in practice. Two particular issues arise with regard to democracy: the role of the United States, especially at ICANN, and the relatively small number of people and institutions that are consistently at the center of all the collective decisionmaking.

The role of the United States at ICANN has prompted complaints that it may compel particular decisions against others' views. While there is no doubt that contractual mechanisms give the United States extra influence, recent cases have demonstrated that U.S. exercise of its power can also have negative consequences and is subject to limits.

Most of the positive results in the development of the DNS would have happened even if the U.S. Government had not exercised a supervisory role. The goals of the business interests that would, in any event, have dominated the process are generally aimed at the expansion and development of an open, stable, and secure Internet, all consistent with the goals of the U.S. Government.

The more important value of the U.S. contracts may be in preventing others from asserting some alternative form of control. At WSIS, the demands for changes in the governance of the DNS were not based on complaints about the quality of ICANN's technological decisions. These complaints could fairly be summarized as political: nations either called for removal of the U.S. Government from ICANN management as an expression of anti-American sentiment, or they wanted their political rather than their technical views more effectively included. That would be a problem. It is difficult enough to achieve consensus under the current structure, but affording governments—with their broad range of political interests—greater influence in the mix would undercut the openness, transparency, efficiency, and effectiveness of the current structure, without any compensating benefit to the operation of the DNS.

The second democracy issue is that of the small number of players. Notwithstanding the dispersed and diffuse nature of Internet governance, the system has worked. A fundamental reason is that a relatively small number of people, representing a relatively small number of governments, international organizations, and corporations, participate in all of the work. The process depends not upon strangers from around the world getting together, but on a core group whose members know each other well, doing business together on a regular basis.

The question is whether this small group of active participants in Internet governance could somehow use its influence adversely against the rest of the world. Thus far, that does not seem to have been a significant complaint. Part of the reason is that all participants, particularly businesses, are aware of the constraints imposed by competition policies in the United States, EU, and Japan. So long as there is vigilance about price-fixing and patent abuse, Internet decisions are unlikely to have anticompetitive aspects that would pit users against providers or operators against manufacturers. The key is the continued enforcement of a

vigorous set of competition policies.

Reasonably transparent. The decisionmaking processes at ICANN, IETF, the ITU study groups, IEEE, IEC, and ISO have reasonable transparency. Part of that transparency is organizational commitment; part of it is due to the power of the Internet itself, which allows virtual worldwide conversations in real time. There are shortcomings, and some processes are under review. Administrative and management decisions by study group chairs or their equivalents are not as well documented as other parts of the process.

One problem is lack of trust in decisions of the ICANN board, partially because of suspicions about U.S. Government involvement. It is an ongoing challenge for a small group of ICANN participants to convince a worldwide audience that it has taken their views into account to come to a reasonable decision.

Another problem with transparency is the lack of coverage of many issues by the mainstream media. Much of the news about the Internet winds up on specialized Web sites or on the business or technology pages of the newspaper. For issues that have the potential to be highly visible to the general public, that may be the equivalent of little coverage at all.

Generally dynamic, but with some challenges. The Internet has grown rapidly and has scaled remarkably well. However, it has some potential weaknesses. First, the structure does not generally rely on laws or regulations to which states can compel compliance but rather rests largely on agreed standards. Their force comes in the logic of the system: participants must either follow them or lose the Internet's interoperability. The system has worked well, but it depends on the primacy of interoperability and related values. As an alternative, a nation might, for its own political reasons, create its own alternative Internet in order to better filter traffic from the rest of the world. One other potential source of weakness is that many of ICANN's goals are not even subject to contract: implementation of DNSSec and IPv6, for example, depend on the enlightened self-interest and economic judgment of the parties. The system has worked thus far, but there is no guarantee it will do so in the future.

Second, dynamism is also about coping with the negative consequences of growth. Here, Internet governance is somewhat deficient. The lack of a truly worldwide agreement on how to deal with spam or cyber crime is a major problem. The deficiency is not just a process problem; the Internet has brought various cultures and political systems closer together technologically than they are socially.

Third, other issues may soon demand more dynamism. Net neutrality, for example, calls for a decision on whether to institute a worldwide standard for tiered or neutral provision of service. The issue is ripe for decision in the United States and in Europe (even if the decision is to do nothing). Similarly, there is concern about the need for extensive changes to the core Internet structure to accommodate major increases in traffic, such as implementing higher capacity algorithms and more capable routers and other hardware. The problems are apparent, but the responses may not be in place when needed.

Adequately adaptable so far. The greatest current challenges to adapt-ability of the Internet governance system have to do with Internet security, such as increases in spam and more technologically sophisticated denial-of-service and other attacks. The problem centers upon coordination of the law enforcement and regulatory activity that could curtail security problems. Only a minority of nations have ratified the Cybercrime Convention. Antispam legislation is more effective in some places than in others, but in many countries there is no effective control. Until there is greater consensus on these issues, the response to spam and cyber crime will have to focus on technological fixes.

Accountable, somewhat. All of the Internet governance standards organizations described in this chapter operate on a consensus or strong super-majority basis, except for the ICANN board and ISO. In the IETF, it is easier to stop a proposal than to try to hold others accountable for its adoption, but that structure is sufficient to satisfy questions of legitimacy. ICANN's policy development process makes it easy to stymie a contentious policy; however, someone who is unhappy with a decision and is unable to get satisfaction from any of ICANN's internal accountability mechanisms cannot do much to turn out those who voted for it. At the ITU, there is no way to remove a government from participation in the process, but one could simply wait for a change of study group chairs, which takes place every 4 years. The greatest lack of accountability overall may be with regard to spam and cyber crime. There is no way to force governments to work together to reduce threats to Internet security and stability. The system is not presently prepared to cut any of them off, and as a result, they can benefit from the system even as they, or some of their citizens, may pose threats to its smooth and reliable functioning.

Efficient enough—for now. The Internet governance process can seem slow. Decisions can take years to work their way through the various study groups and other decision processes. Judgment about whether the process is efficient in that sense may need to be tempered by the recognition that the decisionmakers are attempting to achieve worldwide consensus.

Efficiency is more of an issue at the level of national governments. First, resolution of security issues has not kept pace with the growth of the problems. Second, with regard to the developing world, the private sector has long com- plained that many governments have failed to foster "enabling environments" for the Internet—that is, regulatory structures that foster market solutions and competition. Moreover, such environments require education and capacity- building, both of which can take time.

Overall, effective. In sum, Internet governance should be given high marks. Whether one looks at it by scrutinizing each decisionmaking process or by looking at the overall results, the conclusion is positive. Some issues could, nonetheless, raise problems.

First, ICANN must solve its remaining transparency problems, and it must also continue to perform well.

Second, the U.S. Government must work to reduce the international tension surrounding its ICANN contracts, either by convincing the world that the current arrangement, whatever its deficiencies, is better than any alternative, or by terminating its agreements, if it can continue to protect ICANN from less benign influence.

Third, all of the collective decisionmaking bodies must continue to cooperate and collaborate. Attempts by the ITU to take over subject areas now dealt with by ICANN or IETF could be disruptive.

Fourth, national governments and the EU must continue to scrutinize all collective decisionmaking closely to ensure that competition policies are enforced and that Internet governance decisions promote fair competition and a level playing field. There will inevitably be more Internet-related enterprises as growth continues in Asia, Latin America, and Africa. Those governments must be encouraged to give priority to competition over protection.

Fifth, the key players, who are few in number, must continue to focus on the overall good of the Internet. Any attempts to gain undue advantage for a few would risk destroying support for systems that are now private sector– dominated.

Sixth, there must be much more international dialogue on spam and cyber crime. In particular, civil society and the private sector must take more of a lead in developing a consensus on what needs to be controlled and how to control it. Finally, governments, business, and civil

society should be encouraged to recognize that the Internet and its governance rely on widespread acceptance of the values of deregulation, private enterprise, free markets, free speech, and participatory democracy. Participatory democracy must constantly be reconciled with more vertical structures: the pledge of broad participation at ICANN, for example, cannot be allowed to destroy the representative structure that makes decisions possible. If the U.S. Government determines that it is time to terminate the ICANN contracts, it is going to have to rely on these values to create whatever environment will make it feel comfortable that ICANN can continue to function in the way it intended when ICANN was first created.

The dominance of the United States, and the U.S. Government in particular, is likely to decline, whether or not the Government gives up its ICANN contracts. It should worry about that decline only if it believes that without its current influence, the Internet's decisionmaking would no longer support the fundamental U.S. goals of a secure, stable, and competitive system. In the short term, that question is likely to lead to a discussion of the ICANN contracts; eventually, it leads to longer term questions about the configuration of a mature Internet governance structure. The best way for the U.S. Government to promote one that serves its interests is to assure that none of the problems enumerated above come about.

The challenge to those who do not like the status quo is to convince people there is a better alternative. At present, those who want change can make no persuasive case that they could do better. As awkward as aspects of the current system are, it has embraced the powerful values of democracy, the free market, free speech, and private enterprise, and it has delivered a powerful, inexpensive tool for economic, social, and political life.

---

[1] "The Internet's domain-name system (DNS) allows users to refer to web sites and other resources using easier-to-remember domain names (such as 'www.icann.org') rather than the all-numeric IP [Internet Protocol] addresses (such as '192.0.34.65') assigned to each computer on the Internet." "Top Level Domains," Internet Corporation for Assigned Names and Numbers Web site, available at <www.icann.org/tlds/>.

[2] Comments by David Hendon, European Union chief negotiator at the World Summit on the Information Society (WSIS), before a meeting of the Information Technology Association of America's Government Affairs Committee, April 25, 2007, at which the author was present. The two WSIS conferences were convened by the United Nations in 2003 in Geneva and in 2005 in Tunis to address the "digital divide" between the developed and developing worlds.

[3] See Joyce K. Reynolds and Jon Postel, "Assigned Numbers," October 1994, available at <www.ietf.org/rfc/rfc1700.txt>.

[4] "Bylaws for Internet Corporation for Assigned Names and Numbers," available at <www.icann.org/general/bylaws.htm#I>.

[5] "Top Level Domains," available at <www.icann.org/tlds/>. "Each TLD includes many second-level domains (such as 'icann' in 'www.icann.org')."

[6] Ibid. "Domain names may be registered in three of these (.com, .net, and .org) without restriction; the other four have limited purposes."

[7] Ibid. "The responsibility for operating each TLD (including maintaining a registry of the second-level domains within the TLD) is delegated to a particular organization…referred to as 'registry operators,' 'sponsors,' or simply 'delegees''…[These] designated managers…operate the ccTLDs according to local policies that are adapted to best meet the economic, cultural, linguistic, and legal circumstances of the country or territory involved."

[8] Root zone servers are directories that can be queried for the location of Internet protocol addresses for top level domains (they do not route the traffic themselves). There are 13 root zone servers, of which the "A" server is the master; 10 are in the United States. Because of concerns about robustness and reliability, most of the root zone servers now make use of multiple "anycast" servers distributed around the world, which hold duplicate files. See <www.root-servers.org/>.

[9] The Internet Architecture Board has tried to remind ICANN that the technical registration functions for IETF protocol parameters and other technical assignments are separate from IANA's other functions, but the distinctions

have long been blurred. The significance of this caution is that in performing what are generally referred to as the "IANA functions," ICANN is not solely responsible to the U.S. Government. It may complicate how to resolve disputes between the United States and various foreign governments about the ICANN–U.S. Government IANA contract, a significant issue in Internet governance that is discussed below.

[10] When ICANN was formed in 1998, the intent was that it would initially be under the direction of Jon Postel, a member of the University of Southern California's Information Sciences Institute, which had previously performed much the same work under contract to the U.S. Government. Although Postel died shortly after, ICANN came into existence as a continuation of his previous work.

[11] See "Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers," available at <www.icann. org/general/icann-mou-25nov98.htm>. The memorandum has been amended several times.

[12] "Domain Names," National Telecommunications and Information Administration Web site, available at <www.ntia.doc.gov/ntiahome/domainname/icann.htm>.

[13] See below. Critics dispute that characterization.

[14] The memorandum of understanding/joint project agreement does require ICANN to seek governmental advice, which it does through its Governmental Advisory Committee, discussed below. The U.S. Government is a member of the committee.

[15] See "ICANN to Cut U.S. Apron Strings?" *Business Week*, July 28, 2006, available at <www.businessweek.com/technology/content/jul2006/tc20060728_701788.htm>; Associated Press, "US Extends ICANN Agreement Three Years," October 2, 2006, available at <http://entmag.com/news/article.asp?EditorialsID=7846>.

[16] NTIA, "Domain Names: Management of Internet Names and Addresses," available at <www.ntia.doc.gov/ntiahome/domainname/iana.htm>. "The responsibility for operating each TLD (including maintaining a registry of the second-level domains within the TLD) is delegated to a particular organization. . . . [These organizations are] referred to as 'registry operators,' 'sponsors,' or simply 'delegees'…[D]esignated managers…operate the [country-code] ccTLDs according to local policies that are adapted to best meet the economic, cultural, linguistic, and legal circumstances of the country or territory involved."

[17] "United States Announces Intention to Maintain Control Over Internet," *Globalization101.org*, August 9, 2005, available at <www.globalization101.org/index.php?file=news1&id=14>.

[18] Declan McCullagh, "Porn-friendly '.xxx' domains approved," C/netNews.com, June 1, 2005, available at <http://news.com.com/Porn-friendly+.xxx+domains+approved/210 0-1030_3-5728713.html>.

[19] ICANN Press Release, "ICANN's Board of Directors has voted against a proposed agreement for creating a new Top Level Domain, Dot xxx," May 11, 2006; "ICANN meeting passes on .com, .xxx decisions," *CBROnline*, December 5, 2005, available at <www.cbronline.com/news/icann_meeting_passes_on_com_xxx_decisions>.

[20] Eric Bangeman, "ICANN shoots down .xxx yet again," March 30, 2007, available at <http://arstechnica.com/news.ars/post/20070330-icann-shoots-down-xxx-yet-again.html>.

[21] "Cooperative Agreement Between the Department of Commerce and VeriSign (Network Solutions)," NTIA Web site, available at <www.ntia.doc.gov/ntiahome/domainname/nsi.htm>.

[22] Ibid. See particularly Amendments 11 (October 6, 1998) and 19 (September 28, 1999). The amendments required NSI (later VeriSign) to enter into the agreements with ICANN.

[23] VeriSign is still a registry for other TLDs. It won the right to continue with *.net* following an open competition in 2005. Kieren McCarthy, "VeriSign wins back .net registry," *The Register*, March 29, 2005, available at <www.theregister.co.uk/2005/03/29/verisign_keeps_net/>; ICANN, "ICANN Publishes Telecordia Report on their Findings and Rankings for .NET," March 28, 2005, accessed at <www.icann.org/announcements/announcement-28maro5.htm>.

[24] According to recent figures, *.com* now has 112 million registrations. Andrew Allemann, "Domain Registrations Hit 112 Million," *CircleID*, November 30, 2006, available at <www.circleid.com/posts/domain_registrations_hit_112_million/>. Also see remarks by Secretary of Commerce William M. Daley, September 28, 1999, available at <www.ntia.doc.gov/ntiahome.domainname/agreements/92899spicann.htm>.

[25] Amendment 11, October 6, 1998.

[26] In 2006, the Department of Commerce approved a new agreement between ICANN and VeriSign. However, the approval process drew it into a dispute over the agreement, which had been the subject of considerable

dissatisfaction in the Internet community. NTIA eventually forced VeriSign to agree to certain changes, reflected in amendments to the Cooperative Agreement. NTIA, "NTIA Approves New .Com Domain Name Registry Agreement," November 30, 2006, available at <www.ntia.doc.gov/ntiahome/press/2006/icanncom_113006.htm>. Issues included "competition and Internet security and stability issues" and "proposed increase in prices for .com registrants."

[27] ICANN Web site. The non-U.S. voting members come from Canada, Australia (two, including the president of ICANN), France, Kenya, New Zealand (chair), Italy (vice-chair), Norway, Chile, Brazil, Ireland, and India. Of six non-voting liaison members, three are American.

[28] See, for example, Governmental Advisory Committee Secretariat, "The Internet Domain Name System and the Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN)," available at <http://gac.icann.org/web/about/gac-outreach_English.htm>.

[29] See <www.hrea.org/lists/huridocs-list/markup/msg01354.html>.

[30] The Internet Society has local chapters, often referred to as Internet societies. The term may also loosely refer to groups composed of Internet users, some of which may be recognized participants in the ICANN At Large Advisory Committee.

[31] A range of institutions operate country code top level domain (ccTLD) registries. Initially, few, if any, had government ties; most were technical specialists or academics who had the requisite skills. There has been a trend toward more government control in recent years, although it is not clear how many ccTLD registries are now effectively under such influence.

[32] One of the four principles the NTIA announced in 2005 regarding the DNS was, "Governments have a legitimate interest in the management of their ccTLDs. The United States recognizes that governments have legitimate public policy and sovereignty concerns with respect to the management of their ccTLD." NTIA, "U.S. Principles on the Internet's Domain Name and Addressing System," June 30, 2005, available at <www.ntia.doc.gov/ntiahome/domainname/USDNSprincipleso6302005.htm>.

[33] T. Wright, "EU and U.S. clash over control of Net," *International Herald Tribune*, September 30, 2005, 1. The story points out that the European Union briefly also pushed for a replacement to ICANN that would have given governments more control. See Kenneth Neil Cukier, "Who Will Control the Internet?" *Foreign Affairs* 84, no. 6 (November-December 2005), 7.

[34] For example, the Internet Governance Project (IGP) published an extended critique of U.S. Government influence shortly before the 2005 WSIS. IGP, "Political Oversight of ICANN: A Briefing for the WSIS Summit" (November 1, 2005), 3. IGP later criticized the 2006 JPA on the grounds that: "ICANN still gets general policy guidance from the DoC." IGP, "ICANN's New MoU: Old Wine in New Bottle," September 30, 2006, accessed at <www.internetgovernance.org/news.html>. As evidence to support its complaint, IGP pointed to a provision in the 2006 JPA that required ICANN to continue its current practice regarding disclosure of information about IP address holders reflected in its WHOIS database. IGP saw this as dictating substantive decisionmaking. However, ICANN Board member Susan Crawford, defending her vote in favor of the JPA, wrote that she had considered the provision a potential departure from longstanding policy and practice but was specifically assured that the provision would not be enforced if the ICANN Board decided to change WHOIS policy. Susan Crawford, "ICANN and the DOC," *CircleID*, September 29, 2006, available at <www.circleid.com/posts/icann_and_the_doc/>. The WHOIS database has since become the subject of significant internal debate, suggesting that the JPA did not foreclose consideration of major changes.

[35] The author was present at a working group at the Rio de Janeiro Internet Governance Forum in 2007 where ICANN was strenuously attacked. Various conspiracy theories involving the U.S. Government were advanced to explain other decisions, such as the failure to deploy IPv6, but little proof was offered.

[36] ICANN Bylaws, Article VI, Section 6, available at <www.icann.org/en/general/bylaws.htm#VI>.

[37] Wired, "ICANN, VeriSign Reach Accord," *Wired*, October 25, 2005, available at <www.wired.com/science/discoveries/news/2005/10/69346>.

[38] "Lawsuits Filed Against ICANN-VeriSign Settlement," *CircleID*, November 29, 2005, available at <www.circleid.composts/lawsuits_filed_against_icann_verisign-settlement/>; Justin Lee, "ICANN Closes Deal, Upsets Registrars," *WHIRnews*, March 3, 2006, available at <www.thewhir.com/features/030306_ICANN_Closes_Deal_Upsets_Registrars.cfm>. See also Non-Commercial Users Constituency, "NCUC response to the ICANN-VeriSign settlement," available at <www.ncdnhc.org/policydocuments/ncuc- icann-verisignsettlement.pdf>.

[39] VeriSign has subsequently received NTIA approval for renewal of its *.com* registry agreement through 2012, with a

presumption that it will continue thereafter. Amendment 30 to NCR 92–18742, <www.ntia.doc.gov/ntiahome/domainname/agreements/amend30_11292006.pdf>.

[40] One World Trust, "Independent Review of ICANN's Accountability and Transparency— Structures and Procedures," London, March 2007, available at <www.icann.org/ announcements/announcement-4-29mar07.htm>.

[41] Ibid., 5.

[42] "Independent Review of ICANN's Accountability and Transparency."

[43] See <www.icann.org/lists/principles-comments>.

[44] There are two policy development processes; the Generic Names Supporting Organization considers more requests for PDPs because of its broader constituency base, while the ccNSO, PDPs focus on issues related to global ccTLD issues. The Address Supporting Organization, composed of the regional registries, also provides advice on IP address allocations, but has no equivalent process in its bylaws, although they outline opportunity for public comment. See Address Supporting Organization Web site at <www.iso.icann.org>.

[45] London School of Economics Public Policy Group and Enterprise LSE, *A Review of the Generic Names Supporting Organization (GNSO)*, London, September 2006.

[46] Ibid., 9–10.

[47] ICANN, "ICANN Response to One World Trust Review of ICANN's Accountability and Transparency— Structures and Practices," June 7, 2007, available at <www.icann. org/transparency/mop-update-07jun07.htm>.

[48] See "Internet Architecture Board," *Wikipedia*, available at <http://en.wikipedia.org/wiki/Internet_Architecture_Board>. The IAB grew out of the Internet Configuration Control Board formed by the Defense Advanced Research Projects Agency in 1979; it became the Internet Advisory Board in 1984, the Internet Activities Board in 1986, and the Internet Architecture Board in January 1992. The Internet Engineering Task Force began in 1986 as a meeting of 21 U.S. Government–funded researchers. See <www.isoc.org/internet/history/brief.shtml>.

[49] "The Internet and the World Wide Web are not synonymous. The Internet is a collection of interconnected computer networks, linked by copper wires, fiber-optic cables, wireless connections, and so forth. In contrast, the Web is a collection of interconnected documents and other resources, linked by hyperlinks and URLs. The World Wide Web is one of the services accessible via the Internet, along with many others, including email [and] file sharing." "Internet," *Wikipedia*, available at <http://en.wikipedia.org/wiki/ Internet>.

[50] Anick Jesdanun, "Internet Board Picks New Zealander Chair," Associated Press, November 2, 2007, available at <www.newsvine.com/_news/2007/11/02/1069437- internet-board-picks-new-zealander-chair>.

[51] See <www.isoc.org/internet/history/brief.shtml>.

[52] Request for Comment 3935.

[53] These are Applications; General; Internet; Operations and Management; Real-time Applications and Infrastructure; Routing; Security; and Transport. "Active IETF Working Groups," available at <www.ietf.org/html.charters/wg-dir.html>.

[54] "Glossary," available at <www.ietf.org/glossary.html>.

[55] As of summer 2007, 11 of the 16 area directors were American or employed by American- based organizations.

[56] Ibid. See also <http://222.iab.org/index.html>.

[57] See <www.iab.org/about/overview.html>; Request for Comment 4677, Part 3.2.4.

[58] The Internet Research Task Force mission is "to promote research of importance to the evolution of the future Internet by creating focused, long-term and small Research Groups working on topics related to Internet protocols, applications, architecture and technology." There is a steering group whose members are chosen by the chair "in consultation with the rest of Steering Group on approval of the IAB." See <www.irtf. org>; Request for Comment 2014.

[59] See <www.isoc.org/isoc/related/ietf>.

[60] See <www/isoc/org/members-php>.

[61] Request for Comment 4677, Part 4.

[62] Ibid. "The exact method of determining rough consensus varies from Working Group to Working Group. Sometimes consensus is determined by 'humming'—if you agree with a proposal, you hum when prompted by the chair; if you disagree, you keep your silence. Newcomers find it quite peculiar, but it works. It is up to the chair to decide when the Working Group has reached rough consensus."

[63] Request for Comment 4677, Part 5.2.

[64] John Markoff, "Software via the Internet: Microsoft in 'Cloud' Computing," *The New York Times*, September 3,

2007, available at <www.nytimes.com/2007/09/03/technology/ 03cloud.html>.
[65] See <www.w3c.org/Consortium>.
[66] See <www.w3c.org/AboutW3C.mht>.
[67] See the World Wide Web Consortium's Web site, <www.w3c.org>, for a more extended discussion of the process.
[68] A formal treaty, the International Telecommunication Regulations, governs some aspects of international telephone service. It has not been open for revision or amendment for almost 20 years, so it does not directly address the Internet, although its language has been adapted for IP communication. At the ITU's Plenipotentiary Conference in 2006, there were several proposals to reopen the treaty. There may well be a treaty conference on the document in 2012, depending on future ITU decisions.
[69] The bulk of the ITU's Internet-related work is in the ITU–T. The ITU has two other bureaus, Radiocommunication, which deals with some Internet issues related to wireless communication, and Telecommunication Development, which is involved in promoting expansion of the Internet in the less developed world.
[70] See, for example, letter, Houlin-Zhou, Director of the Telecommunication Standardization Bureau, to NTIA, March 3, 2006 (suggesting ITU could operate the IANA function); Circular Letter, Houlin-Zhou, Document CO6/4, March 2006 (suggesting to ITU members that the ITU could operate a dual parallel system of address allocations).
[71] See <www.itu.int/ITU-T/membership/join-itut.html>.
[72] Governments take an active role in the management of the ITU, even if not in the development of individual recommendations. The ITU Council, made up of 46 member- nations elected at the Plenipotentiary every 4 years, oversees the union. Sector members do not participate in the council meetings and only recently have been allowed to have a limited number of "observers."
[73] See Telecommunication Standardization Bureau, "ITU–T Guide for Newcomers," available at <www.itu.int/ITU-T>.
[74] The ITU–T and ITU–R also participate in the Global Standards Collaboration (GSC), an annual meeting of the major national and regional telecom standards bodies that discuss issues where there are both national and international interest, such as next generation networks (which focus on converged IP-based services), broadband rural access, and networked radio frequency identification. An ad hoc group in Intellectual Property Rights advises the TSB director on issues such as the Common Patent Policy adopted by the ITU along with the International Organization on Standardization and the International Electrotechnical Commission. See <www.itu.int/ITU-T/othergroups/ipr-adhoc/index.html>.
[75] See <www.itu.int/ITU-T/focU.S.governmentgroups/index.html>.
[76] Sector members often disagree with each other, offer competitive positions for consideration, and lobby their fellow private sector members and government officials outside the ITAC process. When negotiations lead to no conclusion, the individual private sector member must fend for itself or find an international partner to bring forward the same proposal through some other government.
[77] See <www.itu.int/ITU-T/app>.
[78] The main approval process is set forth in WTSA–04 Resolution 1, Section 9. The Alternative Approval Process is contained in ITU–T Rec. A.8, and its revision is in TSB Circular Letter 110 (August 18, 2006). See <www.itu.int/ITU-T/tap> or <www.itu.int/ ITU-T/app>.
[79] A recent example of the overlap creating a problem involved multiprotocol label switching (MPLS), which is designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients. See <www.wikipedia.org/wiki/MPLS>. The IETF had been working on MPLS for 8 years, the ITU–T for 3. The resolution of the overlap reflects how complex the conflicts can be; the proposal states, "Future work will be progressed by first analyzing the requirements and desired functionality." Since T [Sector]-MPLS utilizes MPLS functionality extensively, the experts recommend that "the IETF Standards Process will be used for extensions or modifications of IETF MPLS Technology." It was clearly noted that there are aspects of the problem space that lie outside the domain of expertise in the IETF or straddle both organizations— for example, management of transport equipment, and some aspects of OAM and survivability. The working team will be tasked to help identify which of these aspects are best standardized in IETF RFCs and which in ITU-T Recommendations." See <www.itu.int/ITU-T/newslog/TMPLS+Agreement+ITUT+And+IETF.aspx>.
[80] As of mid-2007, there were three U.S. ITU–T study group chairs and seven U.S. vice chairs. See <www.itu.int/ITU-T/study groups>.
[81] Resolution 102, Final Acts, ITU Plenipotentiary Conference, Antalya, Turkey, November 2006, available at <www.itu.int/osg/spu/wtpf/wtpf2009/documents/ ITUresolution102_publicpolicy_IPB>.

[82] See <www.itu.int/osg/spu/mina/consultations/contributions_memberstates.html>.
[83] WSIS Plan of Action, available at <www.itu.int/wsis/docts/geneva/official/poa.html>; Article 102, WSIS Tunis Agenda for the Information Society and Annex A, available at <www.itu.int/wsis/documents>.
[84] ITU, "Connect Africa Summit to be held in Kigali, Rwanda, 29–30 October 2007, Marshall Plan for ICT to meet 2015 development goals," July 11, 2007, available at <www.itu.int/ newsroom/press_releases/2007/18/html>; TMCnet, "International Telecommunication Union (ITU); Connect Africa Summit to be held in Kigali, Rwanda, 29–30 October 2007," July 11, 2007, available at <www.tmcnet.com./usubmit/2007/07/11/2775508. htm>; ITU Global Cyber-security Agenda, available at <http://222.itu.int/osg/csd/cybersecurity/gca/background.html>.
[85] Request for Comment 3356; Supplement to ITU–T A-series Recommendations, available at <www.itu.int/ITU-T/recommendations>.
[86] The ITU also has formal agreements setting up collaboration with the International Organization for Standardization and the International Electrotechnical Commission; these are discussed below. ITU–T Resolution 7, "Collaboration with ISO and IEC;" ITU–T Recommendation A.23, "Collaboration with ISO and IEC on Information Technology."
[87] For example, the secretary-general made such comments before the U.S. International Telecommunication Union Association meeting held in Washington, DC, March 5, 2007, at which the author was present.
[88] See, for example, Circular Letter C06/4 from Houlin Zhao, "ITU Activities related to the Internet Protocol (IP) based networks and management of internet domain names and addresses; including activities related to internet governance," March 2006.
[89] See <www.oecd-toolkit.org>.
[90] Ibid., 6.
[91] Ibid., 15.
[92] See <http://londonactionplan.org>.
[93] See also chapter 22 in this volume, "International Law and Information Operations."
[94] Kristin Archick, *Cybercrime: The Council of Europe Convention*, Congressional Research Service Report RS21208 (Washington, DC: Congressional Research Service, July 22, 2004), 3. Also see the 2001 Council of Europe report on the protocol, available at <http://assembly.coe.int/Documents/WorkingDocs/doc01/EDOC9263.htm>. Some European nations and Canada have now signed the protocol. "Canada signs protocol to fight online hate," *OUT-LAW News*, December 7, 2005, available at <www.out-law.com/ page-5901>. For U.S. concerns, see, for example, "Protocol to Cybercrime Convention," *American Journal of International Law* 96 (October 2002), 973–975; Michelle Madigan, "Internet Hate-Speech Ban Called 'Chilling'," *PC World*, December 2, 2002, available at <www.pcworld.com/article/id,107499-page,1/article.html>.
[95] Archick, 3.
[96] Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times*, May 24, 2007.
[97] "Joint Programmes between the Council of Europe and the European Commission," available at <www.jp.coe.int>.
[98] EU privacy guidelines have, among other things, significantly complicated the debate over the WHOIS database. The European Commission's position is set forth in "Opinion 2/2003 on the application of the data protection principles to the Whois directories," 10972/03/EN final WP 76 (June 13, 2003). See also Declan McCullagh, "Is it time to get rid of the WHOIS directory," *C/NET News*, October 30, 2007, available at <www.news.com/8301-13578_3-9807356-38.html>.
[99] The Millennium Development Goals were adopted in 2000. Goal 8 called for a partnership for global development, "in cooperation with the private sector, [to] make available the benefits of new technologies—especially information and communications technologies." See <www.un.org/millenniumgoals/>.
[100] Report of the Secretary-General to the Economic and Social Council, "Promoting the building of a people-centred, development-oriented and inclusive information society: Progress made in the implementation of and follow up to the World Summit on the Information Society outcomes," E/CN 16/2007/2, April 3, 2007.
[101] See, for example, "Summary of Activities, Working Group IV, 1997 to present: Electronic Commerce," <www.uncitral.org.uncitral.en.commission.working_groups/4Electronic_ Commerce>.
[102] Jonathan Zittrain and Benjamin Edelman, "Internet Filtering in China," *IEEE Internet Computing* (March-April 2002); Open Net Initiative, "Internet Filtering in China in 2004– 2005: A Country Study," available at

<www.opennetinitiative.net/studies/china/>; Rebecca McKinnon, "China's Internet: Let a Thousand Filters Bloom," *Yale Global Online*, June 28, 2005, available at <http://yaleglobal.yale.edu/display.article?id=5928>; Amnesty International, "Censorship in China," <www.amnestyusa.org/Internet_Censorship/Implicated_companies/page.do?id=11015>; Rita Desai, "China Filters the Internet," *The Bivings Report*, October 10, 2006, available at <www.bivingsreport.com/2006/china- filters-the-internet>.

[103] Steve Gibbard, "Myanmar Internet Shutdown," CircleID, October 4, 2007, available at <www.circleid.com/posts/710413_myanmar_internet_shutdown/>.

[104] Both the ITU and the OECD have cautioned that the problem is complex. See ITU Study Group 13, discussion of quality of service for Next Generation Networks, available at <www.itu.int/ITU-T/studygroups/com13/sg13-q4.html>; OECD Working Party on Telecommunication and Information Services Policies, "Internet Traffic Prioritisation: An Overview," DSTA/ICCP/TISP(2006)4/Final (6 April 2007), 5, available at <www.oecd.org/dataoecd/43/63/38405781.pdf>.

[105] See <www.iso.org>; <www.iee.org>; <www.iec.ch>.

[106] "IEC, ISO and ITU, the world's leading developers of international standards, agree upon common patent policy," March 19, 2007, available at <www.itu.int/newsroom/press_releases/2007/05.html>.

[107] Although ANSI is private nonprofit organization, its membership comprises both government and nongovernment organizations, as well as corporations, academic and international bodies, and individuals.