THE NEVERENDING CCTLD STORY

Peter K. Yu[*]

A long time ago in a galaxy not so far away, there was a decentralized, global network of computers. These computers shared information with each other regardless of how far apart they were and whether there was any direct line of communication. In the very beginning, this network was used exclusively by government and military agencies, educational and research institutions, government contractors, scientists, and technological specialists.[1] Instead of the domain names we use today, such as "www.amazon.com," users typed in numeric addresses, such as "123.45.67.89," and later host names to send information to other computers.[2]

This network soon expanded, and domain names became a practical necessity, for two reasons.[3] First, alphabetical texts are generally easier for humans to remember than numeric addresses. Second, as Internet traffic increases and as computer systems get reconfigured, the computer server that is used for a particular Web site may change from time to time. In fact, some busy Web sites might use multiple servers, requiring them to take turns to address requests directed to a single domain name. While the Web site owner (or his or her technical staff) might know internally which numeric address the Web site corresponds to at a particular moment, the general public does not. Domain names are therefore needed for identification purposes.

Although domain names are easy for humans to remember, computers do not understand these catchy names. Instead, they have to "translate" these names back to numeric addresses before they can locate the information the users requested. To maximize efficiency and minimize storage, the Domain Name System (DNS) was designed as a hierarchy, like a pyramid. To "resolve" a domain name, the computer issues a query to the name server at the bottom of the hierarchy. If the computer fails to obtain an answer, it will move up the hierarchy. If it still does not obtain an answer, it will continue to move up the hierarchy until it finally succeeds.

At the apex of this hierarchy is a set of 13 root zone servers, which identify the name servers storing the root zone files for all the top-level domains, including both the generic domains—such as .com, .net, or .org—and ccTLDs.[4] Each of these servers is assigned a letter from A to M. For example, the Internet Software Consortium operates the "F Root Server," and the server in London is called the "K Root Server." More than three-quarters of these servers are located in the United States, and the rest is found in Japan, Sweden, and the United Kingdom.

To perform its identifying function, a domain name needs to be unique. Thus, all root zone files must contain identical data.[5] As a past legacy, the database in the A Root Server, which the Internet Corporation for Assigned Names and Numbers (ICANN) currently controls by virtue of its contract with the U.S. Department of Commerce (DoC), is considered authoritative. The other root servers merely copy this root zone file to their servers.

Due to this hierarchy and the lucrative market created by the sale of domain names, there has been an ongoing power struggle over the control of the DNS and authority to delegate and administer ccTLDs. This Chapter recounts the story of this struggle. It traces how ccTLD policymaking has been transformed from *ad hoc*, informal coordination to international, contract-based governance. It also discusses the various major players in the ccTLD debate: ICANN, the Internet Assigned Numbers Authority (IANA), ccTLD managers, national governments, the International Telecommunication Union (ITU), and the World Intellectual Property Organization (WIPO).

This story began when scientists, including Jon Postel and Paul Mockapetris, developed the DNS in 1983.[6] Under a contract with the U.S. government, Postel, and later IANA, managed the DNS and delegated ccTLDs to foreign managers.[7] The first ccTLD .us was created and delegated in March 1985 (see Chapter 11).[8] Two other delegations—.uk (for the United Kingdom) and .il (for Israel)—followed in the same year.

In the very beginning, very few countries were connected to the Internet backbone and, therefore, had no need for a ccTLD. Even when they needed one, ccTLD delegations usually fell into the hands of university computer science departments and educational and research networking organizations, rather than government agencies and organizations that historically provided postal, telephone, or telegraph services.[9]

From 1985 to 1993, Postel delegated ccTLDs on a first-come, first-served basis. Using the notion of a "responsible person," Postel required very limited basic administrative criteria before he delegated a ccTLD. As he wrote, the person in charge of assigning second-level domain names "is generally the first person that asks for the job (and is somehow considered a 'responsible person')."[10]

To avoid political problems, Postel used the ISO 3166-1 country codes to define what entity would warrant a ccTLD.[11] Because these codes were provided by the International Organization for Standardization, a United Nations agency, their objectivity successfully shielded IANA from the political pressure from deciding what was and what was not a country.

Although the use of ISO 3166-1 codes appears systematic and well-planned, the .uk ccTLD betrayed the *ad hoc* nature of early ccTLD policymaking.[12] The ISO 3166-1 country

code for the United Kingdom is .gb (for "Great Britain"). Yet, Postel assigned .uk as the country's ccTLD. Moreover, during a brief period in 1996, IANA delegated codes under the ISO 3166 reserve list, which the ISO 3166 Maintenance Agency reserved specifically for postal purposes.[13]

Notwithstanding the *ad hoc* nature of ccTLD delegation, conflicts rarely arose. Even if they did, when two parties competed for the same ccTLD, Postel usually succeeded in using subtle pressure to induce disputing parties to settle the issue before delegation.[14] As IANA reasoned in a later document, dispute resolution "is usually a long drawn out process, leaving at least one party unhappy, so it is far better when the parties can reach an agreement among themselves."[15]

By the early 1990s, the Internet had exploded on to the world stage. As more countries became connected and as national governments (and private companies) began to realize the full socio-economic potential of a ccTLD, requests for ccTLD delegations increased substantially. The number of ccTLD delegations went from 46 in 1990 to 108 in 1993. By the mid-1990s, IANA had delegated virtually all the ccTLDs, including those in countries that had limited Internet access.[16]

With the increasing interest in ccTLDs, a more explicit delegation and administration policy was in order. In March 1994, Postel published RFC 1591, which described his delegation and administration policy.[17] It stated, first and foremost, that there must be a designated manager for supervising the ccTLD name space, and the administrative contact must reside in the country. Because the manager is the "trustee" for both the nation *and* the global Internet community, the manager must be equitable to all those who request a domain name. In addition, the manager must do a "satisfactory job" of operating the DNS service for the domain, and "significantly interested parties" in the domain must agree that the delegation is appropriate.

Moreover, RFC 1591 assured that IANA would strictly adhere to the ISO 3166-1 list as the basis of ccTLD delegations. As the document stated, "IANA is not in the business of deciding what is and what is not a country." Should a dispute arise, IANA would "tr[y] to have any contending parties reach agreement among themselves, and generally take[] no action to change things unless all the contending parties agree." IANA would only intervene "in cases where the designated manager has substantially mis-behaved," although RFC 1591 did not indicate what constituted misbehavior.

Since the publication of RFC 1591, IANA has issued a number of ccTLD News Memos.[18] Although many of these memos were issued for communication purposes, the first memo addressed the relationship between ccTLD managers and national governments. It stated that IANA "takes the desires of the government of the country very seriously, and will take them as a major consideration in any transition discussion."[19]

Notwithstanding RFC 1591 and the first ccTLD News Memo, controversies existed. For example, RFC 1591 required that ccTLD managers reside in the requested domain. Yet, a British company successfully registered Libya's ccTLD .ly by listing its owner's Tripoli address as the address of the administrative contact.[20] In addition, IANA has delegated ccTLDs to unaccountable commercial entities that had limited ties to the concerned domain. Out of

recourse from IANA, the government of Bhutan sought assistance from the ITU, the UnitedNations-affiliated body that governs international telecommunications matters, to reclaim its ccTLD .bt.[21] Even worse, IANA was dragged into domestic disputes and had to make arbitrary decisions in the case concerning Haiti's ccTLD .ht.[22]

Moreover, not all political entities were included in the ISO 3166-1 list, and those omitted were understandably concerned about how IANA's actions (or the lack thereof) could frustrate their political aspirations. For example, the Palestinians did not receive the .ps domain until the ISO 3166-1 list included the Occupied Palestinian Territory.[23] Conversely, despite its dissolution in 1991, the Soviet Union continues to exist in cyberspace, because IANA fails to delete the .su domain from the root zone file.[24]

The European Union is equally unhappy about the ISO 3166-1 codes. Despite its size and economic importance, it failed to obtain its .eu name space, because the ISO 3166-1 list does not recognize supranational entities.[25] In September 2000, the ICANN board finally passed a resolution approving the delegation of the .eu ccTLD.[26] The European Commission subsequently adopted the regulation for the creation of the yet-to-be-determined .eu registry.[27]

Meanwhile, the Internet had become increasingly commercial and global. By the mid-1990s, the U.S. government decided to privatize the DNS.[28] Following a request for comments from the public, the DoC published a proposal to reform the DNS administration in January 1998.[29] Known as the DNS Green Paper, this proposal mapped out the Clinton administration's domain name policy and explained why the DoC had authority to regulate the DNS. Although the Green Paper was intended to be consultative by nature, many found the document controversial.

In light of this reaction, the DoC abandoned its original rulemaking plan. Instead, it issued a nonbinding statement of policy that became known as the DNS White Paper.[30] The White Paper delineated four basic principles that were used to develop the new DNS system, namely "stability, competition, private bottom-up coordination, and representation." Noting the need to withdraw the U.S. government from DNS administration, the policy statement called for the establishment of a private entity that would take over the DNS. As the White Paper stated, "overall policy guidance and control of the TLDs [top-level domains] and the Internet root server system should be vested in a single organization that is representative of Internet users around the globe."

In addition, the White Paper noted, "neither national governments acting as sovereigns nor intergovernmental organizations acting as representatives of governments should participate in management of Internet names and addresses." Nonetheless, the White Paper recognized the need to ensure international input into the new DNS. It also acknowledged the authority of national governments "to manage or establish policy for their own ccTLDs."

Finally, the White Paper identified cybersquatting—the pre-emptive registration of trademarks as domain names by third parties—as a major problem in the DNS. It called upon the World Intellectual Property Organization (WIPO) to "initiate a balanced and transparent process" to provide the new entity with recommendations on how to deal with cybersquatting. Pursuant to this invitation, WIPO launched the First WIPO Internet Domain Name Process, a

lengthy and extensive global consultative process that involved consultation meetings in 14 countries in six continents and the participation of a large number of government agencies, intergovernmental organizations, professional associations, corporations, and individuals.[31]

Shortly after the DoC published the White Paper, ICANN was incorporated as a private not-for-profit corporation in California, with Postel as its chief technical officer and a board of directors that have limited knowledge of the Internet and domain name matters.[32] In November 1998, the DoC entered into an agreement with ICANN concerning the transfer of DNS management.[33] To take over IANA's operation, ICANN also entered into an agreement with the Information Sciences Institute at the University of Southern California, where Postel worked until his untimely death.[34]

A few months later, the DoC officially recognized ICANN as the private entity mentioned in the White Paper.[35] As Professor Michael Froomkin observed, this development was "no coincidence…. The whole point of the White Paper had been to find a more formal structure for DNS management that left it in Postel's capable hands—and could be presented as a pro-Internet, deregulatory victory for the Clinton administration (and Ira Magaziner). ICANN exists because the Department of Commerce called for it to exist."[36]

Structurally, ICANN benefits from the input of its directors, supporting organizations, and special advisory committees.[37] The committee that deals with global policy and ccTLD matters is the Governmental Advisory Committee (GAC), which is regularly attended by national governments, distinct economies, and intergovernmental organizations, such as the ITU and WIPO. Under the recently reformed structure, the GAC provides direct advice to the ICANN board and appoints liaisons to the board, the committee that nominates the directors, and the various supporting organizations.[38]

To "announce" its taking over IANA's function and to emphasize its authority over ccTLD matters, ICANN issued ICP-1 (ICANN Corporate Policy) in May 1999.[39] Combining RFC 1591 and the ccTLD News Memo #1, this document strengthened the power of national governments on ccTLD matters. As it stated, "The desires of the government of a country with regard to delegation of a ccTLD are taken very seriously. The IANA will make them a major consideration in any TLD delegation/transfer discussions."

In February 2000, the GAC presented to ICANN the *Principles for Delegation and Administration of ccTLDs* ("*GAC Principles*"),[40] which ICANN later used extensively to justify their redelegation efforts. Although the *GAC Principles* sought to provide "the model for institutionalizing the relationship between ICANN, ccTLD delegations, and the relevant national governments or public authorities,"[41] many found the document controversial and antithetical to the interests of ccTLD managers.

Since its establishment, ICANN has delegated the .ps to the Occupied Palestinian Territory and deleted Zaire's .zr in light of the country's change of name.[42] It has also redelegated 10 ccTLDs—Pitcairn Island's .pn, Canada's .ca, Australia's .au (see Chapter 12), Japan's .jp, Burundi's .bi, Malawi's .mw, Laos' .la, Sudan's .sd, Kenya's .ke, and Afghanistan's .af.[43] With the exception of Canada, ICANN has entered into contractual relationships with all of the new ccTLD managers upon redelegation.[44]

In addition, ICANN has been working actively with other ccTLD managers to document their relationships. These relationships vary greatly with respect to the type of organization, policies followed, economics, language, culture, legal environment, and relations with governments.[45] While ICANN expected ccTLD managers to enter into contracts in which the managers would acknowledge ICANN's authority and would agree to contribute fees to the organization,[46] the managers refused. In response, the managers questioned ICANN's authority and criticized the organization for its lack of openness, accountability, and representation.

In February 2002, ICANN President Stuart Lynn openly admitted the need for reforms, something critics have advocated since ICANN's establishment.[47] He wrote, "if ICANN comes to be seen . . . as simply a tool of the U.S. Government, it will no longer have any hope of accomplishing its original mission." Seeking to reconcile the organization's relationship with ccTLD managers, the proposal recommended that ICANN replace the five at-large board seats with government representatives.

In December 2002, ICANN finally completed its reforms.[48] Under the new structure, ICANN has a volunteer board of directors, including 15 voting and six non-voting members, all of which will be selected by the supporting organizations and ICANN's Nominating Committee. To facilitate interests of the ccTLD managers and national governments, a new Country Code Domain Name Supporting Organization (CCNSO) will be established.

While ICANN remains relevant to the ccTLD debate, the increasing concern of ccTLD managers and national governments over ccTLD policymaking might affect how ICANN develops its policy. As Kenneth Cukier pointed out, ccTLD managers have the potential to control ICANN's future: "The confederation of independent ccTLD administrators could bring ICANN vitally-needed legitimacy and funding if it formally recognizes the authority of ICANN and pay it fees. Conversely, if the ccTLD community continues to balk from establishing a formal relationship with ICANN, it would weaken the institution."[49] After all, if the ccTLD managers could convince the DoC that ICANN could not handle ccTLD matters, the DoC might decide not to renew ICANN's contract.

Apart from ccTLD managers, national governments have played an increasingly important role in the ccTLD debate. In a recent survey, Professor Michael Geist found a diverse array of relationships between national governments and ccTLD managers.[50] While government agencies and departments manage 10 ccTLDs, national governments have contractual or informal relationships with many others. Some registries, like those in Canada and the United States, also create a relationship between the country and the domain name registrants by requiring local presence as a prerequisite to registration.[51]

Today, national governments recognize ccTLDs "as a component of their sovereignty and a vital national interest."[52] Realizing that ccTLDs may denote the "brand of the country," some governments openly embrace ccTLDs as "a platform for national economic growth and the institutions of civil society brought online."[53] Some, like Tuvalu, even use ccTLDs as a revenue-generating source, selling off rights in its name space for tens of millions of dollars.[54]

As ccTLDs become increasingly important, national governments begin to assert control over the administration of their ccTLDs. For example, Australia, Canada, and Japan have

petitioned ICANN for the redelegation of their domains. Likewise, the European Union is working closely with ICANN to create the .eu name space.

However, not all governments are interested in working with ICANN. Some might prefer to act alone, or to abandon ICANN for a more favorable international forum, such as the ITU.[55] Indeed, some governments have already sought to use national legislation to regulate local ccTLD managers. A case in point is the government of South Africa, which recently introduced legislation to reclaim control of the .za name space from the incumbent ccTLD manager.[56] Similarly, during the controversial redelegation of the .au domain, the Australian government reminded ICANN that "as a last resort the Australian Government could invoke legislation relating to the self-regulation of the domain name system."[57]

Legally, some governments can consider using the "eminent domain" doctrine,[58] which, if applicable, allows governments to take away private property at fair market value to promote an overriding public interest.[59] Given the socio-economic importance of a ccTLD these governments would likely be able to convince the courts that their actions are constitutional. Nonetheless, such governmental action might not be desirable, for it would bring formal political control over the ccTLD system, and impose constraints on the DNS that ICANN was designed to prevent.[60]

To break free of ICANN, the governments can also join together to establish an alternative root zone file, or a system of root zone files, that replaces the current root zone file. ICANN's governance structure is premised on the general consensus that there can be only one authoritative root zone file, lest there be inefficiency, inconnectivity, economic injury, or even chaos in the DNS. However, if governments become so frustrated with ICANN that they would rather risk infrastructure damages than remain subjected to an overbearing "Leviathan," many might consider alternative roots desirable.[61]

Finally, in the absence of ICANN's intervention or oversight, the international community can work together to develop a "code of practice" to promote harmonization and compliance while minimizing disputes. For example, they can draft an international treaty that sets the parameters of ccTLD management and administration practice. They can also work together to develop a nonbonding document that provides guiding principles to ccTLD managers and national governments.

A case in point is the *WIPO ccTLD Best Practices for the Prevention and Resolution of Property Disputes*,[62] which WIPO released in June 2001. This document provides voluntary guidelines concerning registration practices and dispute resolution procedures. These guidelines were particularly needed, because ccTLD managers retain the power to set policies for their domain—for example, they can decide whether registrants have to be residents of the country, whether they are subject to the Uniform Dispute Resolution Policy (UDRP), and whether their personal information will be displayed on a publicly available WHOIS database.

Of notable interest is the final section of the Report, which advocates the adoption of the UDRP in the absence of any contrary local privacy regulations.[63] The UDRP was introduced in October 1999. It sets forth the terms and conditions related to a dispute between the registrant and a third party over the registration and use of a domain name.[64] Although commentators have

criticized the UDRP for its procedural weaknesses,[65] the policy has been widely acclaimed for its simplicity and cost-effectiveness in resolving trademark disputes. Since the UDRP entered into force in December 1999, thousands of cases have been filed, and the majority of these cases has been resolved satisfactorily and efficiently.

Over the next few years, the struggle for control of the DNS and ccTLD delegations will likely continue. Unlike this story, however, the sequel will be very different. There is little doubt that the story will still include ICANN, IANA, ccTLD managers, national governments, GAC, ITU, and WIPO. However, the story will also feature new, emerging players, like CCNSO, CENTR (Council of European National Top-Level Domain Registries),[66] powerful individual ccTLD managers,[67] intellectual property rights holders, Internet service providers, and major telecommunications and information technology companies. As a result, few can forecast how the future will unfold.

---

[1] For interesting discussion of the origin of the Internet, see generally Tim Berners-Lee, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web* (New York: HarperBusiness 2000); Katie Hafner & Matthew Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (New York: Touchstone 1996); John Naughton, *A Brief History of the Future: From Radio Days to Internet Years in a Lifetime* (New York: Overlook Press 2000); Barry M. Leiner et al., "A Brief History of the Internet," http://www.isoc.org/internet/history/brief.shtml, 4 August 2000.

[2] The use of host names dates back to 1974. *See* M.D. Kudlick, Host Names On-Line (Network Working Group, Request for Comments No. 608), http://www.rfc-editor.org/rfc/rfc608.txt, 10 January 1974. By 1977, the use of numeric addresses was "strongly discouraged." David H. Crocker et al., Standard for the Format of Arpa Network Text Messages (1) (Network Working Group, Request for Comments No. 733), http://www.rfc-editor.org/rfc/rfc733.txt, 21 November 1977, 19. *See also* Jonathan Weinberg, "ICANN and the Problem of Legitimacy," *Duke Law Journal* 50, no. 1 (October 2000): 187-260, 194-195 (discussing pre-DNS Internet addressing).

[3] See Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* 39-40 (Cambridge, Mass.: MIT Press 2002).

[4] For the location of these root servers, see Testimony of Michael M. Roberts, President and CEO, ICANN Before the Senate Committee on Commerce, Science, and Transportation, Subcommittee on Communications, http://www.icann.org/correspondence/roberts-testimony-14feb01.htm, 14 February 2001. In January 2003, Espanix and the Internet Software Consortium announced their plan to jointly develop, install, and set up a root server in Madrid, Spain. *See* "Internet Software Consortium and Espanix to Jointly Deploy a Root Name Server in Spain," *Business Wire*, 7 January 2003.

[5] See ICP-3: A Unique, Authoritative Root for the DNS, http://www.icann.org/icp/icp-3.htm, 9 July 2001 (noting that "[f]rom the inception of the DNS, its most fundamental design goal has been to provide the same answers to the same queries issued from any place on the Internet"). But see note 61 (discussing alternative root servers).

[6] See Paul Mockapetris, Domain Names—Concepts and Facilities (Network Working Group, Request for Comments No. 882), http://www.rfc-editor.org/rfc/rfc882.txt, November 1983.

[7] See Jon Postel, Assigned Numbers (Network Working Group, Request for Comments No. 790), http://www.rfc-editor.org/rfc/rfc790.txt, September 1981; Vinton Cerf, IAB Recommended Policy on Distributing Internet Identifier Assignment and IAB Recommended Policy Change to Internet "Connected" Status (Network Working Group, Request for Comments No. 1174), http://www.rfc-editor.org/rfc/rfc1174.txt, August 1990, 1. IANA was first mentioned in RFC 1083 in 1988. Internet Activities Board, IAB Official Protocol Standards (Network Working Group, Request for Comments No. 1083), http://www.rfc-editor.org/rfc/rfc1083.txt, December 1988, 9.

[8] For the dates of ccTLD delegations, see DNSO, ICANN, History of the Internet: ccTLDs in Chronological Order of Top Level Domain Creation at the InterNIC, http://www.cctld.dnso.icann.org/ccwhois/cctld/ccTLDs-by-date.html, 7 November 2002.

[9] See Mueller, *Ruling the Root*, 88.

---

[10] See Mueller, *Ruling the Root*, 88-89 (quoting Postel).

[11] The list of ISO 3166-1 country codes is available at http://www.iso.ch/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html.

[12] See John Klensin, Reflections on the DNS, RFC 1591, and Categories of Domains (Network Working Group, Request for Comments No. 3071), http://www.rfc-editor.org/rfc/rfc3071.txt, February 2001, 6 [hereinafter RFC 3071] (stating that the .uk ccTLD predates the adoption of the ISO 3166-1 codes).

[13] Examples of these ccTLDs include .ac (for Ascension Island), .gg (for Guernsey), .im (for the Isle of Man), and .je (for Jersey). *See* Kim G. von Arx & Gregory R. Hagen, "Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control," *Richmond Journal of Law & Technology* 9, no. 1 (Fall 2002), http://www.law.richmond.edu/jolt/v9i1/article4.html, ¶ 40 n.86; *see also* RFC 3071, 6 (recognizing that these exceptions "are arguably, at least in retrospect, just mistakes").

[14] Mueller, *Ruling the Root*, 89.

[15] IANA, ccTLD News Memo #1, http://www.iana.org/cctld/cctld-news1.htm, 23 October 1997.

[16] Mueller, *Ruling the Root*, 127.

[17] Jon Postel, Domain Name System Structure and Delegation (Network Working Group, Request for Comments No. 1591), http://www.rfc-editor.org/rfc/rfc1591.txt, March 1994 [hereinafter RFC 1591]. RFC stands for "Request for Comments." Although RFCs were sometimes published in final form, they generally "were intended to be an informal fast distribution way to share ideas with other network researchers." Leiner et al, "A Brief History of the Internet." As Don Mitchell described, the RFC process was a "sometimes brutal process of someone advancing an idea and everyone beating on it until the group consensus was that it would work." Mueller, *Ruling the Root*, at 94 (quoting interview with Don Mitchell). Once consensus was achieved, the RFC would become an Internet standard until it was replaced by another RFC. For a detailed discussion of RFCs and Internet standard-making, see generally A. Michael Froomkin, "Habermas@Discourse.Net: Toward a Critical Theory of Cyberspace," *Harvard Law Review* 116, no. 3 (January 2003): 749-873. As RFC 1718 stated: "there are . . . two special sub-series within the RFCs: FYIs and STDs. The For Your Information RFC sub-series was created to document overviews and topics which are introductory. . . . The STD RFC sub-series was created to identify those RFCs which do in fact specify Internet standards." IETF Secretariat et al., The Tao of IETF: A Guide for New Attendees of the Internet Engineering Task Force (Network Working Group, Request for Comments No. 1718), http://www.rfc-editor.org/rfc/rfc1718.txt, November 1994, 15. Thus, not all RFCs are Internet standards, although all Internet standards are RFCs.

[18] All the ccTLD News Memos are available at http://www.iana.org/cctld/cctld-news.htm. The first memo appeared in October 1997. Four others were published in the next two years. The sixth memo came in October 2001, after a three-year hiatus. Released in the wake of the 2001 ICANN meeting in Los Angeles, this memo invited ccTLD managers to "initiate a bottom-up effort to assess and improve ccTLD registry security practices." Disappointedly, though, the Los Angeles conference focused primarily on online security issues, as a result of the September 11th terrorist attacks, and sidestepped important accountability and ccTLD matters. *See* Verne Kopytoff, "ICANN Forum Warns of Web Vulnerability," *San Francisco Chronicle*, 17 November 2001, 1(B). In February 2003, in the wake of its contract renewal with the DoC, IANA published its seventh memo, discussing Internationalized, or multilingual, domain names and its ccTLD database.

[19] IANA, ccTLD News Memo #1.

[20] Mueller, *Ruling the Root*, 127, 283 n.31.

[21] Kenneth Neil Cukier, "Eminent Domain: Initial Policy Perspectives on Nationalizing: Country-Code Internet Addresses," http://inet2002.org/CD-ROM/lu65rw2n/papers/g03-b.pdf, June 2002, 4.

[22] John S. Quarterman, "Haiti and Internet Governance," *Matrix News* 7, no. 5 (May 1997), http://www.mids.org/mn/705/ht.html.

[23] See IANA, IANA Report on Request for Delegation of the .ps Top-Level Domain, http://www.icann.org/general/ps-report-22mar00.htm, 22 March 2000.

[24] See Arx & Hagen, "Sovereign Domains," ¶ 41; Sergey Kuznetsov, "Russia May Say 'See Ya' to Dot-Su," *Wired News*, http://www.wired.com/news/print/0,1294,55687,00.html, 19 October 2002.

[25] The European Commission believed that the creation of the .eu domain was justified by "a decision by the ISO 3166 Maintenance Agency to extend the reservation of the existing EU code for the purposes of the Internet." European Commission, *The Creation of the .eu Internet Top Level Domain* 5, http://europa.eu.int/comm/information_society/policy/internet/pdf/doteu_en.pdf, 2 February 2000.

[26] See Arx & Hagen, "Sovereign Domains," ¶¶ 42; *see also* ICANN, Preliminary Report, Special Meeting of the Board, http://www.icann.org/minutes/prelim-report-25sep00.htm, 25 September 2000.

[27] For a discussion of the creation of the .eu ccTLD, see generally Arx & Hagen, "Sovereign Domains," ¶¶ 42-44.

[28] For an excellent history of the U.S. government's efforts to privatize the DNS and early development of ICANN, see A. Michael Froomkin, "Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution," *Duke Law Journal* 50, no. 1 (October 2000): 17-186. *See also* Jay P. Kesan & Rajiv C. Shah, "Fool Us Once Shame on You—Fool Us Twice Shame on Us: What We Can Learn from the Privatizations of the Internet Backbone Network and the Domain Name System," *Washington University Law Quarterly* 79, no. 1 (2001): 89-220.

[29] Improvement of Technical Management of Internet Names and Addresses, *Federal Register* 63 (Feb. 20, 1998): 8826-33 (1998). The Green Paper is available at http://www.ntia.doc.gov/ntiahome/domainname/022098fedreg.htm.

[30] Management of Internet Names and Addresses, *Federal Register* 63 (June 5, 1998): 31,741-51 (1998). The White Paper is available at http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm.

[31] WIPO, *The Management of Internet Names and Addresses: Intellectual Property Issues: Final Report of the WIPO Internet Domain Name Process* (Geneva: WIPO 1999): 4. The final report of the First WIPO Internet Domain Name Process is available at http://wipo2.wipo.int/process1/report/index.html.

[32] Unfortunately, Postel died in October 1998, as a result of complications from open heart surgery. As Professor Milton Mueller noted, "His death robbed the organization of its moral center, a good part of its institutional memory, and most of what remained of its legitimacy." Mueller, *Ruling the Root*, 181. For discussions and criticisms of ICANN, see generally James Boyle, "A Nondelegation Doctrine for the Digital Age," *Duke Law Journal* 50, no. 1 (October 2000): 5-16; Tamar Frankel, "The Managing Lawmaker in Cyberspace: A Power Model, *Brooklyn Journal of International Law* 27, no. 3 (2002): 859-902; Froomkin, "Habermas@Discourse," 838-55; Froomkin, "Wrong Turn in Cyberspace"; Joseph P. Liu, "Legitimacy and Authority in Internet Coordination: A Domain Name Case Study," *Indiana Law Journal* 74, no. 2 (Spring 1999): 587-626; Weinberg, "ICANN and the Problem of Legitimacy"; Jonathan Zittrain, "ICANN: Between the Public and the Private—Comments Before Congress," *Berkeley Technology Law Journal* 14, no. 3 (Fall 1999): 1071-93.

[33] Memorandum of Understanding Between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers, http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm, 25 November 1998. This agreement has since been amended a number of times. The amendments are available at http://www.ntia.doc.gov/ntiahome/domainname/icann.htm.

[34] Contract Between ICANN and the United States Government for Performance of the IANA Function, http://www.icann.org/general/iana-contract-09feb00.htm, 9 February 2000.

[35] Letter from J. Beckwith Burr, Acting Associate Administrator for International Affairs, National Telecommunications and Information Administration, U.S. Department of Commerce, to David Graves, Director, Business Affairs, Network Solutions, Inc., http://www.ntia.doc.gov/ntiahome/domainname/icannnewco.htm, 26 February 1999.

[36] Froomkin, "Wrong Turn in Cyberspace," 70.

[37] Some ICANN critics have pointed out that this formal structure existed merely on paper. It, however, did not exist in reality. In December 2002, ICANN reformed its organizational structure. Under the new structure, ICANN will have a volunteer board of directors that include 15 voting and six non-voting members, all of which will be selected by the three supporting organizations and ICANN's Nominating Committee. The Nominating Committee is composed of members selected by the supporting organizations, the advisory committees, and the board of directors. The three supporting organizations include the Generic Domain Name Supporting Organization (GNSO), the Address Supporting Organization (ASO), and the Country Code Domain Name Supporting Organization (CCNSO). In addition, ICANN is supported by the Governmental Advisory Committee, the At-Large Advisory Committee, the DNS Root Server System Advisory Committee, the Security and Stability Advisory Committee, and the Technical Liaison Group. *See* ICANN, ICANN and the Global Internet, http://www.itu.int/itudoc/itu-t/workshop/cctld/024r1.html, 25 February 2003; *see also* ICANN, ICANN and Reform, http://www.itu.int/itudoc/itu-t/workshop/cctld/025r1.html, 25 February 2003.

[38] ICANN, ICANN and the Global Internet, 4.

[39] IANA, ICP-1: Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation), http://www.icann.org/icp/icp-1.htm, May 1999. Although some commentators refer to ICP-1 as the "Internet Coordination Policy," the document stands for "ICANN Corporate Policy." *See* ICANN, Proposal to the U.S. Government to Perform the IANA Function, http://www.icann.org/general/iana-proposal-02feb00.htm, 2 February 2000.

---

[40] GAC, ICANN, Principles for Delegation and Administration of ccTLDs Presented by Governmental Advisory Committee, http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm, 23 February 2000 [hereinafter GAC Principles].

[41] Mueller, *Ruling the Root*, 206. As the *GAC Principles* noted:

> The relevant government or public authority ultimately represents the interests of the people of the country or territory for which the ccTLD has been delegated. Accordingly, the role of the relevant government or public authority is to ensure that the ccTLD is being administered in the public interest, whilst taking into consideration issues of public policy and relevant law and regulation.

GAC Principles § 5.1.

[42] In 1997, Zaire changed its name to the Democratic Republic of the Congo. It has since occupied the .cd name space. *See* IANA, Report on Deletion of the .zr Top-Level Domain, http://www.iana.org/reports/zr-report-20jun01.htm, 20 June 2001.

[43] Documents concerning the redelegation of these ccTLDs are available at http://www.iana.org/reports.

[44] Notably, ICANN did not enter into an agreement with Neustar, the .us ccTLD manager. *See* Arx & Hagen, "Sovereign Domains," ¶ 37.

[45] ICANN, ccTLD Resource Materials, http://www.icann.org/cctlds, *last updated* 13 January 2003.

[46] See Model ccTLD Sponsorship Agreement—Triangular Situation (Initial Version), http://www.icann.org/cctlds/model-tscsa-02sep01.htm, 2 September 2001; *see also* Arx & Hagen, "Sovereign Domains," ¶¶ 32-34 (discussing ICANN's contractual powers).

[47] Stuart Lynn, ICANN, President's Report: ICANN—The Case for Reform, http://www.icann.org/general/lynn-reform-proposal-24feb02.htm, 24 February 2002.

[48] *See* ICANN, ICANN and the Global Internet; ICANN, ICANN and Reform.

[49] Cukier, "Eminent Domain," 2.

[50] See Michael A. Geist, ccTLD Governance Project, http://www.itu.int/itudoc/itu-t/workshop/cctld/cctld006.html, 10 December 2002.

[51] Arx & Hagen, "Sovereign Domains," ¶ 21.

[52] Cukier, "Eminent Domain," 1. As Milton Mueller explained:

> Just as the physical world was divided up into mutually exclusive territories controlled by sovereign governments, so could the name space be. Country codes were the most direct and obvious point of entry for this kind of thinking. If national governments could gain control over the assignment of their own country code, they could translate their geographic jurisdictions into cyberspace and gain a significant role for themselves in Internet governance.

Mueller, *Ruling the Root*, 205.

[53] Cukier, "Eminent Domain," 1.

[54] Kate Mackenzie, "Tuvalu's .tv Yields $88m," *Australian*, 29 January 2002, 27.

[55] See, e.g., Akash Kapur, "United Nations vs. ICANN: One ccTLD at a Time," CircleID, http://www.circleid.com/articles/2564.asp, 29 January 2003.

[56] In March, the government of South Africa introduced the Electronic Communications and Transactions Bill, which proposed to set up a new domain name authority within South Africa with board members chosen by the Minister of Communications. *See* Arx & Hagen, "Sovereign Domains," ¶ 23; Geist, ccTLD Governance Project.

[57] Letter from Richard Alston, Senator and Minister for Communications, Information Technology and the Arts, Australia, to M. Stuart Lynn, President and CEO, ICANN, http://www.iana.org/cctld/au/alston-to-lynn-04jul01.htm, 4 July 2001.

[58] Cukier, "Eminent Domain," 6; *see also id.* at 7-9 (outlining a plan to nationalize ccTLDs).

[59] See generally Roger A. Cunningham, William B. Stoebuck & Dale A. Whitman, *The Law of Real Property* (St. Paul, Minn: West Publishing, 2d. ed., 1993): 505-12; *Nichols on Eminent Domain* (New York: Matthew Bender, Perm. ed., 2003).

[60] Cukier, "Eminent Domain," 6.

[61] See Arx & Hagen, "Sovereign Domains," ¶ 83 (advocating the acknowledgment by national governments that each nation is authoritative for its respective ccTLD and the introduction of a peer-to-peer protocol into the DNS). Theoretically, any computers can resolve domain names by querying different name servers that point to different root servers. Alternative top-level domains and alternative root servers indeed exist. Nonetheless, very few computers look up domain names using alternative root servers, and the vast majority rely on the set of 13 "legacy" root servers to resolve domain names. *See* Mueller, *Ruling the Root*, 53-55; Weinberg, "ICANN and the Problem of Legitimacy," 197-98.

---

[62] The *WIPO ccTLD Best Practices for the Prevention and Resolution of Property Disputes* is available at http://ecommerce.wipo.int/domains/cctlds/bestpractices/index.html. The document is available in Arabic, Chinese, English, French, Spanish, and Russian.

[63] The Uniform Domain Name Dispute Resolution Policy is available at http://www.icann.org/dndr/udrp/policy.htm.

[64] Under the UDRP, each registrant agrees to participate in a mandatory administrative proceeding when a third party complains to a dispute resolution service provider. The person bringing the case must then prove not only that the registrant's domain name is identical, or confusingly similar to a trademark, or service mark, in which the complainant has rights, but also that the person who registered the domain has no rights, or legitimate interests, to the domain name and the domain name has been registered *and* is being used in bad faith.

[65] Among the criticisms are the selection and composition of the dispute resolution panel, the failure to provide adequate time for a domain name registrant to reply to a complaint, the failure to ensure that the registrant has received actual notice of the complaint, and the registrant's limited access to courts for review when the dispute resolution panel decides against a party. For criticisms of the UDRP, see generally Michael Geist, "Fair.Com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP," *Brooklyn Journal of International Law* 27, no. 3 (2002): 903-37; A. Michael Froomkin, "ICANN's 'Uniform Dispute Resolution Policy'—Causes and (Partial) Cures," *Brooklyn Law Review* 67, no. 3 (spring 2002): 605-718. *See also* Laurence R. Helfer & Graeme B. Dinwoodie, "Designing Non-National Systems: The Case of the Uniform Domain Name Dispute Resolution Policy," *William and Mary Law Review* 43, no. 1 (October 2001): 141-274; Froomkin, "Wrong Turn in Cyberspace"; Milton Mueller, Rough Justice: An Analysis of ICANN's Uniform Dispute Resolution Policy, http://www.acm.org/usacm/IG/roughjustice.pdf, *last visited* 2 March 2003.

[66] CENTR is an international association of ccTLD registries. CENTR provides a forum to discuss policy matters concerning ccTLD registries, acts as a channel of communication to Internet governing bodies and related organizations, and promotes the interests of not-for-profit ccTLDs by lobbying on their behalf. Although CENTR has a European focus, full membership is open to all ccTLD registries. Among the non-European members include CIRA (for Canada), IPM (for Iran), ISOC-IL (for Israel), and the Palestinian Registry. The Web site of CENTR is available at http://www.centr.org.

[67] Examples of these powerful ccTLD managers include Nominet UK (.uk) and DENIC (.de), each of which have millions of registrations. See Michael Geist, "Governments Hold Reins in Those National Domains," *Toronto Star*, 10 March 2003, 3(D).