The Richmond Journal of Law and Technology

Volume IX, Issue 1,
Fall 2002

SOVEREIGN DOMAINS

A Declaration of Independence of ccTLDs from Foreign Control

By Kim G. von Arx and Gregory R. Hagen*

1. INTRODUCTION

In the year 2000, the Government Advisory Committee ("GAC") of the Internet Corporation for Assigned Names and Numbers ("ICANN") passed a set of principles that essentially claimed national sovereignty over country code top-level domains ("ccTLD"s) such as .us, .ca, .uk and .au.[1] Shortly thereafter, ICANN redelegated several ccTLDs in accordance with new GAC principles. Despite the outcry accompanying the passage of these principles[2] and ICANN's self-professed adherence thereto, the entire exercise could easily be criticized as merely symbolic because of the overriding power of ICANN in the operation of the Domain Name System ("DNS"). Indeed, Stuart Lynn, ICANN's current president, summed up the lack of power that ccTLDs have within the governance structure of the Internet when he opined that "ICANN could, in theory, recommend that a particular ccTLD be redelegated to a cooperating administrator. If the United States government accepted that recommendation, non-cooperating ccTLD administrators would be replaced."[3]

As Lynn's remarks suggest, ICANN's power to redelegate domains is subject to the approval of the United States government; in particular to the Department of Commerce ("DoC"). The public face of the DoC may be ICANN, but the DoC retains the ultimate power over domains. The power of the DoC resides in its control over the information that is contained in the A root name server, at the apex of the DNS, which acts as an authority to the world's internet users regarding which top-level domain ("TLD") name servers are authoritative for a particular TLD.

The DoC has a strong enforcement power because it has a domain registrar's or registrant's virtual life in its hands. It has the power to enforce the decision by evicting

anyone from his or her cyberspace domain. As Post quite aptly stated, "the domain name system . . . [is] the one place where enforceable Internet policy can be promulgated without any of the messy enforcement and jurisdictional problems that bedevil ordinary law-making exercises on the Net."[4] Put another way, the hierarchical architecture of the DNS is sufficient to endow those who control the A root with the power to make and enforce law and policy regarding domain names. Equally troubling, the control over the A root also invites economic, political, and social pressures that inevitably force ICANN to go beyond its delegated powers of technical management of the system to include derivative powers.[5] Such derivative powers may be applied to areas considered to be those reserved to national sovereigns, including matters of registry regulation, name policy, electronic surveillance, national defense, and critical infrastructure.

Despite a few early demands that the U.S. withdraw from control of the DNS, and the later demands and claims of GAC, curiously, none of the individual 243 countries with delegated ccTLDs have complained forcefully about the lack of sovereignty over their own ccTLD, nor of any of the general policy implications. This lapse is peculiar since nations desperately guard sovereignty over their physical domains against advancing globalization. Italian prime minister Silvio Berlusconi, for example, in his speech to the Italian parliament, reassured the nation as well as the European Union ("EU"), of Italy's solid commitment to the EU. He made it clear, however, that "[n]obody, I repeat nobody, can think they can put us under their control or worse still treat us as a subject with limited sovereignty."[6]

ICANN originated in part from the recognition of the globalization of the Internet as a communications network. Because of the increasingly global scale of the Internet,

the U.S. Government desired to rid itself of the task of operating the DNS and also wanted to obtain international *input* into the technical management of the DNS.. At the same time, it wanted to maintain control over critical DNS policies through a reservation of control of the A root. The solution that was arrived at was to privatize the management of the DNS by placing management in ICANN, a private California, non-profit corporation, but controlling ICANN through a contract with the U.S. DoC.

Thus, from its inception, ICANN was intended to preclude the participation of "national governments acting as sovereigns… [or] intergovernmental organizations acting as representative of governments."[7] Yet, the formation of ICANN to manage the DNS appeared to be tempered by the United States' recognition of the need for *its* sovereignty over the DNS due to its perceived implications for critical United States national policy. Thus, while there was an intention to "internationalize" the technical management of the DNS, the United States' concern for its sovereign control over the DNS precluded sharing control of the A root with other sovereigns, allowing it to become a means of exerting extraterritorial influence over foreign nations.

As Barber has pointed out, one aspect of globalization – privatization – has had the effect of placing transnational organizations outside the regulatory environment of the nation state.[8] On his view, such organizations are rogue institutions operating in an anarchic realm devoid of significant regulation, unprepared to enter into a form of international civil society.[9] Similarly, ICANN has been placed in the curious position that its conduct is too tightly controlled by the DoC, on the one hand, and not accountable to nation states and the U.S. public on the other. In this latter regard, ICANN's actions

have been roundly criticized as unfair,[10] anticompetitive[11] and its status as a private entity illegitimate.[12]

The source of control over ICANN is control over the A root. Thus, the ultimate problem with DNS, on our account, is precisely that the United States has never *shared* control over the A root with national sovereigns. Its influence over the A root server system and ICANN is too strong and the influence over the DNS by other nations is too weak. One aspect of this paper is to apply a political solution - analogous to the political solution to the problem of globalization - to the management of the DNS. The political solution is to recognize a nation's sovereignty over its ccTLD and to provide an international regulatory framework within which nations can recognize other national ccTLDs and develop related policies in a multilateral environment. A second aspect of the paper is to mirror the political solution in computer architecture. Consequently, we provide a technological solution whereby such (peer-to-peer) name coordination occurs. Such sharing of control of the DNS will increase the global stability in the DNS and related policies and assist in internationalizing democratic values through a multilateral approach to coordinating the DNS rather than a unilateral approach.

While it is possible to overstate the risks associated with foreign control over country domains, the existing system highlights a tension between national interests and the existence of a network architecture which is currently beyond the ability of national governments - other than the U.S. - to control. The foreign control of the A root exerts subtle pressures on nations, other than the United States, and reveals the dangers of letting technology drive policy rather than the converse. Yet nations appear, on the whole, to be content to let the technology of the DNS influence domestic law and

policies. The fundamental aim of this paper, then, is to describe a political solution to DNS management and outline a new DNS architecture that meets the political needs of sovereign countries to make and enforce domestic laws and policies.

This paper will briefly introduce DNS and also introduce the problem of United States control over the DNS. Next, it will describe the risks associated with a system where national domains are controlled by a foreign authority: namely, diminished sovereignty and a consequent lack of local control over name policy, registry affairs, e-commerce, national defense, and critical infrastructure. Finally, it suggests both a political and a technical solution that makes each country an authority over its own ccTLD and allows the countries to operate as a peer with other countries.

2. THE DOMAIN NAME SYSTEM

The existing naming scheme is hierarchical. Internet address names consist of alphanumeric strings separated by a dot (•), e.g., law.richmond.edu, and are read from left (the lower level of the domain) to right (the higher level of the domain). Theoretically, there is a highest-level domain at the apex of the domain name space, the "root domain," which is usually left unnamed, under which all domains fall.

There are 258 top-level domains ("TLDs"), which are the highest level of named domains, i.e., the part of the address to the extreme right. There are three types of TLDs. One is the generic TLD (gTLD)[13] such as .com, .org, .net, and .mil. The second one is the country code TLD (ccTLD)[14] such as .ca (Canada), .de (Germany), .uk (United Kingdom), .tv (Tivoli), .ch (Switzerland), .au (Australia), and .jp (Japan). Finally, there

is one infrastructure TLD (iTLD)[15] called .arpa. ccTLDs are perceived as being connected to a specific territory or country whereas gTLDs are global and generally not associated with any territory or country. The infrastructure top-level domain ("iTLD") is the Address and Routing Parameter Area domain and is used solely for Internet infrastructure purposes; therefore, it does not affect or concern the normal user in any way.

While the architecture of the DNS is becoming common knowledge, a brief review is helpful as background to our main thesis.[16] Each computer located on the Internet is assigned an Internet Protocol ("IP") address for data packet delivery. Many computers, or hosts, that are connected to the Internet are also assigned an alphanumeric name such as "icann.org." This name, however, is not required by the network software, but is used for human mnemonic convenience and to provide for stability of services, such as e-mail, when there is a change of host. To the network, however, "icann.org" is meaningless until it is translated into a numerical IP address. Name resolution is carried out by the DNS, a distributed naming system comprised of a huge list of computer names and their corresponding numerical IP addresses.

When a domain name is entered into the location box of an Internet browser, a local DNS resolver, a small piece of client software, first contacts a name server close to the Internet surfer to determine the website's IP address. Generally, the local ISP name server is able to supply the IP address associated with the domain name. If the local DNS server does not contain the needed information, then it will forward the request to the A root name server controlled by ICANN. This A root name server contains the IP address of all the authoritative name servers for TLDs in a file, the A root zone file. This A root

name server will return the information about the location of the authoritative name server for the requested domain name.

In fact, there is no single unique root name server. There are thirteen root name servers (which are assigned letters from A – M).[17] Only one of them, the so-called A root, contains the "original" root zone file. The A root, the primary server, resolves queries by referring the inquiring computers to the Internet address of the computer that has the authoritative list of the registered domain names in the relevant TLD. This single root zone file is made available to the twelve other root servers, the secondary root servers. Nine of the secondary servers are also physically located in the U.S., seven of which are owned by the United States government. The three remaining secondary servers, the only ones outside of the United States, are located in the United Kingdom, Japan, and Sweden.[18]

The sharing of control over the A root suggested in this paper would amount to "splitting" the root in the sense of defying the authority of the A root. In the past, there were concerns that secondary root servers could split, endangering internet stability. It has been argued, however, that, as long as the United States government retains control of the A root, the probability that any of the other secondary root servers would choose to split, i.e., that they would no longer regard the A root as authoritative, is very remote.[19] The reasons proffered are as follows. First, as discussed above, eight of the legacy root servers (including the A root) are owned by the United States government and two more are within United States' territory. Only three root servers are outside the United States' jurisdiction. Second, the key people involved in Internet management have an aversion to a split root, and as such there is no significantly powerful push for splitting the root.

Third, it has been said that "the ur-lord of the DNS, the late Jon Postel [the "father" of the Internet], apparently unsuccessfully tried to redirect the root from the 'A' server and was intimidated into withdrawing the attempt. If Postel could not do it, it is unlikely that others could today."[20] Nevertheless, we propose a method whereby control over the ccTLDs is shared amongst nations.

3. DoC's CONTRACTUAL CONTROL OF ICANN

DoC controls ICANN through a contractual framework underpinned by the DoC control of the A root domain server. DoC control of the A root came about because the U.S. government traditionally controlled the DNS as a private service and funded its creation and operation. However, in a directive entitled "A Framework for Global Electronic Commerce," the Clinton administration proposed a process that would lead to the "privatization" of the DNS.[21] The directive focused upon the commercial value of the Internet and set forth principles to guide government support for the development of e-commerce. In June of 1998, the U.S. issued the famous DNS White Paper entitled "Management of Internet Names and Addresses."[22] The DNS White Paper suggested the delegation of DNS supervision to a private entity identified in the paper as "NewCo."[23]

Fortuitously, a new corporation, ICANN, was soon incorporated and the U.S. duly recognized it as the "NewCo" described in the DNS White Paper. The contractual framework of the relationship between ICANN and DoC is based upon four contractual pillars:[24] (1) the contract between DoC and ICANN and DoC and NSI/VeriSign requiring NSI/Verisign to obtain written approval from DoC before modifying the A

root;[25] (2) the Memorandum of Understanding between DoC and ICANN providing that ICANN manages the DNS on an experimental basis, that DoC retains ultimate oversight over the DNS, and that both entities shall cooperate; [26] (3) a Cooperative Research and Development Agreement ("CRADA");[27] (4) an unusual no-cost, no-bid 'procurement' contract for the 'IANA [Internet Assigned Numbers Authority] function.'[28] In addition to the contractual framework, ICANN will only be able to operate the DNS as long as DoC recognizes it as the "NewCo" described in the DNS White Paper.

In regard to the Memorandum of Understanding, the original and all subsequent extensions provide for DoC's power to terminate the agreement on 120 days notice. Also, the major contracts between DoC and ICANN require annual or semi-annual renewals, and as such DoC has the power to pressure ICANN into submission by threatening transfer of powers to another body.[29]

4. NATIONAL GOVERNMENTS' ROLE IN THE DNS

Technically, the ccTLDs are subdomains of the "root domain" created by the U.S. government and "contained" in the root zone file. Despite the U.S. reservation of technical control over the A root, the U.S. government states that "[n]ational governments now have, and will continue to have, authority to manage or establish policy for their own ccTLDs,"[30] thereby attempting to downplay the influence that the U.S. may indirectly have over the policies of nations foreign to the U.S. At the same time, the U.S. maintained that national governments and intergovernmental organizations should not directly manage Internet names and addresses.[31] On this account, ICANN was intended

to be a purely technical coordinating body, whereas national governments would continue to control national policies.

In spite of the fact that ccTLDs are subdomains of the root domain, countries are increasingly associating their ccTLD with their respective country. Certain ccTLD registries, such as Canada and the U.S., require a domestic presence for a registrant to obtain a ccTLD, thereby creating an association between the country and the registrant. Not surprisingly, a recent report prepared for the Canadian Registry for the .ca ccTLD ("CIRA"), concluded that positive attitudes toward and preferences for dot-ca generally lie in its great emotional and patriotic appeal as the domain "by and for Canadians."[32] As such, marketing and branding initiatives for the dot-ca domain should largely play on the emotional and patriotic appeal of the dot-ca domain.[33]

According to a recent survey by Market Research commissioned by CIRA 75% of Canadians believe .ca means Canada, 73% attribute .ca websites to Canadian organizations and companies, and 90% believe it is important to have the .ca domain as a resource for Canadians.[34] Some countries and registries view their ccTLD as a national resource, comparable to the treatment of the electromagnetic spectrum in broadcasting. For example, Canada described its .ca as "a key public resource, helping to promote the development of electronic commerce in Canada and important to our country's future social and economic development."[35] The .us registry called its ccTLD a "national resource."[36] The Commission of the European Union in its Working Paper regarding the creation of the .eu TLD suggests that the EU requires "ownership" of the TLD in order to exercise its overseeing powers over the domain.[37]

Some countries have claimed that they are national authorities over their ccTLDs. For example, the EU noted that it appears to be the competent 'public authority' for the purposes of the .eu TLD, and should be recognised as such by ICANN.[38] Australia confirmed its authority over .au during the redelegation of .au, when it said that "as a last resort the Australian Government could invoke legislation relating to the self-regulation of the domain name system."[39] South Africa took a sweeping step in affirming control over its own .za ccTLD when it promulgated its *Electronic Communications and Transactions Bill*[40] on March 1, 2002. Chapter X of the Bill in essence de-privatized the ccTLD and established a juristic person, the .za domain authority.[41] In the United Kingdom, Nominet UK, a private body with no initial government involvement, attracted government interest as early as 2000. Since then, "Nominet has been in regular contact with UK Government departments, who increasingly recognise the Domain Name System as a critical part of the countries commercial infrastructure."[42]

Concerns over national sovereignty culminated in the issuance of a communiqué by GAC establishing principles of delegation and redelegation of ccTLDs.[43] These principles established a set of correspondence that must occur in order for a valid redelegation to take place. In its communiqué, "[t]he GAC also reaffirmed that the delegation of a ccTLD Registry is subject to the ultimate authority of the relevant public authority or government. The GAC discussed the development of best practices for the administration of ccTLDs and agreed to continue this discussion."[44] In the earlier ICP-1, the role of national government had been less influential than that accorded by GAC in the delegation and redelegation process: "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."[45]

Despite the criticisms that have been leveled at ICANN regarding its management of the DNS, there has been little critical comment on the U.S. DoC control over the A root server system. While Stuart Lynn's *President's Report: ICANN – The Case for Reform* noted that "if ICANN comes to be seen … as simply a tool of the US Government, it will no longer have any hope of accomplishing its original mission," [46] this point has not spurred any widely agreed-upon solution. Neither the *Blueprint for Reform*,[47] *The Heathrow Declaration*,[48] the New.net Proposal[49] nor John Perry Barlow's *Accra Manifesto*, [50] substantially criticize the U.S. stronghold over the A root nor the hierarchical architecture which undergirds such control. Moreover, Barlow, the author of the well-known *Declaration of the Independence of Cyberspace*, [51] affirms conventional wisdom that the current control structure of the root servers should remain intact. Barlow remarks in his proposal that "[t]he current structure of the root servers . . . has the servers distributed between government, commercial, academic, and non-profit organizations distributed around the world. Such a structure is highly resistant to capture and leads to the robustness and diversity of the Internet."[52] While the *Accra Manifesto* suggests that the physical location of the A root should be taken out of the U.S., the EU has more recently gone further, suggesting that the U.S. government should remove itself from the control over the DNS A root and place it in ICANN's, GAC's or another international body's hands.[53]

Past and recent developments in the U.S. indicate that the U.S. does not have any intention of giving up control over the A root. Last year's terrorist attacks on the U.S.

have increased its recalcitrant refusal to share control of the A root. Andy Müller-Maguhn, Europe's representative of ICANN, is reported to have said:

> It might be that after the Sept. 11 attacks, the U.S. government is not behaving as if it would give any kind of control away. It doesn't look like it at least to me, to be honest, not all. If the United States government never plans to give authority over the [A] root zone files to ICANN. . . . then the issue might be raised . . . if it's just the simulation of an institution where the real power is the United States government.[54]

Carl Auerbach, an ICANN director, seems to agree with Müller-Maguhn.[55] Both refer to remarks made by Nancy Victory, Assistant Secretary of Commerce for Telecommunications and Information as evidence of this recalcitrance, stating that, "[r]egarding the A Root server, the Department of Commerce has no plans to transfer policy control . . . . [W]hen the necessary technical capacity is in place, the department may enter into a management agreement or other legal arrangement with ICANN for operation of the A Root server."[56]

5. THE POWERS OF ICANN AND THE U.S. GOVERNMENT OVER CCTLDs

The power of the U.S. government over ccTLDs stems from the fact that, historically, the DNS was a service of a private network controlled by the U.S. Department of Defense. Despite the "privatization" of the network, a vestige of this control remains in the U.S control over the A root. Even during the period of the U.S. Green Paper[57] and DNS White Paper, [58] the EU, Australia, Canada and others warned that U.S. control over the DNS risked even greater foreign dependency on the U.S. market.[59]

Canada, among others, had associated "privatization" with a divestment of U.S. government authority over the DNS functions.

> It is clearly not enough for the U.S. government to ensure merely that it has "privatized" the DNS -- i.e. divested U.S. government agencies of control of DNS functions and placed control in the hands of a "private sector" group. The White Paper itself set a higher standard than this, and such bare-bones privatization will certainly not meet the needs of most end-user groups or of the international community . . . . Regardless of the particular features of the proposals being debated, the corporate model finally agreed to by the U.S. government should conform to widely supported principles of accountability and transparency.[60]

The United States government in the White Paper responded as follows to the criticisms from the EU and Australia in particular:

> The U.S. Government believes that the Internet is a global medium and that its technical management should fully reflect the global diversity of Internet users. We recognize the need for and fully support mechanisms that would ensure international input into the management of the domain name system. In withdrawing the U.S. Government from DNS management and promoting the establishment of a new, non-governmental entity to manage Internet names and addresses, a key U.S. Government objective has been to ensure that the increasingly global Internet user community has a voice in decisions affecting the Internet's technical management.[61]

Regardless of the fact that ICANN has directors from diverse geographical areas, the international makeup of ICANN remains more apparent than real. National governments are not members of ICANN, and the GAC is solely an advisory group which ICANN may ignore at its pleasure. More importantly, the U.S. retains the power to control the DNS, and retains derivative powers to influence policy and impose obligations and conditions on registries, registrars and domain name registrants. These powers are described below.

A. *Contractual Powers*

ccTLDs were delegated originally by Jon Postel without the benefit of any formal written agreement. However, ICANN is attempting to remedy the lack of a contractual arrangement between ICANN and the various ccTLDs by pressuring ccTLDs to enter into a formal contractual relationship.[62] This contract-based scheme is already becoming the standard method of governing relations between TLD registrars and registries.[63] Until recently, none of the ccTLD registries had been able to arrive at a mutually acceptable agreement with ICANN. However, on October 25, 2001, Australia's auDA became the first to sign a ccTLD sponsorship agreement.[64] Soon thereafter, on February 27, 2002, Japan's JPRS became the second country domain name registry to sign the contract with ICANN.[65] Following that, Barundi and Malawi each signed a Memorandum of Understanding with ICANN under which a ccTLD registry has many of the same obligations as it would under a sponsorship agreement. The sponsorship agreements specify, among other things, that each of the sponsoring organizations contribute financially to "ICANN's cost of operation in accordance with an equitable scale, based on ICANN's total funding requirements (including reserves), developed by ICANN on the basis of consensus . . . ."[66]

Article 6.2 of the sponsorship agreements sets out when ICANN and the sponsoring authority can terminate the agreement. [67] ICANN can unilaterally terminate the agreement if there is a material breach of the contract, or if arbitration shows that the sponsoring organization is in violation of the agreement. [68] Article 6.3 sets out the effect of termination: upon termination, ICANN must, with coordination of the government authority, notify the sponsoring organization of the successor. [69]

Most countries have not signed an agreement with ICANN due to differences of opinion in regard to adequacy of payments, equality in decision-making, representation within the ICANN structure, and various other matters.[70] This, of course, raises the following question: why were the registries of Australia, Japan, Barundi and Malawi the sole registries to sign an agreement with ICANN? The answer can be found in ICANN's power to redelegate ccTLDs, thereby deciding their identity. The implicit threat of redelegation appears to be sufficient to cause a registry to submit to ICANN's contractual demands and, at the very least, to give ICANN a large bargaining advantage in deciding the terms of an agreement.

B. *Redelegation Powers*

i. The Case of the Redelegation of .au, .jp, .bi and .mw

The source of ICANN's power over registrars is its ability to "recommend [to DoC] that a particular ccTLD be redelegated to a cooperating administrator."[71] As already mentioned above, Australia, Japan, Barundi and Malawi are the only countries whose registries have signed a contract with ICANN. In those cases, ICANN appears to use requests for redelegation as leverage to force the proposed new registry to sign a contract in order for it to be delegated authority over the domain. This bargaining device dates back to September 25, 2000, when the ICANN board passed a resolution requiring an agreement prior to delegation of additional ccTLDs. The resolution says at 00.75:

> It is further RESOLVED [00.75] that in view of the state of ongoing discussions directed toward reaching stable and appropriate agreements

> between ICANN and the ccTLD organizations, delegation of additional ccTLDs should be finalized only upon achievement of stable and appropriate agreements between ICANN and the ccTLD organization, in a form approved by the Board.[72]

Although this resolution concerns the creation of *additional* ccTLDs, it is possible that this policy was applied by ICANN to redelegations as well.[73] On this view, each of the registries of Australia, Japan, Malawi and Barundi signed an agreement with ICANN because it was a condition precedent to becoming a ccTLD registry. In the case of the redelegation of .au,[74] ICANN disregarded its own policies contained in RFC 1591[75] and the ICP-1,[76] but followed the GAC Principles.[77] On the other hand, Pitcairn Island (redelegation on February 11, 2000) and Palestine (delegation on March 22, 2000) redelegations occurred prior to the passing of the resolution, and therefore did not require a sponsorship agreement.

However, this explanation does not explain why Canada (redelegated on December 1, 2000) and the United States (redelegated on November 19, 2001) did not sign a sponsorship agreement. In regard to Canada, the answer seems to be that ICANN simply accepted the word of CIRA, the Canadian Internet Registration Authority, that it was willing to execute a formal agreement either before or soon after the redelegation as sufficient. As the "IANA Report on Request for Redelegation of the .ca Top-Level Domain" explains, "CIRA expressed its willingness to enter into a formal, legally binding agreement with ICANN."[78] In light of this commitment, IANA's evaluation of the request was, "CIRA, for its part, has not only entered into the Umbrella Agreement with the Government of Canada but has also committed to enter into an agreement with ICANN providing for operation of the .ca ccTLD in a manner that facilitates ICANN's performance of its global coordination responsibilities."[79]

ii. *The Case of the .us Redelegation and the Power of the DoC*

Perhaps, the most interesting example of the use of the power to redelegate (without any regard to ICANN policies and procedures which other ccTLDs are meticulously forced to follow)[80] is the redelegation of the .us, in that it reveals that the technological control of DoC allows it to influence policy. This transfer was apparently forced upon the existing .us registry, Verisign, and was done without regard for ICANN's policy that required mutual agreement between the old and new registries. Indeed, it was completed "before the completion of the normal IANA requirements [of a formal written agreement]."[81] While the earlier hostile redelegation of .au was done with ICANN's full approval, the redelegation of .us was not. The official, but obscure, explanation can be found in the only existing communication, an announcement from ICANN about the redelegation. It reads: "[t]he United States Government informed ICANN on 16 November 2001 that, because of complexities of U.S. procurement laws, it was not able to extend the existing arrangements with VeriSign nor complete the necessary three-way set of communications among itself, ICANN, and NeuStar."[82]

ICANN admits that if it had not accepted the request from the U.S., it would have, "[created] a situation where the event would have occurred regardless but there would be inconsistent data in the IANA database."[83] The event was the technical redelegation of the authoritative .us name servers. In other words, ICANN had no power to stop the U.S. from changing the data in the A root, technically redelegating the .us domain, so ICANN was forced to change the legal delegee of authority to concur with the change of

information in the A root. Indeed, given ICANN's primary mission focus on technical stability, which requires such consistency, ICANN had to comply with U.S. wishes.[84] ICANN can redelegate against the wishes of .au, but the U.S. can redelegate even against the wishes of ICANN.

C. *Power to Create and Destroy ccTLDs*

The control over the A root provides the power to create or destroy ccTLDs and implies that no country or union of countries can unilaterally force inclusion in the A root. In this area, ICANN has purported to maintain a separation between technical operation and policy by deferring to the ISO 3166-1 country code list. Because IANA cannot assess whether or not particular areas are "countries," the policy set forth in ICP-1 for delegation matters has been to simply refer to the ISO 3166-1 list as an independent and authoritative source of two-letter abbreviations for countries and areas.[85] Therefore, almost all of the ccTLDs are derived from the official ISO standard. Five ccTLDs, however, have been created by ICANN which are not based on the official ISO list, but which can be found on the ISO country code reserve list.[86]

An example of an uncontentious ccTLD removal is the Zaire (.zr) ccTLD. When Zaire changed its name to Democratic Republic of the Congo, ISO removed the .zr code and changed it to .cd, and because of that, ICANN followed suit. While a change of name may not be controversial, the threatened removal of .su, the ccTLD of the former Soviet Union, has provoked controversy.[87] Curiously, while the Soviet Union dissolved, the "virtual Soviet Union" did not concurrently cease to exist and its fate is now in the

hands of the U.S. The converse power of ICANN, to create ccTLDs, has been displayed when it created the .ps ccTLD for Palestine.[88] A more contentious example of the creation of a domain, the .eu, will be discussed in more detail in the next section. The .eu example reveals that ICANN is willing and able to use its bargaining powers to force country domains to adhere to ICANN-imposed contractual terms.

i. *The EU Example*

In 1999, the EU announced its plan to introduce a new ccTLD -- .eu. Then, on February 2, 2000, the Commission issued a Working Paper[89] discussing the creation of a .eu registry. On July 6, 2001, after "Communications" and other formal EU correspondences between the various bodies, the Commission issued a letter to ICANN, reiterating its interest in the .eu domain.[90] Since the .eu code did not currently appear in the ISO 3166-1 table that is referenced in the ICANN ICP-1 policy document on country code delegations, the creation of .eu required a policy action by the ICANN Board.[91] After negotiations and meetings, on September 25, 2000, the ICANN board passed a complex resolution essentially approving the delegation of .eu.[92]

On December 12, 2000, the Commission proposed a regulation, to be adopted by the European Parliament and the Council, which would provide a legal basis for the creation of the .eu registry.[93] Finally, on March 25, 2002, the regulation was adopted and the EU was ready for the creation of its virtual existence in the form of a .eu domain.[94] In response to the proposed regulation, Louis Touton of ICANN declared, "[a]ny inclusion of (dot-eu) in the root zone would require a contract between ICANN and the operator of

the registry."[95] This 'requirement,' as already discussed above, is derived from Resolution 00.75, dated September 25, 2000.[96] Therefore, the EU can regulate, direct, and create as much as it wants, but ICANN can delay the "creation" of .eu in perpetuity and thereby pressure the EU into a sponsorship agreement pursuant to ICANN specifications.[97]

In light of these powers and the unwillingness to give up any control over ccTLDs, the following question arises: what are the associated risks that come with a U.S.-controlled DNS? They include loss of sovereignty over policies relating to domain registry regulation, name policy, privacy, electronic surveillance, national security and critical infrastructure.

6. RISKS FROM FOREIGN CONTROL OF THE ROOT

A. Loss of ccTLDs' Sovereignty

The power of ICANN to threaten a ccTLD with potential redelegation or annihilation provides ICANN with a mechanism to ensure ccTLD compliance with ICANN policies and to force the adoption of ICANN-friendly contractual terms and conditions. These contractual terms and conditions can mandate or influence the types of policies that will be created and enforced by the ccTLD. Thus, to the extent that ccTLD policies impinge on domestic policy, they also diminish the sovereignty of nations to adopt laws independently of ICANN. The current Model ccTLD sponsorship agreement provides that a ccTLD must conform to ICANN policies where they concern "the interoperability of the Delegated ccTLD with other parts of the DNS and Internet;

technical operational capabilities and technical performance of the ccTLD operator; and the obtaining and maintenance of, and public access to, accurate and up-to-date contact information for domain name registrants."[98] Interpreted broadly, "interoperability" and "technical operations capabilities" could impose subtle effects on the regulation of registries, name policy, privacy, critical infrastructure, and national defense in countries foreign to the United States.

B. Registry Regulation

The ability of ICANN to attach conditions to the use of names enables it to control the supply of domain names. ICANN can effectively decide the identity of registries. Generally speaking, foreign nations have simply accepted the United States government's delegation of registry functions to private entities, rather than governments or governmental agencies, without extensive review. This is due, in part, to the recognition that foreign governments have no power to delegate registry functions to themselves, but require the blessing of ICANN. An additional risk is that ICANN will impose terms on the registrars that are not in the national interest of the country associated with the ccTLD. It could also extend its regulatory functions into areas pertaining to relations between registrars and registries, consumer complaints and mergers of registries, further extending its reach into the domestic affairs of foreign nations.[99]

C. Name Policy

The technological control over the A root has enabled ICANN to embark on a program to enlarge rights exceeding those that formerly existed for names. For gTLDs, this occurs directly through the Uniform Dispute Resolution Procedure, which has been viewed as systemically biased toward complainants and trademark interests.[100] On Mueller's view, the problem with this trend is that it is inconsistent with the function of the DNS.[101] Whatever the merits of such criticism, there is the difficulty that national governments no longer have control over domain name policy independently of ICANN.

An example of this phenomenon is the fact that United States trademark law is now, in certain cases, applicable to gTLD domain name registrations throughout the world.[102] A United States court has ruled that it will have *in rem* jurisdiction over a domain name when the applicable registry is located in its jurisdiction, and the registrant is unidentifiable or *in personam* jurisdiction is unavailable, regardless of the fact that the registrar and both disputants are located in a foreign country.[103] Remarkably, the court maintained that one factor for asserting jurisdiction was that the "[p]laintiff may not be able to assert the same rights in Canada, which lacks a body of law equivalent to the ACPA and whose enforcement of its trademark laws cannot extend into the United States."[104] Thus, regardless of whether a registrant has violated trademark law in its domestic jurisdiction, it can now seek the aid of United States courts to apply United States law. United States interests may eventually push for United States trademark law to apply to ccTLDs as well.

D. Electronic Surveillance & Information Transfer

The ability of someone to engage in anonymous transactions on the Internet has been one of its central appeals, as well as a source of its problems. Recently, a bill was introduced in the United States Congress to provide criminal penalties for providing false information when registering a domain name on the Internet.[105] Ensuring the accuracy of registrant information is considered to be necessary, among other reasons, in order to assist law enforcement with the timely investigation and prosecution of illegal activity.[106] Such activity could extend to enforcing laws regarding Internet taxation and copyright infringement.

However, the United States approach may not be the favored approach of other countries that may differ with respect to their views on privacy, surveillance, anonymity policies, and laws, as well as their relation to the need for registrant information in the investigation, prosecution, and enforcement of illegal activities. Control over the A root implies, however, that ICANN can force ccTLDs to ensure that their registration data is accurate and current, and that ICANN has access to such information. In fact, ICANN's Model ccTLD sponsorship agreement already provides that:

> [t]he Sponsoring Organization shall ensure that the zone file and accurate and up-to-date registration data for the Delegated ccTLD is continuously available to ICANN, in a manner which ICANN may from time to time reasonably specify, for purposes of verifying and ensuring the operational stability of the Delegated ccTLD only.[107]

Such an approach may conflict with certain national privacy laws prohibiting transfer of information across borders into states which do not have privacy legislation that the nation of the transferor considers adequate, unless there is an adequate exemption.

E. National Security

The importance of the Internet as a critical infrastructure has become common knowledge. Former United States President Bill Clinton noted: "The United States possesses both the world's strongest military and its largest national economy…. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyberbased information systems."[108] "In addition to 'traditional' weapons of mass destruction, new forms of Strategic Information Warfare (SIW) will be developed and perhaps used as a new form of offensive warfare. SIW involves cyber-attacks against major national command systems and military-related operating systems."[109]

It is often pointed out that since both civilian and military infrastructure in many nations are becoming increasingly dependent on the existence of the Internet, the ability to disrupt an enemy's communication might be a strategic asset.[110] From the point of view of military reasoning, cyberspace is a new *battle space* to which military principles apply on par with land, sea and aerospace.[111] The principle of full spectrum dominance is said to apply to cyberspace. "The label full spectrum dominance implies that US forces are able to conduct prompt, sustained, and synchronized operations with combinations of forces tailored to specific situations and with access to and freedom to operate in all

domains – space, sea, land, air, and information."[112] A number of military exercises, such as Eligible Receiver and Solar Sunrise have demonstrated that attacks on military information infrastructure can be made successfully.[113]

While it seems clear that the Internet itself has become part of the underlying battle space,[114] and subject to being threatened, it is not clear the degree to which control over the A root is also a strategic asset. For example, the degree to which military operations, including the "digitized battlefield,"[115] depend upon use of the DNS is unknown. Are e-mails, for example, encrypted or not, part of the present or future national defense operations? Given that the importance of the DNS is not sufficiently known it is not surprising that control over the DNS would be viewed as critical.

Recently the Energy and Commerce Committee sent a letter to Secretary Donald L. Evans of DoC in response to Lynn's ICANN reform proposal which confirmed that the control over the root is regarded as a threat to national security. The letter said:

> Finally, we want to strongly reiterate our support for continued Department of Commerce control over the so-called "A-root" server. We believe that any assumption of control over that asset by any outside entity would be contrary to the economic and national security interests of the United States.[116]

Similarly, New.net suggests in its proposal to reform ICANN that, "the U.S. Government would be responsible for making all policy decisions regarding the legacy DNS root,"[117] and that "[b]y maintaining control over the legacy DNS root, the United States could be assured that its national interests are protected."[118] This point of view certainly would receive backing from traditional military reasoning which would demand

that the U.S. "[e]stablish and control cyber superiority (or supremacy). Never cede control over the battle space to an adversary."[119] Therefore, on this view, it is unlikely that the U.S. would voluntarily concede power over the DNS.

U.S. control over the DNS may itself be used as a U.S. strategic military advantage as opposed to the target of a threat. For example, the U.S. could have decided not to create a country code for Palestine in view of its apparent support of Israel's interests against Palestinian aspirations for sovereignty. Or it could decide to extend the U.N. embargo against Iraq into cyberspace by deleting the Iraq .iq ccTLD.[120] The more integrated the DNS becomes with "real-world" services, the more control over such services is ceded to whoever controls the DNS.

Of course, if the DNS is vital to the national security of the United States, then parity of reasoning suggests that it is vital to every other country as well. Therefore, the national security arguments that the United States military and governmental officials have advanced favoring U.S. control over the DNS apply equally well to the interests of other nations. To the extent that the control over the root may be a national security concern to the U.S., it is also a concern to every other country with regard, at the very least, to its ccTLD.

F. *Critical Infrastructure*

Critical Infrastructures are systems whose incapacity or destruction would have a debilitating impact on the defense or economic security of a nation. These include: telecommunications, electrical power systems, gas and oil, banking and finance,

transportation, water supply systems, government services and emergency services.[121] The Internet is increasingly becoming a universal platform on which such critical infrastructure depends and is, therefore, itself a critical infrastructure.

A central concern is to ensure that the Internet is protected from threats. The President's Commission on Critical Infrastructure Protection concentrated on threats to the information infrastructure. It noted that:

> Threats to the Internet are of primary concern because we are becoming increasingly dependent on it for communications—including government and military communications—for commerce, for remote control and monitoring of systems, and for a host of other uses; because our ability to understand its full impact on society seems unable thus far to keep up with its explosive growth; and because it is inherently insecure.[122]

Malicious attacks on DNS servers can result in "falsified" DNS responses that divert or hijack traffic to counterfeit web pages and misdirect e-mail.[123] The widespread use of DNS data caches by ISPs and lower-level networks allows attackers to engage in cache poisoning and cache spoofing to accomplish similar results. As a result of these and other deficiencies in the original DNS specification, the Internet Engineering Task Force ("IETF") has been working on a set of security-enhancing tools, known collectively as DNS Security ("DNSSEC").[124] DNSSEC uses public key cryptography to verify the authenticity of DNS data.[125] DNSSEC essentially facilitates a chain of trust starting with the root name servers and proceeding through the hierarchical resolution of a domain name.[126] At each zone in the DNS, the information is electronically signed and, when received by others, the signature of the upper level zone is verified using an associated public encryption key.[127]

There is a more basic security problem. Due to the hierarchical nature of the DNS, the root name server system is the most vulnerable component of the DNS. The

simplest form of attack is an attack on any of the thirteen root domain servers. The recent distributed denial of service attack on the root name servers showed that, although global reachability and packet loss was affected, the network withstood the attack.[128] There is some discrepancy of opinion, however, regarding the degree of resiliency of the root name servers. ICANN claims that, given that the name servers are widely geographically distributed, it is unlikely that all root name servers would be damaged by an attack, environmental crisis or catastrophe.

In terms of load, it has been estimated, given the amount of current traffic each individual root name server receives, that root name service can function with little to no disruption when 40% of the name servers are offline. Therefore, should a significant catastrophe or attack occur, the diversity of location will permit the root name server system to continue operation while the disrupted name servers are restored.[129] Others do not agree. According to Paul Vixie, one of the developers of BIND, "[t]he Internet is very fragile . . . . [I]t would be very easy for an angry teenager with a $300 computer to create almost unlimited pain for anyone on the Internet and not get caught."[130] It has been suggested by the U.S. National Research Council in an exhaustive study that Internet growth rates will soon outstrip the ability of processing speed of root servers to adequately deal with the number of naming requests.[131]

7. DECLARING ccTLD INDEPENDENCE

A. Political Independence

In order to diminish the risks associated with foreign control over ccTLDs, countries need to gain control over their own ccTLD. The solution proposed here differs from solutions that have been formerly proposed. One solution is to include country representation in ICANN on the basis that countries have some form of property interest in ccTLDs. GAC, for example, grounds national interests in the purported fact that ccTLDs are national resources.[132] The flaw in this proposal is that it ignores the U.S. ownership and control over the legacy A root server and the consequent private nature of the DNS.[133] The control of the A root server by DoC entails that neither ICANN itself, nor its members or directors ultimately control ccTLDs. The claim that ccTLDs are public resources ignores the brute fact that ccTLDs are delegated subdomains of a private U.S. government controlled domain space.

Another proposal takes its cue from analogous proposals regarding the problem of privatization in global commerce. On such a view, ICANN's failure[134] is a symptom of a general problem of globalization. Barber puts the general problem as follows:

> The difficulty nation-states have with globalization comes not just from the force of what is happening in the international arena but from ideological developments within nation-states. The push toward privatization is bipartisan. This is not decentralization -- the devolution of power down the democratic public ladder to provinces, municipalities, and neighbourhoods -- but de-democratization, the shifting of concentrated power at the highest levels from public to private hands. Power shifted from authorities that were hierarchical but also public, transparent, and accountable, to authorities that remain hierarchical but are private, opaque, and undemocratic.[135]

On Barber's account, there are two competing solutions to the problems of accountability of international institutions such as ICANN. One is to attempt to

democratize international institutions and markets through the creation of a "transnational civil society."[136] This effort is led by individuals attempting to create a transnational civic space within which international institutions are accountable. The call for the DNS to be operated by the International Telecommunications Union, which is subject to the existing international telecommunications regime, is an example of this type of solution within the context of the DNS.

A second solution recognizes that international institutions, whether the United Nations, International Monetary Fund, World Trade Organization, are the creation of national governments and hence should be controlled by national governments. Barber again puts the latter point well:

> National sovereignty is said to be a dying concept, but it is a long way from dead. Sovereign nations remain the locus of democratic society and the only viable powers capable of opposing, subduing, and civilizing the anarchic forces of the global economy. International civil society, the emerging global alternative to the world markets, needs the active support of sovereign states for its fragile new institutions to have even a modest impact.[137]

Our solution attempts, first, to reassert sovereignty over ccTLDs because national control over individual ccTLDs ensures national participation, accountability and visibility. Secondly, once individual nation states are in control of their own ccTLDs, multilateral negotiations can take place to create a regulatory framework within which individual nations can recognize each others domains. This reassertion of sovereignty over ccTLDs attempts to provide a form of internationalization of the A root called for by the White Paper that would be sensitive to the sovereign interests of the U.S., as well as those of foreign countries, and creates a framework of greater accountability in which technical management of the DNS can operate.

This change of control may be done either with the cooperation of the U.S. government or without it. If it is done with its cooperation, the political nature of the change will be analogous to the patriation of a constitution of a colony. On such a conception, the architecture of the DNS is analogized to the constitutional documents of physical space. [138] On the patriation model, it is mutually agreed by the U.S. and nation states that the *de facto* technological authority of the DoC to decide who is an authoritative national root - and thereby influence policymaking - be shared by modifying the DNS structural hierarchy in favor of national control over ccTLDs.

Alternatively, if the U.S. does not recognize the authority of nations over their own ccTLDs and cooperate in modifying the DNS architecture, then the change of control could be accomplished through a process analogous to the U.S. Declaration of Independence. In that scenario, nations would refuse to recognize the authority of the A root name server. Just as the U.S. Declaration of Independence emerged in a battle over untapped common resources in the "new" world, the struggle over DNS resources is a struggle for resources in the new "cyberworld." The Declaration of Independence asserted that the Colonies of British America be free from control of Britain and form a confederation of states. But in order to achieve a similar freedom for ccTLDs, nations must be freed from the hierarchical technology inherent in the DNS architecture and create a system recognizing national control over ccTLDs.

Such a Declaration of ccTLD Independence may appear to put nations at odds with the apparent U.S. foreign policy of colonizing cyberspace. In fact, however, sharing control of the A root better meets the requirements of U.S. foreign policy as contained in the DNS White Paper than other proposals. According to the White Paper, the creation

of ICANN was an experiment in global governance through the creation of a private entity which would permit international input into the technical coordination of the DNS, while at the same time recognizing the importance of U.S. interests in maintaining its sovereignty over the root. [139] By sharing control over ccTLDs, each country maintains its control over its own ccTLD while divesting a substantial amount of U.S. control over the DNS.

Barber's account of the problems of privatization is remarkably similar to independent critiques of ICANN, by Boyle Froomkin and others, which tends to confirm the present analysis. While one of ICANN's main rationales was supposed to be an increase in accountability,[140] a consequence of the privatization of the DNS is that the state can use "*privatized enforcement* and state-backed technologies to evade some of the practical and constitutional restraints on the exercise of legal power over the Internet."[141]

Moreover, a government can achieve regulatory ends, often without suffering the political consequences that the same ends, pursued directly, would yield. In other words, the state can indirectly govern, and impose its agenda upon by simply employing private parties to do indirectly that which it is forbidden to accomplish directly.[142] It is in this respect that Froomkin has argued that the delegation of power by the U.S. government to ICANN to manage the DNS was illegal.[143] Boyle has questioned the survival of the doctrine in modern times, but has, nonetheless, called for a digital non-delegation doctrine prohibiting certain types of government delegation of power.[144]

Following Foucault, Boyle noticed that the method of regulation by code on the Internet is a form of discipline.[145] On this view, regulation by the architecture of DNS makes such regulation *invisible* and *automatic*. It provides a method of individuating

registrants and encoding them into a network whose behaviour can thereafter be monitored. Boyle notes that if we understand the methods of "surveillance . . . which presupposes a tightly knit grid of material coercion" rather than an overbearing sovereign who can rule only as far as his/her sword reaches, then we might understand the indirect and hidden regulability of the Internet.[146] This hidden regulability can also allow non-state actors to achieve influence through influence over the "grid of coercion." For example, the recent threat by ICANN to terminate Verisign's contract to manage the .com because it is not ensuring the accuracy of registrant information[147] is grounded in the concern of trademark interests, and others, to be able to know the identity of domain name holders for litigation purposes.

Unfortunately, it is beyond the scope of this paper (and the expertise of the authors) to provide a full technical explanation of how to achieve technical independence. However, a very short summary should suffice for the purposes of this paper.

B. Technical Independence

The ability to declare independence of ccTLDs hinges on the fact that it is possible to create alternate roots.[148] More correctly, alternate roots already exist and operate without disrupting the stability of the DNS. It has been maintained that alternate roots "provide an important check on abuses or bad economic policies of the dominant root operator."[149] As Mueller has further argued, banning alternative roots is "inadvisable [or it] may not even be possible."[150] These inclusive alternate roots have the information from the A root and alternative TLDs. [151]

Ironically, the source of the authority of the A root server and those who control it is the fact that it is accepted as an authority by the Internet community. In particular, it is accepted as an authority by major ISPs throughout the world. Those ISPs and their name servers are in turn recognized as authoritative by individual computer users. In order to achieve independence, then, there is a need to renounce the authority of ICANN and the A root server. In fact, the U.S. government power over the DNS via its A root will and can continue only as long as the other twelve Secondary Root Servers copy and rely on the A root.

One method of attaining independence begins with "enlarging the root." In order to accomplish this, it should be recognized that the legacy DNS is not physically hierarchical. There is a unique root only in a logical or virtual sense.[152] For, while the A root server is technically a root for those servers that accept it as authoritative, other servers accept one or more of the other thirteen root servers as authoritative. Thus, individual nations can take it upon themselves to enlarge the root by creating an additional authoritative root server. The national government could then require domestic ISPs to recognize the national root as authoritative. Essentially, instead of relying on the idea of an authoritative root which is controlled by an independent entity, each country retains authority for its own domain. In this sense, the national government would have control over its own root. As mentioned, however, present technical limitations limit the root to thirteen servers. The issue that then arises is whether the national root will recognize the A root as authoritative.

A second step involves splitting the root.[153] This step requires that the national authority no longer recognizes the A root as an authority. Instead national roots may

directly recognize other national roots as authoritative peers. This peer-to-peer approach can be extended to other name servers as well. Currently, if a local name server cannot provide the answer to a query, such as donaldduck.com, the query is sent to the root which returns the address of the authoritative server for the .com domain. On a peer – to - peer account, each name server would point to the 243 ccTLD root servers as authoritative for ccTLDs and the thirteen Legacy root servers (or the fourteen gTLD servers) as authoritative for gTLDs. Therefore, if someone in Switzerland looked for www.google.de, the resolver would query its local name server as to where it should go and, failing a response, the local name server would direct the query to the German .de root server which then would resolve the query.[154] Apparently, major ISPs already cache the addresses of the TLD registries in order to avoid accessing the root as often as without such caching.[155] We wish to extend this system to national roots as well.[156]

This proposal to share the A root assists with the problem of lessening single points of failure and increases the scalability of the DNS. Two common methods are used to increase the scale of DNS services: caching and server replication.[157] Caching is a technique allowing frequently accessed names to be cached on a local name server. Replication is a method of distributing databases to multiple name servers. For example, replication could allow for a root server to provide several ccTLD (such as .uk, .ca, or .de) name server addresses. Likewise, a name server could provide for the addresses of several root servers. Unfortunately, the names and address of root servers under the current DNS protocol must fit into a single 512–byte packet and this limits the number of root servers to thirteen.[158] After reaching its maximum number of servers, the only method to increase the load of the root is to boost the capacity and processing power of

the root servers. It appears that there must be an effort to enlarge the number of root servers in order to cope with increased DNS queries.

Perhaps a form of a single physical international root listing all the addresses of authoritative ccTLD servers would emerge, but such a root would not likely be controlled by a single country and would not be authoritative. For example, such a root may be a database with shared access rights according to which each country is able to exclusively manage its information regarding the authoritative ccTLD address. This method of a p2p-based DNS for ccTLDs would allow each country a choice whether to participate or not.[159] A non-participating country would continue to recognize the legacy root.

8. CONCLUSION

This paper has argued that the United States possesses significant powers over the DNS because of its control over the A root. This power is due to the fact that the DNS is hierarchical in its operation and that Internet users, including individuals, secondary roots, registries, and ISPs accept the authority of the U.S. over the A root. With this control over the DNS come risks, for countries and registries alike, of increasing extraterritorial influence over domestic policies. These risks reveal the subtle political influences that technology, and those who control it, have over domestic laws and policies.

Emerging national concerns of sovereignty over their own ccTLDs have not been met by the privatization of the DSN. Placing the management of the DNS in ICANN's hands has further decreased the ability of most nations to control domestic policies

affected by the DNS. In order to acquire greater control of the DNS, nations must refuse to recognize the authority of ICANN and the A root server. Instead, the authority over the A root should be shared by a mutual acknowledgment that nations are authoritative for their respective ccTLDs. Such sharing will require increasing the root server system to include national DNS roots and the introduction of a peer-to-peer protocol into the DNS.

On this approach, multilateral collaboration is required to create a new DNS political framework and computer architecture, including protocols, standards, and uniform policies within which mutual recognition of national ccTLD authorities can exist. Such collaboration would ensure that an international DNS policy organization or framework would be accountable to sovereign nations. Sovereign domains would ensure that the power over national policy and law is retained by the country itself and not invisibly housed in technology controlled by a foreign entity.

---

[*] Kim G. von Arx is Legal Counsel to the Canadian Internet Registration Authority (www.cira.ca) and Gregory R. Hagen is Replacement Assistant Professor, Faculty of Law, University of Ottawa (www.uottawa.ca). The opinions expressed herein are personal and not necessarily those of their respective employers. This paper is a substantially revised version of a paper originally submitted in partial fulfillment of the University of Ottawa LLM (concentration in law and technology).

[1] Governmental Advisory Committee, ICANN, *Principles for Delegation and Administration of ccTLDs*, *at* http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm (Feb. 23, 2000).

[2] *See* David G. Post, *The Great Internet Give-Away?*, *at* http://www.temple.edu/lawschool/dpost/icann/ccTLD.html (Mar. 2, 2000); Milton L. Mueller, *Governments and Country Names: ICANN's Transformation into an Intergovernmental Regime*, *at* http://istweb.syr.edu/~mueller/gacnames.pdf (last visited Sept. 19, 2002) (presenting the paper at PCT 2002 Conference in Honolulu, Hawaii and critiquing an increasing international involvement in the DNS).

[3] M. Stuart Lynn, *President's Report: ICANN – The Case for Reform*, *at* http://www.icann.org/general/lynn-reform-proposal-24feb02.htm (Feb. 24, 2002).

[4] David G. Post, *Governing Cyberspace, or Where is James Madison When We Need Him?*, *at* http://www.temple.edu/lawschool/dpost/icann/comment1.html (June 1998) (referring to David G. Post, *Cyberspace's Constitutional Moment*, THE AMERICAN LAWYER (Nov. 1999), *available at* http://www.temple.edu/lawschool/dpost/DNSGovernance.htm).

[5] *Hearing Before the Senate Comm. on Commerce, Sci., and Transp., Subcomm. on Sci., Tech., and Space*, *at* http://www.icann.org/correspondence/lynn-testimony-12jun02.htm (June 12, 2002) (statement of M. Stuart Lynn, President and Chief Executive Officer, ICANN).

[6] BBC News, *Berlusconi Says Italy Committed to Europe, at* http://news.bbc.uk/1/hi/world/europe/1760325.stm (last visited Jan. 14, 2002).
[7] Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (proposed Feb. 20, 1998), *available at* http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm (a statement of policy issued by the U.S. Dep't of Commerce, National Telecommunications and Information Administration) (Jan. 14, 2002).
[8] Benjamin R. Barber, *Globalizing Democracy*, 11 AMERICAN PROSPECT ONLINE 20 (Sept. 11, 2000), *at* http://www.prospect.org/print/V11/20/barber-b.html (last visited Sept. 19, 2002);
see also Alejandro Colás, *The Promises of International Civil Society: Global Governance, Cosmopolitan Democracy and the End of Sovereignty?*, *at* http://www.theglobalsite.ac.uk/press/107colas.pdf (Sept. 19, 2002) (discussing the notion of an "international civil society").
[9] *Id.*
[10] *See* Michael Geist, *Fair.com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP*, *at* http://aix1.uottawa.ca/~geist/geistudrp.pdf (last visited Aug. 2001); Milton Mueller, *An Analysis of ICANN's Uniform Dispute Resolution Policy*, *at* http://www.acm.org/usacm/IG/roughjustice.pdf (last visited Sept. 19, 2002).
[11] A. Michael Froomkin & Mark A. Lemley, *ICANN and Antitrust*, *at* http://www.law.miami.edu/~froomkin /articles/icann-antitrust.pdf (last visited Sept. 19, 2002).
[12] A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17, at 45-46 (2000), *available at* http://www.law.miami.edu/~froomkin/articles/icann.pdf (last visited Sept. 19, 2002); Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187, 188 (2000), *available at* http://www.law.wayne.edu/weinberg/legitimacy.pdf (last visited Sept. 19, 2002).
[13] Internet Assigned Numbers Authority, *Generic Top-Level Domains*, *at* http://www.iana.org/gtld/gtld.htm (last modified Aug. 26, 2002) (providing a complete list of the current fourteen gTLDs and the requirements for obtaining some of the gTLDs).
[14] Internet Assigned Numbers Authority, *Root-Zone Whois Information*, *at* http://www.iana.org/cctld/cctld-whois.htm (last modified Oct. 27, 2001) (providing a complete list of the current 243 ccTLDs).
[15] Internet Assigned Numbers Authority, *Infrastructure Top-Level Domain*, *at* http://www.iana.org/arpa-dom/ (last modified Jan. 28, 2002).
[16] *See generally* DNS Resources Directory, *at* http://www.dns.net/dnsrd/ (last visited Sept. 19, 2002).
[17] The US operates the "E," "G," and "H" root servers. The US contracted out operations of the "A," "B," and "L." "C" and "D" are operated by non-governmental, US-based entities. And only the "I," "K," and "M" root servers are operated in other countries. David Conrad et al., *Root Nameserver Year 2000 Status*, *at* http://www.icann.org/committees/dns-root/y2k-statement.htm (July 15, 1999).
[18] Greek Research & Technology Network, *Root Name Servers*, *at* http://netmon.grnet.gr/stathost/rootns/ (last modified Sept. 20, 2002) (providing the status of each root name server).
[19] Froomkin, *supra* note 12, at 45-46, *available at* http://www.law.miami.edu/~froomkin/articles/icann.pdf (last visited Sept. 19, 2002).
[20] Jon Postel, the "creator" and "safekeeper" of the DNS, seemed to have been revered by the world as being, arguably, the most influential, trustworthy, and dedicated management person since the inception of the non-military Internet. *Id.*
[21] *See* President's and Vice-President's Report on Global Electronic Commerce, *A Framework For Global Electronic Commerce*, Information Technology Management Web, *at* http://www.itmweb.com/essay541.htm (July 1, 1997) (issued by William J. Clinton & Albert Gore, Jr., this document is also known as the "E-commerce White Paper").
[22] Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (proposed Feb. 20, 1998), *available at* http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm (Aug. 21, 2002).
[23] Interestingly, Froomkin and Lemley commented that, "[t]he White Paper did not actually mandate the creation of this corporation, but . . . only said how nice it would be if someone would form it to undertake certain specified tasks so that the government could strike a deal with it." Froomkin & Lemley, *supra* note 11, at 7-8.
[24] Froomkin & Lemley, *supra* note 11, at 8.
[25] *See* U. S. Dep't of Commerce and Network Solutions, Inc., Cooperative Agreement No. NCR-9218742, amend. 11, *at* www.ntia.doc.gov/ntiahome/domainname/proposals/docnsi100698.htm (National Telecommunications and Information Administration Oct. 7, 1998) (Sep 23, 2002).

[26] Memorandum of Understanding, Dep't of Commerce and ICANN, *at* www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm (last visited Sept. 20, 2002); Memorandum of Understanding, Dep't of Commerce and ICANN, amend. 1, *at* www.icann.org/nsi/amend1-jpamou-04nov99.htm (signed Nov. 10, 1999) (Aug. 4, 2002).
[27] Cooperative Research & Development Agreement, U.S. Dep't of Commerce & ICANN, *at* www.icann.org/committees/dns-root/crada.htm (last visited Sept. 20, 2002).
[28] "IANA (Internet Assigned Numbers Authority) is the organization . . . that, under a contract from the U.S. government, has overseen the allocation of Internet Protocol addresses to Internet service providers ("ISP"s). IANA also has had responsibility for the registry for any 'unique parameters and protocol values' for Internet operation. These include port numbers, character sets, and MIME media access types. . . . [T]he U.S. government has withdrawn its oversight of the Internet, previously contracted out to IANA, and lent its support to a newly-formed organization with global, non-government representation, the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN has now assumed responsibility for the tasks formerly performed by IANA." Whatis.com, *at* http://whatis.techtarget.com/definition/0,,sid9_gci214010,00.html (last modified July 30, 2001).
[29] Froomkin & Lemley, *supra* note 11, at 13; Memorandum of Understanding, Dep't of Commerce and ICANN, *supra* note 26.
[30] Management of Internet Names and Addresses, *supra* note 7.
[31] *Id.*
[32] *Id.*
[33] Allan Gregg, Presentation to the Annual General Meeting of the Canadian Internet Registration Authority, *Canadian Attitudes Toward the Dot-ca Domain*, *at* www.cira.ca/official-doc/104.cira_tsc_en.pdf (Dec. 6, 2001).
[34] *Id.*; *see also* Press Release, Canadian Internet Registration Authority, Results of a CIRA Study of Canadian Companies, *at* www.cira.ca/news-releases/72.html (May 28, 2002). It appears that the WIPO Standing Committee on Trademarks, Industrial Designs and Geographical Indicators is going to recommend to the WIPO General Assembly that country codes should be protected as geographical indications. Both the long name and short name of the country, appearing in the UN and the ISO 3166 lists, plus any other "common" names (like "Holland," "Ceylon," "Burma" in the six official languages of the UN (English, French, Spanish, Russian, Arabic, and Chinese), in all those alphabets/characters, plus the official language(s) of the country (South Africa has 11). Protection is to be given in all gTLDs, existing and future, as well as all ccTLDs. If that was not enough, not only are the exact names protected, but any misleading spellings. *See also* World Intellectual Property Organization, Standing Committee on Trademarks, Industrial Designs and Geographical Indicators, Second Special Session on the Report of the Second WIPO Internet Domain Name Process, The Protection of Country Names in Domain Name System, *at* http://www.wipo.int/sct/en/documents/special_session/pdf/sct_s2_3.pdf (Mar. 29, 2002).
[35] Letter from Michael Binder, Assistant Deputy Minister, Industry Canada, to Robert Hall, Chair, Canadian Internet Registration Authority, *at* www.iana.org/reports/industry-canada-letter-11mar99.htm (last visited Mar. 11, 1999).
[36] Press Release, NeuStar, Inc., U.S. Government Selects Neustar To Manage America's Internet Address, .us, *at* www.neustar.us/press/pr_archives/dotus_pr_10.29.01.pdf (last visited Oct. 29, 2001).
[37] Commission Working Paper, The Creation of the .EU Internet Top Level Domain, at 5, *at* http://europa.eu.int/comm /information_society/policy/internet/pdf/doteu_en.pdf (Feb. 2, 2000).
[38] *Id.*
[39] Letter from Richard Alston, Senator and Minister for Communications, Information Technology and the Arts, Australia, to M. Stuart Lynn, President and Chief Executive Officer, Internet Corporation for Assigned Names and Numbers, *at* www.iana.org/cctld/au/alston-to-lynn-04jul01.htm (July 4, 2001).
[40] Electronic Communications and Transactions Bill No. 23195, GOV'T GAZETTE, Mar. 1, 2002, *available at* www.gov.za/gazette/bills /2002/23195.pdf (last visited Sept. 19, 2002) (S. Afr.).
[41] *Id.*
[42] Namespace, *Government Involvement in ccTLD Administration*, CCTLD REVIEW, *at* http://www.namespace.org.za/cctld_review.html (Mar. 26, 2002)*; see also* Nominet .UK News, *Annual General Meeting 2000*, *at* www.nominet.org.uk/members/agm2000 .html (last visited Sept. 20, 2002); Nominet.UK News, *Reflections on the AGM 2001*, *at* www.nominet.org.uk/news/agm-reflect.html (last visited Sept. 20, 2002).

[43] Governmental Advisory Committee, *supra* note 1.
[44] Communiqué of the Government Advisory Committee, ICANN, *at* http://cyber.law.harvard.edu/icann/santiago/archive/GAC-Comminuque-mtg3.html (last visited Aug. 24, 1999).
[45] Internet Coordination Policy, ICANN, *ICP-1: Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation), at* www.icann.org/icp/icp-1.htm (May 1999) (containing a summary of current practices of the ICANN).
[46] Lynn, *supra* note 3.
[47] ICANN. ICANN: *A Blueprint for Reform, at* http://www.icann.org/committees/evol-reform/blueprint-20jun02.htm (last visited June 20, 2002).
[48] Elliot Noss, et al., *A New Approach to ICANN Reform: The Heathrow Declaration, at* http://www.byte.org/heathrow/heathrow-declaration-v0r0d5-032502.html (Mar. 25, 2002).
[49] New.Net, *A Proposal for More Realistic Domain Name Governance, at* http://www.new.net/WhitePaper_v2.html (last visited Mar. 2002).
[50] John Perry Barlow, *The Accra Manifesto, at* http://lists.essential.org/pipermail/random-bits/2002-March/000792.html (last visited Mar. 12, 2002).
[51] John Perry Barlow, *A Declaration of the Independence of Cyberspace, at* http://www.eff.org/~barlow/Declaration-Final.html (Feb. 8, 1996).
[52] Barlow, *supra* note 50.
[53] *Id.*; *See* ICANNWATCH.ORG, *The EU Weighs in on ICANN Reform, at* www.icannwatch.com/article.php ?sid=822 (last visited June 26, 2002); Lynn, *supra* note 3.
[54] Steve Kettmann, *Will US Release Grip on ICANN?*, WIRED NEWS, *at* http://www.wired.com/news/infostructure/0,1377,49836,00.html (Jan. 12, 2002) (quoting Andy Mueller-Maguhn, Europe's Representative of the Internet Corporation for Assigned Names and Numbers).
[55] *Id.*
[56] *Id.*
[57] Improvement of Technical Mgmt. of Internet Names and Addresses, 63 Fed. Reg. 8826 (Feb. 20, 1998).
[58] Management of Internet Names and Addresses, *supra* note 7.
[59] Angela Proffitt, *Drop the Government, Keep the Law: New International Body for Name Assignment Can Learn from United States Trademark Experience*, 19 LOY. L.A. ENT. L.J. 601, 608 (1999).
[60] Industry Canada, *Reform of the Domain Name System: Current Developments & Statement of Principles: An Information Paper Prepared by Industry Canada with the assistance of Omnia Communications Inc., at* http://e-com.ic.gc.ca/english/strat/651d2.html (Sept. 1998).
[61] Management of Internet Names and Addresses, *supra* note 7.
[62] ICANN, *Proposed TLD Sponsorship Agreement, at* http://www.icann.org/tlds/agreements/sponsored/sponsorship-agmt-16oct01.htm (Oct. 16, 2001).
[63] *See, e.g.*, ICANN, *Registrar Accreditation Agreement, at* www.icann.org/registrars/ra-agreement-17may01.htm (May 17, 2001).
[64] ICANN, *ccTLD Sponsorship Agreement (.au), at* www.icann.org/cctlds /au/sponsorship-agmt-25oct01.htm (Oct. 25, 2001).
[65] ICANN, *ccTLD Sponsorship Agreement (.jp), at* www.icann.org/cctlds/jp /sponsorship-agmt-27feb02.htm (Feb. 27, 2002).
[66] *Id.* art. 4.6; *ccTLD Sponsorship Agreement (.au), supra* note 64, art. 4.6; *see also* ICANN, *ccTLD Sponsorship Agreement (.au): Attachment E, at* http://www.icann.org/cctlds/au/sponsorship-agmt-atte-25oct01.htm (last visited Oct. 25, 2001); ICANN, *ccTLD Sponsorship Agreement (.jp): Attachment F, at* http://www.icann.org/cctlds/jp/proposed-sponsorship-agmt-9feb02.htm (Feb. 27, 2002). *Cf.* Namespace ZA, *Comments on the Electronic Communications and Transactions Bill, at* http://www.namespace.org.za/020424A_ectresp.htm (Apr. 24, 2002) (suggesting ICANN attempts to impose artificial and arbitrary changes upon registries with whom ICANN has no contractual relations).
[67] *CcTLD Sponsorship Agreement (.au), supra* note 64, art. 6.2; *ccTLD Sponsorship Agreement (.jp), supra* note 65, art. 6.2.
[68] *CcTLD Sponsorship Agreement (.au), supra* note 64, art. 6.2; *ccTLD Sponsorship Agreement (.jp), supra* note 65, art. 6.2.
[69] *CcTLD Sponsorship Agreement (.jp), supra* note 65, art. 6.3; *ccTLD Sponsorship Agreement (.au), supra* note 64, art. 6.3.

[70] Burundi and Malawi most recently signed a Memorandum of Understanding with the ICANN in order to achieve their desired pseudo-control over their own domain. *See* IANA, *IANA Report on Redelegation of the .bi Top-Level Domain*, *at* http://www.iana.org/reports/bi-report-16jul02.htm (July 16, 2002); IANA, *IANA Report on Redelegation of the .mw Top-Level Domain*, *at* http://www.iana.org.reports/mw-report-12aug02.htm (Aug. 12, 2002). *See generally* Heise News Online, *Controversy over "Superregistry"*, *at* http://www.heiss.de/newsticker/data/anw-03.02.02-044/ (Feb. 3, 2002) (describing controversial relationship between ICANN and ccTLDs); Peter de Blanc, *ccTLD Briefing Document*, *at* http://www.wwtld.org/meetings/ccTLD/Geneva2001/ccTLD_Briefing_document.html (Feb.19, 2001) (suggesting new possibilities for the relationship between ccTLDs and ICANN); ICANN Watch, *ICANN and Centr at Odds*, *at* http://www.icannwatch. org/article.php?sid=510 (last visited Mar. 26, 2002) (stating that ICANN had far to go in terms of understanding the issues and problems ccTLDs face and in terms of working with them as equal partners).

[71] Lynn, *supra* note 3.

[72] ICANN, *Preliminary Report, Special Meeting of the Board*, *at* http://www.icann.org/minutes/prelim-report-25sep00.htm (Sept. 25, 2000).

[73] *See, e.g.*, ICANN, Memorandum of Understanding between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers, amend. 2, *at* http://www.icann.org/general/amend2-jpamou-07sep00.htm (Aug. 30, 2000); Governmental Advisory Committee, *supra* note 1.

[74] IANA, *IANA Report on Request for Redelegation of the .au Top-Level Domain*, *at* www.iana.org/reports/au-report-31aug01.htm (Aug. 31, 2001); IANA, *Second IANA Report on Request for Redelegation of the .au Top-Level Domain*, *at* www.iana.org/reports/au-report-19nov01.htm (Nov. 19, 2001).

[75] J. Postel, Domain System Structure and Delegation, Memo in response to Request for Comments, No. 1591, *at* www.isi.edu/in-notes/rfc1591.txt (Mar. 1994) (J. Postel is associated with the University of Southern California, Information Sciences Institute).

[76] Internet Coordination Policy, *supra* note 45.

[77] Governmental Advisory Committee, *supra* note 1.

[78] IANA, *IANA Report on Request for Redelegation of the .ca Top-Level Domain*, *at* http://ww.iana.org/reports/ca-report-01dec00.htm (Dec. 1, 2000); *see also* Letter from Maureen Cubberley, Chair, Canadian Internet Registration Authority, to Michael Roberts, President and Chief Executive Officer, Internet Corporation for Assigned Names and Numbers, *at* http://www.iana.org/reports /cira-letter-30nov00.htm (Nov. 30, 2000).

[79] IANA, supra note 78.

[80] *See generally* Letter from Derek A. Newman, attorney, Newman & Newman LLP, to Louise Touton, Vice President and General Counsel, IANA, *at* www.wwtld.org/Tracking_IANA/CX_Touton_Nameserver_Changes_20011213.pdf (Dec. 13, 2001) (regarding the .cx Christmas Islands). To this date, there has still not been a redelegation of .cx.

[81] ICANN, *Announcement, Redelegation of .us Country-Code Top-Level Domain*, *at* www.icann.org/announcements/announcement-19nov01.htm (Nov. 19, 2001) (noting a full report will be posted "as soon as it is complete").

[82] *Id*.

[83] *Id.*

[84] ICANN, *Articles of Incorporation*, para. 3, *at* http://www.icann.org/general/articles.htm (Nov. 21, 1998).

[85] ISO 3166 Maintenance Agency, English Country names and Code Elements, *at* www.din.de/gremien/nas/nabd/iso3166ma/codlstp1/en_listp1.html (last modified June 12, 2001).

[86] ISO 3166 Maintenance Agency, *ISO 3166-1 and Country Coded Top-Level Domains (ccTLDs)*, *at* http://www.iso.org/iso/en/prods-services/iso3166ma/04background-on-iso-3166/iso3166-1-and-ccTLDs.html (last visited Sept. 19, 2002). The ccTLDs which ICANN has created which are not based on the official list of country codes but on the list of reserved ISO 3166-1 code elements are: .uk for the United Kindgom as opposed to GB. ICANN explains the reasons as follows, "[t]he United Kingdom was assigned the ccTLD .uk in the mid-1980s even though ISO 3166-1 calls for use of .gb. This assignment occurred before the IANA began using any standard list of country-code abbreviations." IANA, *IANA Report on Request for Delegation of the .ps Top-Level Domain*, *at* http://www.icann.org/general/ps-report-

22mar00.htm (Mar. 22, 2000). The others are AC for the Ascension Island (from the reserved list), GG for Guernsey (from the reserved list), IM for the Isle of Man (from the reserved list), JE for Jersey (from the reserved list). J. Klensin, *Reflection on the DNS, RFC 1591, and Categories of Domains*, at 6, *at* http://www.rfc-editor.org/rfc/rfc3071.txt (Feb. 2001).

[87] Sergey Kuznetsov, *Russia May Say 'See Ya' to Dot-Su*, *at* http://www.wired.com/news/print/0,1294,55687,00.html (last visited Nov. 14, 2002).

[88] ICANN, *Internet Assigned Numbers Authority Report on Request for Delegation of the .ps Top-Level Domain*, *at* http://www.iana.org/reports/ps-report-22mar00.htm (Mar. 22, 2000).

[89] Commission Working Paper, *supra* note 37.

[90] Letter from Erkki Liikanen, Member of the European Commission, to Mike Roberts, President and Chief Executive Officer Internet Corporation for Assigned Names and Numbers, *at* http://europa.eu.int/ISPO/eif/InternetPoliciesSite/DotEU/LetterLiikanenRoberts.html (July 6, 2000).

[91] Letter from Michael M. Roberts, President and Chief Executive Officer Internet Corporation for Assigned Names and Numbers, to Erkki Liikanen, Member of the European Commission, *at* www.icann.org/correspondence/roberts-letter-to-liikanen-10aug00.htm (Aug. 10, 2000).

[92] ICANN, *Preliminary Report, Special Meeting of the Board*, *supra* note 72; *see also* Posting of Ant Brooks, ant@hivemind.net, to cctld-discuss@wwtld.org, *at* http://www.wwtld.org/mailarchive/cctld-discuss/vol01/msg00287.html (discussing Andrew McLachlin's interpretation of the resolution) (Sept. 30, 2000).

[93] *See* Commission of the European Communities, Proposal for a Regulation of the European Parliament and of the Council on the Implementation of the Internet Top Level Domain ".EU," *at* http://europa.eu.int/eur-lex/en/com/pdf /2000/en_500PC0827.pdf (Dec. 12, 2000).

[94] *See* Press Release, European Commission, Commission Welcomes Adoption of Regulation for ".eu" Internet Domain Names, *at* http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/02/468 |0|RAPID&lg=EN (last visited Sept. 19, 2002).

[95] David McGuire, *ICANN Has Final Say on Dot-EU Internet Domain – Update*, NEWSBYTES (Mar. 26, 2002).

[96] ICANN, *Preliminary Report, Special Meeting of the Board*, *supra* note 72.

[97] This may raise an interesting issue of undue influence.

[98] ICANN, *Model ccTLD Sponsorship Agreement – Triangular Situation*, para. 4.5.1, *at* http://www.icann.org/cctlds/model-tscsa-31jan02.htm (Jan. 31, 2002).

[99] *See also* MILTON L. MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 211-26 (The MIT Press 2002).

[100] Milton L. Mueller, *An Analysis of ICANN's Uniform Dispute Resolution Policy*, *at* http://www.acm.org/usacm/IG/roughjustice.pdf (last visited Sept. 19, 2002).

[101] MUELLER, *supra* note 99, at 228-53.

[102] Heathmount A.E. Corp. v. Technodome.com, No. CA-00-00714-A, 2000 U.S. Dist. LEXIS 20316, at *20-21 (E.D. Va. Dec. 29, 2000).

[103] *Id.*

[104] *Id.*

[105] Rep. Howard Coble, *To Provide Criminal Penalties for Providing False Information in Registering a Domain Name on the Internet* (introduced 5/2/2002) *at* http://thomas.loc.gov/cgi-bin/query/z?c107:h.r.4640: (last visited Nov. 14, 2002).

[106] *See The Accuracy and Integrity of the Whois Database: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Prop. of the House Comm. on the Judiciary*, 107th Cong. (statement of Michael D. Palage), *at* http://www.house.gov/judiciary/palage052202.PDF (2002) (last visited Nov. 14, 2002).

[107] ICANN, *Model ccTLD Sponsorship Agreement – Triangular Situation*, *supra* note 98, at para. 4.2.

[108] Dan Bart, *Nations and a World at Risk*, Report of the Telecommunications Standards Advisory Council of Canada 3, *available at* http://www.tiaonline.org/standards/cip/ciptsacc.pdf (Mar. 24, 1999).

[109] UNITED STATES COMMISSION ON NATIONAL SECURITY/21ST CENTURY, NEW WORLD COMING: AMERICAN SECURITY IN THE 21ST CENTURY, SUPPORTING RESEARCH AND ANALYSIS 52 (1999), *available at* http://www.nssg.gov/NWR_A.pdf (Sept. 15, 1999).

[110] Froomkin, *supra* note 12, at 48-49.

[111] *See* Glenn H. Takemoto, *Information Warfare in the Cyber Domain*, at 3-5 (2001), *at* http://www.infowar.com/mil_c4i/01/IWinCyberDomain.pdf (last visited Sept. 19, 2002).
[112] CHAIRMAN OF THE JOINT CHIEFS OF STAFF, JOINT VISION 2020, at 8, *available at* http://www.dtic.mil/jv2020/jv2020.doc (June 2000).
[113] *Id.*
[114] *See generally* Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, *at* http://www.nautilus.org/info-policy/workshop/papers/denning.html (last visited Nov. 14, 2002) (discussing use of the Internet during the Kosovo conflict at the Georgetown University Information Technology and American Foreign Policy Decisionmaking Workshop).
[115] *See generally* Mike Balough, Army Digitization Overview, Report to the Defence Industry Association, *available at* http://www.dtic.mil/ndia/cannon/balough.pdf (June 21, 2000) (presenting slides for an overview of the technologies contributing to the digitized battlefield).
[116] Letter from Billy Tauzin, et al, Chairman, House Committee on Energy and Commerce, to Donald L. Evans, Secretary of Commerce, *at* http://www.politechbot.com/p-03268.html (Mar. 13, 2002).
[117] New.net, *supra* note 49.
[118] *Id.*
[119] Takemoto, *supra* note 111, at 3-5.
[120] There does not appear to be an active .iq registry.
[121] Executive Summary, President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures, *available at* http://www.ciao.gov/resource/pccip/PCCIP_Report.pdf (Oct. 1997).
[122] *Id.* at 16.
[123] ICANN, ICANN DNS Security Update #1, *at* http://www.icann.org/committees/security/dns-security-update-1.htm (Jan. 4, 2002).
[124] *Id.*
[125] *Id.*
[126] *Id.*
[127] *Id.*
[128] Matrix Systems, *Distributed Denial of Service Attack*, *available at* http://www.matrixnetsystems.com/ea/advisories/20021022_instant_alert.jsp. (last visited Oct 22, 2002).
[129] *Id.*
[130] Reuters, *Experts: Hackers Could Easily Shut Down Net*, USA TODAY, Nov. 14, 2001, *available at* http://www.usatoday.com/life/cyber/tech/2001/11/14/internet-vulnerable.htm (last visited Sept. 19, 2002).
[131] NATIONAL RESEARCH COUNCIL, COMMITTEE ON THE INTERNET IN THE EVOLVING INFORMATION INFRASTRUCTURE, COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD, THE INTERNET'S COMING OF AGE 63 (National Academy Press,. 2001), *available at* http://www.nap.edu/books/0309069920/html (last visited Sept. 19, 2002).
[132] Governmental Advisory Committee, *supra* note 1.
[133] This issue is more fully discussed in G. Hagen, *Sovereign Domains and Property Claims*, INT J.L. TECH. (forthcoming Spring, 2003).
[134] *See* Froomkin & Lemley, *supra* note 11, at 1-2; Froomkin, *supra* note 12, at 29-32.
[135] Barber, *supra* note 8.
[136] *Id.*
[137] *Id.*; *see also* Colás, *supra* note 8.
[138] *See* G. Hagen & K. G. von Arx, *Patriation of the .ca*, CAN. J.L. & TECH. 1:3 (November 2002).
[139] Management of Internet Names and Addresses, 63 Fed. Reg. 31,741 (proposed Feb. 20, 1998), *available at* http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm (last visited Nov. 14, 2002).
[140] Management of Internet Names and Addresses, *supra* note 7.
[141] James Boyle, *Foucault In Cyberspace: Surveillance, Sovereignty, and Hard-Wired Censors*, *at* http://www.wcl.american.edu/pub/faculty/boyle/foucault.htm (1997) (emphasis added).
[142] James Boyle, *A Nondelegation Doctrine For The Digital Age?*, 50 DUKE L.J. 5, 8-9 (Oct. 2000), *available at* http://www.law.duke.edu/shell/cite.pl?50+Duke+L.+J.+5.
[143] Froomkin, *supra* note 12, at 143.
[144] Boyle, *supra* note 142 at 13-14.
[145] Boyle, *supra* note 142.

[146] *Id.*
[147] David McGuire, *ICANN Threatens to Take Away VeriSign's '.com' Privileges*, WASHINGTON POST, Sept. 4, 2002, at E05, *available at* http://www.washingtonpost.com/wp-dyn/articles/A34373-2002Sep3.html; David McGuire, *ICANN Threatens To Revoke VeriSign's Right To Sell Dot-Com Names*, WASHINGTON POST, Sept. 3, 2002, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A33395-2002Sep3?language=printer.
[148] This conflicts with ICANNs assertion in ICP-3, that it is the "single, authoritative public root for the Internet Domain Name System." Indeed, its claim is 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." ICANN, *ICP-3*: *A Unique, Authoritative Root for the DNS, at* http://www.icann.org/icp/icp-3.htm (July 9, 2001). This claim has been endorsed by the Internet Architecture Board and the Internet Engineering Task Force. *See* Internet Architecture Board, *Technical Comment on the Unique DNS Root, at* http://www.icann.org/correspondence/iab-tech-comment-27sept99.htm (Sept. 27, 1999); The Internet Engineering Task Force, ICANN Protocol Standards Organization, Minutes, *at* http://www.pso.icann.org/PSO_Minutes/PSO-Minutes-4Sept2001.txt (Sept. 4, 2001).
[149] Milton L. Mueller, *Competing DNS Roots: Creative Destruction or Just Plain Destruction*?, at 16, *at* http://www.itu.int/osg/spu/seminars/mueller/tprc2001.pdf (Nov. 23, 2001) (concluding his presentation at the ITU Strategy and Policy Unit Lunch Seminar in Geneva).
[150] *Id.*
[151] *See, e.g.*, New.net, *supra* note 49.
[152] *See, e.g.*, Simon Higgs, *Routing Around a Single Point of Failure, at* http://www.icannwatch.org/article.php?sid=198 (last visited Sept. 19, 2002); Simon Higgs, *Alternative Roots and the Virtual Inclusive Root, at* http://www.higgs.com/publications/id/draft-higgs-virtual-root-00.txt (May 2001); Simon Higgs, *Root Server Definitions*, *at* http://www.higgs.com/publications/id/draft-higgs-root-defs-00.txt (Feb. 2001).
[153] Recently Stuart Lynn contended that, "it is simply unthinkable that a large fraction of the TLDs in the root zone file should be permitted to operate independently of the global community and of policies established by the global community. In each case, it is essential that these critical entities formally agree not to break the DNS, and to abide by standard global operational practices arrived at through the ICANN process." Lynn, *supra* note 3.
[154] *See generally* Hagen & von Arx, *supra* note 138.
[155] MUELLER, *supra* note 99, at 48.
[156] This simple outline of a p2p based system seems to confirm the judgment of the ICANN Protocol Supporting Organization that it is technically to devise a multiple root DNS. "Although, it would be technically possible to devise and standardize a fully compliant alternative multiple root server system, there appears no technical reason for changing from the present working system, as this would require the development of a new set of protocols for use by the DNS." ICANN Protocol Standards Organization, Minutes, *at* http://www.pso.icann.org/PSO_Minutes/PSO-Minutes-4Sept2001.txt (Sept. 4, 2001); ICANN Protocol Standards Organization, Minutes, *at* http://www.pso.icann.org/PSO_Minutes/PSO-Minutes-28Sept2001.txt (Sept. 28, 2001). We have argued that it is politically reasonable as well.
[157] NATIONAL RESEARCH COUNCIL, *supra* note 131.
[158] *Id.*
[159] Of course, the above scheme could also apply to all TLDs. We have not proposed such a solution in this paper. However, as time goes on, the DNS may have 257 root servers. In other words, each gTLD and ccTLD would have its own root server, which points to other authoritative root servers.