Global Governance 13 (2007), 237–254

The Internet and Global Governance: Principles and Norms for a New Regime

Milton Mueller, John Mathiason, and Hans Klein

Since the mid-1990s, efforts have been under way to construct an international regime for global Internet governance. Beginning with the formation of the Internet Corporation for Assigned Names and Numbers, efforts at regime construction were a main focus of the 2001–2005 UN World Summit on the Information Society. However, little progress was made toward an international agreement. This reflected policymakers' ill-advised attempt to shortcut regime construction: they attempted to define regime rules and procedures without first defining underlying principles and norms. This article offers example sets of principles and norms of the type that are missing and that could provide the foundation for an Internet governance regime. The authors conclude that a framework convention would be the appropriate institutional mechanism for advancing regime construction. KEYWORDS: Internet governance, regime theory, World Summit on the Information Society, ICANN, framework convention.

Since the mid-1990s, efforts have been under way to construct a global coordination and policymaking framework for the Internet. Such an international regime for Internet governance would be, at minimum, the sole global authority for the allocation of network addresses and domain names to users around the world. It could do much more, however—perhaps make global public policy on issues like unsolicited e-mail (spam), computer network security, and freedom of expression. Over the ten years of work on this regime, there have been several loci of activity: the Internet Corporation for Assigned Names and Numbers (ICANN), the International Telecommunication Union (ITU), the World Intellectual Property Organization (WIPO), and the World Summit on the Information Society (WSIS). Despite enormous efforts over those years, however, rather limited progress was made toward collective agreement. ICANN does perform technical coordination, but the organization did not win formal international recognition at the UN's WSIS. As for WSIS, it sought a broad solution to regime formation, but after four years of debate, it succeeded only in launching the Internet Governance Forum to continue that discussion.

In what follows, we seek to explain policymakers' very limited success to date in regime construction, and we suggest a way forward. Using concepts from regime theory, we argue that policymakers unwisely skipped foundational tasks in regime construction and immediately addressed second-order tasks. They did not attempt to forge agreements on underlying principles and norms for international cooperation on Internet governance, so that when they tried to build global rules and procedures, they had no consensus. We sketch out that process of regime construction and identify its weaknesses.

In the second half of this article, we propose sets of substantive principles and norms that could provide the initial content of an Internet governance regime. These are offered as an early draft of what could become a collective international agreement. Policymakers need to begin the task of making such a collective agreement. This could take the form of composing an international framework convention that defines collective principles and norms of the type we propose here.

ICANN, Internet Governance, and WSIS

This section sketches out the ten-year history of regime construction efforts and analyzes its modest results to date. ICANN was established as a California nonprofit public benefit corporation in 1998. Its creation was invoked by the US Department of Commerce during a public proceeding in 1997–1998 that invited international participation. ICANN took over the centralized coordination of the Internet's domain name and address assignments that had been performed by two US government contractors: University of Southern California–based computer scientist and Internet pioneer Jon Postel, who acted as the "Internet Assigned Numbers Authority" (IANA), and a company known as Network Solutions, now known as VeriSign. ICANN was deliberately set up as a private sector, multistakeholder governance organization, although it eventually included some governmental input through its Governmental Advisory Committee (GAC). It also retained its contractual relations with the US government, operating under three separate agreements. The US government maintains unilateral oversight of ICANN through these agreements.

ICANN's unique governance arrangement was prompted by two concerns. The first was an attempt to achieve *global* as opposed to *territorial* regulation of the domain name system (DNS). In forming its policy toward the Internet and global electronic commerce, the Clinton administration and major information technology executives at firms like IBM, MCI, and AOL worried that electronic commerce would be undermined by widespread assertions of territorial jurisdiction. With some legitimate cause, it feared that national governments would impose on the naturally global arena of the

Internet a patchwork of inconsistent or conflicting national laws and regulations. A private sector governance authority was perceived as a way around this problem. The Clinton administration's policy called on governments to "establish a predictable and simple legal environment based on a decentralized, contractual model of law rather than one based on top-down regulation."[1] The nonstate governing authority would enter into "private contracts" with industry stakeholders that would be global in scope, rather than subject themselves to a welter of different laws based on territorial jurisdictions. Regarding domain names in particular, the United States proposed in mid-1997 that "it may be possible to create a contractually based self-regulatory regime that deals with potential conflicts between domain name usage and trademark laws on a global basis without the need to litigate."[2]

US policy was driven not only by its positive assessment of global contractual approaches, but by its desire to avoid existing international institutions. US industry and policymakers shared a long-standing antipathy toward the ITU in particular. This was partly a legacy of the war over dominance of global data networking standards in the 1980s, and partly because US technology leadership and its often aggressive liberalism were typically blunted within one country–one vote forums such as the ITU. The United States was also leery of European-led efforts to create a new international treaty or charter for regulation of the Internet, fearing that it would open the door to the imposition of an ITU or UN-like bureaucracy. Thus, the 1998 Commerce Department white paper that served as the founding document for ICANN avoided direct government action while inviting international participation in governance. In recognizing ICANN, the United States delegated its authority to "a new, not-for-profit corporation formed by private sector Internet stakeholders to administer policy for the Internet name and address system."[3]

Prior to the creation of ICANN, the ITU had worked with the Internet Society and WIPO in an attempt to create their own privatized domain name administration regime. That effort, known as the Generic Top Level Domain Name Memorandum of Understanding" (gTLD-MoU),[4] was torpedoed when the US government, which controlled the central coordinating functions of the system through Network Solutions, refused to go along. During the subsequent formation of ICANN, European governments, fearful of being left out of the new regime, pushed hard for the inclusion of governments and international organizations. One result was the addition of a Governmental Advisory Committee (GAC) to ICANN's structure. GAC would provide a consultation and advice forum but was not supposed to have direct influence on board appointments or policy. Another result was the decision to permit the WIPO to develop rules governing domain name trademark disputes. The ITU, to the contrary, was pretty much frozen out, although it could participate indirectly via GAC.

Thus, in the ICANN regime, the United States succeeded in establishing a governance regime dominated by itself and by nonstate actors. The US government privatized and internationalized key policymaking functions but retained considerable authority for itself, acting as contractor to ICANN and also asserting "policy authority" over the domain name system's root, reserving to itself the right to review and approve any changes to the root zone file proposed by ICANN. Initially, the United States promised that this authority was temporary; ICANN would become fully privatized and independent after two years. Later, the United States delayed and eventually retracted that position, retaining its unilateral authority over the DNS root.

Beginning in 2003, the ICANN drama intersected with the WSIS, a United Nations summit comparable in scope and purpose to the Earth Summit of 1992 and the Fourth World Conference on Women of 1995.[5] The idea for a summit that would focus on information and communication technology and development was hatched by the ITU in 1998[6] and authorized by a General Assembly resolution in 2001.[7] WSIS was an unusual two-phase event, with the first summit located in Geneva in December 2003 and the second in Tunisia in November 2005.

The first WSIS summit provided a forum where criticism of ICANN could be formally expressed. The governments of South Africa, China, and Brazil, backed by several other developing countries and the ITU, gained formal recognition of their dissatisfaction with current Internet governance arrangements. Those critics and others questioned ICANN's legitimacy, portraying it, not inaccurately, as a unilateral creation of the United States government[8] and lamenting its ability to make global public policy decisions independently of national governments or international agreements.

This was a clash between two conceptions of the appropriate governance model of the global information infrastructure. The disaffected nations, in league with the world's oldest intergovernmental organization, were asserting the need for a more traditional intergovernmental model—or, at the very least, a multilateral decision by national sovereigns to confirm or amend the existing arrangements. They were also protesting what they saw as dominance of the Internet and its governance by the United States. Others, including private sector defenders of ICANN, the Internet Society, and the US government, downplayed the very need for any "governance of the Internet," or claimed that the existing patchwork quilt of governance arrangements affecting the Internet—extending across ICANN, WIPO treaties, the Internet Engineering Task Force (IETF) and ITU standards, and other conventions—was fundamentally sound and did not need to be tinkered with.

The 2003 WSIS Phase 1 Action Plan produced at the first summit mandated the creation of a Working Group on Internet Governance (WGIG).

The WGIG was tasked to (1) develop a working definition of Internet governance; (2) identify the public policy issues relevant to Internet governance; and (3) develop a common understanding of the respective roles and responsibilities of governments, existing intergovernmental and international organizations, and other forums as well as the private sector and civil society from both developing and developed countries.[9] Constituted in November 2004, the WGIG was a group of forty people more or less evenly representing business, government, and civil society. After several public consultations, it issued a report in July 2005.[10] While the primary impetus for creating WGIG had come from dissatisfaction with ICANN, the working group widened the concept of Internet governance to include all kinds of public policy related to the Internet.

The 2005 WGIG final report studiously avoided defining the Internet, but it did come up with a broad definition of Internet governance drawn directly from regime theory. Its main recommendation was to create a new multistakeholder forum to deal with Internet issues. As the report stated, "[The forum] could address . . . issues, that are cross-cutting and multidimensional and that either affect more than one institution, are not dealt with by any institution, or are not addressed in a coordinated manner."[11] The report did not provide much detail about the forum's methods and procedures, other than that it should be open to all stakeholders and involve especially those from developing countries. On the fundamental issue of roles and responsibilities, the report seems to have been guided by a consensus that governments should control "public policy," but leave "technical management" or "day to day operation" of the Internet to the private sector and civil society. This was a major conceptual flaw, however, because on the Internet, policy issues are often intimately and inextricably related to technical and operational decisions. Moreover, the report failed to deal directly with the problem of the global nature of the Internet and the limits it might place on both the legitimacy and the capacity of national governments.

Confusion was reflected in the report's discussion of governmental oversight, where it could not reach a clear consensus. It only managed to set out four very different organizational models in a very brief outline format. The WGIG report thus reflected an early stage of understanding of Internet governance. The second summit of WSIS, held in Tunis in November 2005, produced the Tunis Agenda for the Information Society.[12] WSIS participants were unable to agree on any concrete changes in ICANN's political oversight, but the agenda's wording challenged specific aspects of the current ICANN regime and set the stage for long-term change. It declared that all governments, not just the United States, should have "an equal role and responsibility"[13] for the DNS root and for Internet public policy oversight. It called for the development of "globally-applicable principles on public policy issues associated with the coordination and management of critical internet resources."[14] The proposed mechanisms for developing these principles, however, were vague and indeterminate. The only tangible change was the creation of a multistakeholder Internet Governance Forum (IGF), which was widely seen as little more than a way to continue the inconclusive discussions of the summit regarding the Internet.

Thus, four years of WSIS debate had produced little concrete change to ICANN and had contributed little to defining a framework for global Internet governance. ICANN would continue to operate unchanged, but its problems of legitimacy continued: the final WSIS agenda had studiously avoided mentioning the organization by name and conferred no explicit legitimacy on it. Yet no alternative arrangement had emerged either. The WGIG final report had sketched out four possible organizational arrangements for governance, but none of them received further refinement at the final WSIS summit. The main WSIS product, the IGF, was a mechanism for continued deliberation.

Such an inconclusive result can be explained only partially in terms of interest-based politics. True, US interests were served by the preservation of ICANN, over which the United States retained unilateral control. However, the inability of other policymakers to even envision an alternative to ICANN or to propose a larger vision of an international regime suggests that ideas, not interests, played a role in the outcome.

We explain these events using regime theory, which holds that international institutions are established through a hierarchy of agreement that starts with principles, proceeds to norms, and then comes to agreement on rules and decisionmaking procedures.[15] In Steven Krasner's full, canonical definition, regimes are "implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations."[16]

Regimes have considerable cognitive content. Regime principles may include scientific theories of causation recognized by actors in an issue area, or concepts of rectitude and standards of behavior defined in terms of rights and obligations. Norms are value judgments or prescriptions for conduct. The inclusion of "rules and decision-making procedures" means that regimes can also translate principles and norms into formal organizations, explicit rules, and even laws.

The elements of regimes are a hierarchy, with "principles" as the foundation. In practical terms, regime construction can manifest a sequential relationship between the different elements in the regime hierarchy. First, the principles are agreed. Without an agreement about the nature of the problem or issue, no subsequent agreement can be reached on what to do about it. Agreement about norms—the standards and obligations that the parties should follow—is highly dependent on agreements about principles.

Once principles and norms are agreed, rules—prescriptions and proscriptions for action—can be defined. As a final step, decisionmaking procedures and the organizations through which they are implemented can be established.

Agreement on decisionmaking procedures and organizations is the last step in negotiating a regime. Partly this is because this step involves what are termed "financial implications" for the parties to the regime. Mostly, however, it reflects the fact that the rules, procedures, and organizations have to be appropriate in terms of both principles and norms. Acceptance of principles and norms will largely determine what rules, procedures, and organizations will be deemed appropriate; conversely, inability to agree on principles can prevent progress on norms, rules, procedures, and organizations.

The 1992 UN Framework Convention on Climate Change offers a simple example. It represented an international agreement on foundational regime principles, such as the basic facts that climate change is taking place and that human pollution plays a significant role in causing it. Without agreement on such underlying principles of scientific causation, no higher-level agreement on limits to pollution would have been possible. Agreement on foundational regime principles was a necessary prerequisite to agreement on higher-level regime rules and procedures.

The WSIS discussion of Internet governance was in a muddle because it did not follow this logical sequence of regime formation. WSIS suffered from a deep flaw in its approach to regime construction: it focused on specific policy issues and on rearranging organizations and procedures without first having reached agreement on the underlying principles and norms of the regime. The result was a confused process in which participants made little progress on practical issues because they were not in agreement about basic facts and assumptions.

Principles for the Global Internet

Having hopefully illuminated the underlying problem of the WSIS process, we now offer concrete suggestions on how to fix it. What is needed are principles and norms for an Internet governance regime. We offer both. Krasner defines principles as beliefs of fact, causation, and rectitude. In this section, we offer a set of principles—basic definitions and statements of fact—that must be recognized and taken into account in any attempt to establish an Internet governance regime. We propose seven principles:

1. Definition: the Internet
2. Definition: Internet governance
3. Fact: Internet standards create a global commons

4. Fact: the Internet is largely composed of private networks
5. Fact: the Internet incorporates an end-to-end design
6. Fact: the Internet requires exclusive and coordinated resource assignment
7. Fact: the Internet is nonterritorial

Definition: The Internet

Any Internet governance regime must build on an understanding of what the Internet is. Two essential features of the Internet are that it is software (not hardware) and that it is an *inter*network (not simply a network.) The Internet does not consist of a physical infrastructure of wires, radio waves, cables, or terminals, although it depends on those physical media for implementation. What we call "the Internet" is really a standardized set of software instructions (known as *protocols*) for sending data over a network, and a global set of unique addresses so the data can be told where to go. The Internet protocols can operate on any physical technology.

The second key concept here is "internetworking." Using the Internet protocols, preexisting networks can communicate with each other, giving users the functionality of a global network, even though there is only a standards-enabled cross-network communication capacity. The actual networks on which the communication occurs are owned and operated by individual organizations, public or private, that either operate their own networks for internal users or that sell network access to external users.

We can therefore offer the following regime principle: The Internet is the global data communication capability realized by the interconnection of public and private telecommunication networks using Internet Protocol (IP), Transmission Control Protocol (TCP), and the other protocols required to implement IP internetworking on a global scale, such as DNS and packet routing protocols.

Definition: Internet Governance

Governance in political science refers to ordering processes, in which different elements are coordinated in a system. We define governance in terms of intentional ordering, in which coordination is achieved according to some plan, and on legitimacy, in which decisions affecting a community are accountable to the members of that community. Thus Internet governance consists of intentional decisions made by the collectivity of the Internet community.

The Internet community consists of the owners, operators, and users of the networks and interconnection protocols discussed above. They either provide communication capabilities or use those capabilities. Significantly, this definition includes nonstate actors as parties to governance. If one understands how the Internet distributes decisionmaking power over the internetworking process, this cannot be avoided and, in some ways, requires an innovation in the way international governance arrangements are constructed.

There are three distinct domains in which the Internet may need governance—that is, intentional and legitimate ordering. Each serves distinct purposes and requires different kinds of processes and methods, so it is vital to distinguish between them in order to develop high-level rules and procedures. The first is technical standardization. This involves reaching agreement about networking protocols and data formats and documenting these agreements. Because standards structure the behavior of machines and people, it is useful to consider them as part of an intentional ordering process. The second is resource allocation and assignment. In the case of the Internet, this means virtual resources—Internet identifiers such as domain names and IP addresses, as well as protocol port numbers. These identifiers require exclusive use, because they must be unique and exclusive to function properly as an address.[17] Resources may also be scarce and require rationing. Allocation and assignment processes coordinate the distribution of Internet resources to users, to maintain uniqueness and/or to ration consumption. The third area of governance is human conduct, which is governed by defining and enforcing regulations, laws, and policies. Whereas the first two governance functions are concerned with the specification or coordination of the technical system, the governance of human conduct orders the actions of *people.* It includes global public policy for such areas as spam, cybercrime, copyright and trademark disputes, consumer protection issues, and public and private security. The discussion yields this definition of Internet governance: *Internet governance is collective decisionmaking by owners, operators, developers, and users of the networks connected by Internet protocols to establish policies, rules, and dispute resolution procedures about technical standards, resource allocations, and/or the conduct of people engaged in global internetworking activities.*

Before considering further principles, we pause to observe how the definitional principles offered here can reduce confusion in higher-level policy debates. These definitions draw a clear boundary around Internet governance issues. They eliminate the problem faced in the early stages of the WSIS/WGIG process, when definitional debates centered on the distinction between a "narrow" conception of Internet governance that included only ICANN and its resource assignment functions, and a "broad" definition that seemed to include anything and everything related to information and communication.[18] Both extremes missed the mark. Confining concepts of Internet governance to ICANN was arbitrary. Many other forms of intentional ordering target communications and behaviors that rely on the Internet protocols. Obvious examples are the World Intellectual Property Organization treaty regulating the distribution of copyrighted materials over the Internet, or international conventions on cybercrime and Internet-based e-commerce. A clear definition of Internet governance facilitates comprehension of the diversity of governance activities.

At the same time, these definitions counteract the widespread tendency to blur the line between Internet governance and governance of all forms of communication and information. The Internet is just a subset of information and communication technologies (ICTs). Many important governance issues related to ICTs, such as spectrum allocation, or telecommunication infrastructure financing and development, are independent of the use of the Internet protocols. Not all of them can be addressed by developing principles, norms, or rules for Internet governance. Many issues involving physical infrastructure are best handled at the national level. Our definitions facilitate a clearer focus on the problems specific to global internetworking. If accepted and used consistently, the definitions prevent Internet governance from becoming a proxy for other problems that really have little to do with the Internet per se.

Fact: Internet Standards Create a Global Commons

Having provided a number of foundational definitions, we now turn to a set of statements of fact. The Internet is based on global and nonproprietary standards that can be freely adopted by anyone. They are "open source" software, published openly and usable by anyone without paying a fee. These standards constitute a global commons.

Fact: The Internet Is Largely Composed of Private Networks

Unlike the standards and software protocols, the networks connected by Internet protocols are *not* open, nonexclusive, and nonproprietary. The Internet is a network of privately owned and administered networks. They are heterogeneous, belonging to households, small businesses, large enterprises, nonprofit organizations, and the (usually privately owned) commercial networks of Internet service providers.

This aspect of the Internet is crucial to understanding how it works and how it might be governed. By facilitating interoperability of heterogeneous networks, the Internet allows for the privatization and decentralization of network operations and policies; it also facilitates privatization and decentralization of software applications and the ability to originate information content as well.

This principle means that the Internet has less need than many other systems for global governance. Private networks or users can build electronic "fences" or adopt filters or practices that can, to some extent, shelter themselves from undesirable forms of communication while maintaining some form of compatibility and interconnection with the rest of the world. Whereas traditional notions of government and governance imply uniformity, the Internet permits variation in policies adopted in response to the same problem.[19]

Fact: The Internet Incorporates an End-to-End Design

End-to-end design is one of the Internet's few general architectural principles. End-to-end means that the design of the network is not optimized for any particular service or set of applications; the network provides basic data transport only, leaving the implementation of user-specific applications to devices attached to the ends of the network.[20] This permits the network to serve as a relatively neutral and transparent platform for the widest possible variety of applications and services, including services never anticipated by the designers. The end-to-end principle is believed to promote innovation, network growth, and market competition.

Although we present commons, private networks, and end-to-end as three distinct principles, it is better to think of them as interrelated. At the end points, the Internet is private; at the core standards level, it is public. The end-to-end principle ensures that private and public complement each other. The market in Internet-related applications, content, and networking requires neutral coordinating mechanisms that enable interoperation. With end-to-end, the sharing and coordinating mechanisms are deliberately minimized to provide maximum scope for initiative and innovation, and there is a clear separation between the parts of the system that are subject to private initiative and control and the parts that are subject to global coordination and nonexclusive access.

Fact: The Internet Requires Exclusive and Coordinated Resource Assignment

The commons aspect of the Internet is in many ways a great enabler, but it comes with one major constraint. The Internet standards create resource spaces that require exclusive and unique assignments to users. By "resource spaces" we refer to names, addresses, and protocol parameter numbers; more specifically, we mean responsibility for DNS root servers, the assignment of top-level domain names, IP address allocation and assignment, and management of the routing tables, which is closely related to address assignment. Exclusivity and uniqueness require some kind of coordination. One can solve the coordination problem in various ways—for example, by centralizing authority in a single organization like ICANN and the Regional

Internet Registries (RIRs), or by interconnecting distributed authorities—but one cannot avoid it if there is to be one single Internet.

Fact: The Internet Is Nonterritorial

The Internet's methods of establishing communication are nonterritorial. This is one of the most critical principles and one that the WSIS process repeatedly failed to deal with. Internet names and addresses create a virtual space that is often independent of geography. Its routing structure is also independent of political jurisdictions, and the costs of routing packets are insensitive to distance. This has created a nonterritorial arena for human interaction and thus for policy and governance. One cannot quite claim that this is inherent in the technology itself. At the earliest stages of the Internet's development, it might have been possible for its connectivity arrangements to be structured to conform to national boundaries. A national or territorial address assignment policy might have been adopted instead of a provider-based address assignment. Global top-level domains such as .com, .net and .org could have been avoided, and everyone could have been forced to register names under country codes. But this is not the way the Internet evolved, and any attempt to force it into a territorial model now would involve enormous transitional costs. Thus, the Internet is de facto nonterritorial, and this must be recognized as a principle.

Norms for the Global Internet

Krasner defines norms as standards of behavior defined in terms of rights and obligations. Norms build on principles.[21] They motivate rules and procedures. Taking into account the principles cited above, we propose the following norms for an Internet regime.

One norm is that the *technical model should be preserved.* The Internet model has an unparalleled record of success in facilitating communication, providing public access to information, rapidly adapting technologically to changing conditions, and making efficient use of available infrastructure. Therefore, a future Internet regime must not contradict the basic architectural principles of the Internet, defined as standards commons; decentralized responsibility for networks, content and services; and end-to-end architecture. There are many advocacy groups and interests that emphasize one aspect of the architectural model to the exclusion of the other. There are those who call the Internet a "commons" or a "global public good" but fail to see the critical role played by private initiative, exclusivity among networks, and market forces. There are those who make the opposite mistake. Both fail to see that it is the powerful, complementary combination of standards commons; market for networks, content and applications; and end-to-end architecture that account for the Internet's success and continued growth.

Another norm is that we *should not allow the commons to be privatized.* Ownership of infrastructure, software, or services should not become concentrated in the hands of commercial providers to the point that it threatens the open, nonproprietary status of the core Internet standards. Global competition policy initiatives and standardization activities, especially regarding software patents, should be guided by this norm. By the same token, we *should not transform the standards commons into a basis for overregulating the private market.* Overzealous applications of the end-to-end-principle may be used as an excuse to regulate conduct at the edges. At its worst, such regulation can change the essential character of the Internet from an association that adds value to all who are connected, to a compulsory compact that binds users in dysfunctional or suboptimal relationships. While action should be taken to prevent privatization of the internetworking standards themselves, the freedom of subsets of users to implement new technologies and adopt new, possibly even incompatible, standards should not be limited.

A fourth norm is that *technical coordination and standardization functions should not be loaded with policy functions.* Recognizing the inevitability of some kind of centralization of power to achieve coordination, this norm is intended to counter the temptation to use control of critical resources to exert leverage over areas of policy unrelated to the technical function of the resource itself. For example, domain names may be withheld or taken away to facilitate censorship or to link enforcement of intellectual property laws to technical management of the Internet. This bundling of the resource assignment and policy enforcement functions typically leads to overcentralized, intrusive policymaking, a lack of due process, and compromised technical management. Insofar as is possible, resource assignment procedures should be uniform, objective, and impersonal and focus on the coordination of decentralized private activity at the end points.[22] This implies that regulation of the fraudulent and criminal aspects of Internet use must be directed at the responsible end points, not at the internetworking process itself. The idea that the content of Internet communication should be regulated through controls within the channel itself rather than through sanctions on the sender or receiver should be resisted. Efforts to control users by controlling the technical architecture of the Internet will stifle its growth and impose major externalities on innocent parties. There is an analogy with other efforts to deal with illicit activities where, as in the case of drug trafficking, the best approach is to address supply or demand rather than to try to interdict transportation.

A fifth norm is that *control of the centralized aspects of the Internet should be distributed and limited as much as possible.* One of the factual principles noted is that the Internet's need for coordination brings with it some degree of centralization of power. As a norm, we posit that this power should be widely distributed, carefully limited, and subject to stringent checks and balances to prevent abuse. Therefore, the unilateral control of the DNS root currently held by the US government is undesirable. But traditional "multilateral" control of the root zone file is not enough, and could make matters worse. One must enact or maintain checks and balances on any possible abuses of the centralized choke points of the Internet by *collections* of governments as well. One reason WSIS failed to make progress on US unilateral control was that many on the Internet feared that US power would simply be seized by others with an equal or greater chance of abusing it. Until this norm is recognized and institutional procedures developed to tame abuses of centralized power, the status quo is likely to remain in place.

A final proposed norm is that *multistakeholder governance should be legitimized and maintained.* This norm is a logical extension of principles relating to private networks and global scope. The Internet is in effect a global confederation of network operators and users and should not be regulated in a top-down manner via agreements among states alone. Internet-based communications do not conform to national boundaries, and the Internet's "public interest" cannot be adequately represented by territorial states alone. Overlapping communities of technologists, educational and research institutions, private corporations, end users, and civil society organizations constitute an informal and diverse "Internet community." Standards organizations affecting applications in particular are diverse and rely primarily on voluntary adoption. Thus, traditional intergovernmental models of governance are not appropriate. We posit as a norm that governance institutions should be structured to harness this diversity and energy by empowering all relevant parties based on their specific role in the aspects over which governance is sought. A new governance regime should seek to take advantage of the Internet's capacity for self-governance as a supplement to and check on governments' capacity for legitimized coercion. The rhetoric of tripartite representation (government, business, and civil society) is not enough; we must pay close attention to the details of representation in governance structures and make sure that end users and individuals, who must overcome steep collective action problems, are adequately empowered. Governmental forms of supervision and oversight must be strategically placed but also carefully limited and lawful.

Moving Forward: A Framework Convention

What would move policymakers forward in the quest for such foundational agreements? The main product of WSIS, the Internet Governance Forum, only provides an arena for continued discussion. It provides no basis for negotiating meaningful agreements. We know from WSIS that it will not be easy to reach agreement on the basic principles and norms that apply to international governance of the Internet. The situation is very similar to that faced in dealing with climate change in the 1980s. In that case, the first step was to agree that the problem existed and to agree on its dimensions. The second step was to agree on the norms that should be applied. Similar to Internet governance, a large number of national actors and different international organizations were involved in climate change issues (the World Meteorological Organization, the United Nations Environment Programme, and UNESCO, to name a few), and NGOs showed significant interest. It was recognized that any new regime would have to have a sound basis in international law, and therefore an international convention would be needed.

Rather than seeking to solve all of the problems of climate change in a single agreement, the governments and organizations concerned decided instead to pursue what they called a "framework convention." This convention would establish the principles and norms under which international action would proceed and set up a procedure for negotiating the more detailed arrangements that would be necessary to deal with climate change. The conference of states party to the convention would become the oversight body and negotiating forum, and its secretariat could provide the necessary studies. The United Nations Framework Convention on Climate Change (UNFCCC) was adopted in 1992 and has provided a basis for subsequent negotiation that has led to progress in dealing with the issue.

The situation with regard to Internet governance is remarkably similar. A large number of national governments and international organizations are involved (ITU, WIPO, the World Trade Organization, UNESCO, and the United Nations itself), as are many businesses, nongovernmental organizations, and individuals. Any effort to deal with Internet governance will have to be firmly grounded in international law, suggesting a convention as a means of providing the necessary standing. The time is ripe for negotiating principles and norms, as well as procedures for dealing with future issues as they arise.

A United Nations Framework Convention on Internet Governance seems to be a reasonable option for states to consider. What should such a convention contain? First, it should define clearly the governance problem and its boundaries. Like the UNFCCC, it should have agreed definitions for key facts or principles about the Internet and should clearly establish the norms that should be applied to Internet governance. This could include the principles and norms formulated above or, at a minimum, such elements as maintaining the openness and freedom of the Internet as a communication channel. A framework convention should indicate those areas in which further agreements need to be reached, particularly in terms of interregime conflicts (like intellectual property and freedom of expression). The norms should clearly indicate the role of civil society and private sector organizations, which have been critical to the development and maintenance of the Internet, in the formal governance process. While there are precedents for the involvement of civil society in international decisionmaking, the framework convention would be an opportunity to advance this element of global governance because of the uniquely important role of business and civil society in the Internet. Third, it should establish agreements on when negotiations should take place—a kind of trigger mechanism based on disputes among other areas, or with the functioning of the Internet. It could establish the concept that when additional legal agreements are needed, these can be in the form of protocols to the convention. Fourth, it should empower the meetings of states party to the convention to act as a kind of overseer of that limited set of Internet-related issues that are deemed appropriate for governance. It is important that the states party set the basis for vigorous participation of business and civil society in this function.

For a United Nations Framework Convention on Internet Governance to be elaborated and agreed upon, considerable further work needs to be done. The WGIG report was part of that work, as was the final WSIS agenda and the civil society declarations that emerged from WSIS. Governments will, of course, also play a critical and probably decisive role. This is a great opportunity to both protect and promote the Internet as one of the world's most important global services.

In conclusion, policymakers need to take one step back if they hope to take more steps forward. To date, the process of regime construction in Internet governance has suffered from a lack of foundational agreement on principles and norms. A framework convention would be the appropriate policy mechanism for addressing these underlying issues and promoting share understanding and agreement. The sets of regime principles and norms presented here offer at minimum an example, and at most a first draft, of the kind of collective agreements that are needed. 🌐

Notes

Milton Mueller is professor at the Syracuse University School of Information Studies, and directs its graduate program in telecommunications and network management. His research centers on policy, institutions, and institutional change in communications and information. He is a founder and partner of the Internet Governance Project, and authored the book *Ruling the Root: Internet Governance and the Taming of Cyberspace* (2002). He is active in ICANN's policymaking processes and in the WSIS civil society Internet Governance Caucus. John Mathiason is adjunct professor of international relations in Syracuse University's Maxwell School of Citizenship and Public Affairs, and a partner of the Internet Governance Project. He has thirty years of experience working with various United Nations organizations, including the International Atomic Energy Agency, the United Nations International

Institute for Training and Research for the Advancement of Women, and the United Nations Development Programme. Hans Klein is associate professor in the School of Public Policy at the Georgia Institute of Technology. His research focuses on public interest dimensions of communication policy. He has published articles on Internet governance, Internet and democracy, social movements, US technology policy, and community media. A partner in the Internet Governance Project, Klein directs Georgia Tech's Internet and Public Policy Project (IP3), and formerly chaired the board of Computer Professionals for Social Responsibility.

1. Bill Clinton and Al Gore, "A Framework for Global Electronic Commerce," 1 July 1997, available at www.technology.gov/digeconomy/framewrk.htm.

2. Ibid.

3. US Department of Commerce, National Telecommunications and Information Administration, "Management of Internet Names and Addresses" (white paper), 63 FR 31741-01, 10 June 1998.

4. For a more detailed history of the gTLD-MoU, see Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (Cambridge: MIT Press, 2002), chap. 7.

5. Hans Klein, "Understanding WSIS: An Institutional Analysis of the UN World Summit on the Information Society," *Information Technology and International Development* 1, no. 3–4 (Spring–Summer 2004): pp. 3–13.

6. Resolution 73, Plenipotentiary Conference of the ITU, Minneapolis, 1998, available at www.itu.int/council/wsis/R73.html.

7. General Assembly Res. 56/183, 90th Plenary Meeting, 21 December 2001.

8. US Department of Commerce, National Telecommunications and Information Administration, "Management of Internet Names and Addresses" (white paper), Docket No. 980212036-8146-02, 5 June 1998, available at www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm.

9. World Summit on the Information Society "Plan of Action," Doc. WSIS-03/GENEVA/DOC/5-E, 13 December 2003, pp. 6–7.

10. WGIG Final Report, "Report of the Working Group on Internet Governance," available at www.wgig.org.

11. Report of the Working Group on Internet Governance, Château de Bossey, June 2005, UN Doc. 05.41622, p. 11, available at www.wgig.org/docs/WGIGREPORT.pdf.

12. Tunis Agenda for the Information Society, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 November 2005, available at www.itu.int/wsis.

13. Tunis Agenda, par. 68.

14. Tunis Agenda, par. 70.

15. Steven D. Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables," in Steven D. Krasner, ed., *International Regimes* (Ithaca: Cornell University Press, 1983).

16. Ibid., p. 19.

17. Mueller, *Ruling the Root,* chap. 2.

18. For a record of some of these discussions, see Don MacLean, ed., *Internet Governance: A Grand Collaboration* (New York: United Nations ICT Task Force, 2004).

19. D. R. Johnson and D. G. Post, "And How Shall the Net Be Governed? A Meditation on the Relative Virtues of Decentralized, Emergent Law," in Brian Kahin and James Keller, eds., *Coordinating the Internet* (Cambridge: MIT Press, 1997).

20. J. Saltzer, D. Reed, and D. Clark, "End-to-End Arguments in System Design," *ACM Transactions on Computer* 2, no. 4 (November 1984): 277–288.

21. Krasner, “Structural Causes.”

22. For an example of the application of this norm to domain name policy, see M. Mueller and L. McKnight, “The Post-Com Internet: Toward Regular and Objective Procedures for Internet Governance,” *Telecommunications Policy* 28, no. 7–8 (2004): 487–502.