DRAFT (TPRC / 2 Oct. 2004)

Multilateral Control of Internet Infrastructure and its Impact on US Sovereignty

By Kenneth Neil Cukier *

Abstract:
As the US continues its transitional oversight of ICANN until the group is given autonomy, there has been a lack of discussion on what the implications of this transfer of control from the US to ICANN means for US interests. This paper is a pragmatic attempt to identify the potential impact of greater participation in Internet management by other stakeholders, notably governments and intergovernmental organizations.

The paper first explains what is the Internet, Internet coordination, and ICANN, in the context of its hallmark: its decentralization and capacity for innovation. It then notes what Internet infrastructure means for the national interests of all countries, and specifically the US, in terms of security, economy and political society. From there, it considers the potential effects of greater intergovernmental participation in the four main areas of Internet infrastructure coordination (domain names, IP numbers, root servers and protocols), and future policy formation.

The paper concludes that although ceding control entails a minor loss of sovereignty, it may not harm US interests; in fact, over time, a global multi-stakeholder approach may actually benefit the US. At the same time, the US should be vigilant that the transfer happens in a manner and timeframe that preserves the openness that is currently inherent in the architecture of the network. The US should also be agnostic as to institutional design so long as its long-term interests are achieved.

* Kenneth Neil Cukier <knc@cukier.com> is a technology correspondent for *The Economist* in London, focusing on the international policy aspects of the Internet. From 2002 to 2004 he was a research fellow at the National Center for Digital Government at Harvard University's John F. Kennedy School of Government, where he prepared this paper. The author thanks the Center's directors and fellows for the rich intellectual environment they provided, and expresses his gratitude to the many people who educated him over the years on Internet matters. Special thanks go to Scott Bradner and Matthew Hindman.

Outline:

Introduction

Part I: The Internet, Internet coordination, and ICANN

1. What is the Internet
2. What is Internet ~~Governance~~ Coordination *(sic)*
    - A. Classic Coordination Areas (Names, Numbers, Root and Standards)
    - B. Internet Balance-of-Power Considerations
3. What is ICANN

Part II: Internet Infrastructure and Common National Interests

1. Common National Interests: Overview
2. Security
    - A.. National Control of Country-Code Domains
    - B. Stability of Root and Security in Standards
3. Economy
    - A. Commercial Innovation and Standards
    - B. Services and Devices Related to IP Numbers
    - C. Online Identity and Domain Names
    - D. Universality of Communications and Root Servers
4. Socio-Political
    - A. Privacy, Freedom, Globalism, Innovation in Domain Names
    - B. Services and Ease-of-Use from IP Numbers and Standards
    - C. Empowerment and Symbolism

Part III: US Interests and Potential Impact of International Control

1. US Interests Related to US Control: Overview
    - A. National Interests (Security, Economy and Socio-Political)
    *(*Subtopics: *reliability and domains; stability and root servers; security and surveillance; US military interests; predictability and institutional design; intellectual property and standards; the economics of names and numbers.)*
    - B. National Power (Influence Abroad)
    - C. National Sovereignty (Domestic Autonomy)
2. Possible Effects of Shared, Multilateral Control
    - A. Classic Coordination Areas (Names, Numbers, Root and Standards)
    - B. Policy Formation and Scope ("*XCANN*," GAC, Institutional Model)

Conclusion

Appendix A: Internet Infrastructure Resources as a Matter of International Politics
Appendix B: Country-Code Domains and National Control
Appendix C: ICANN's Registry Funding and Domain Name Innovation
Appendix D: Control of the Root Servers and Policy Evolution

Notes

Introduction

Most of us appreciate the Internet and depend on it enormously, yet we take for granted that it works as smoothly as it does. So to understand the importance of how its underlying infrastructure is managed, consider a few worst-case scenarios:

* *Everything needs pre-approval.* All Internet content needs to be tagged based on internationally-agreed norms (for such things as decency and intellectual property legality) or routers won't send the data through the network. Additionally, all software used on computing devices must be authorized in advance or the device can't be used on the Internet.

* *Huge amounts of sites on the Internet are unreachable to most users.* The reason: Countries issue Internet domain names in local-language scripts, but don't follow agreed upon standards on the technical format of those names. As a result, users without the proper keyboard or software are not able to access those Web sites or send email to those email addresses. And this is a problem multiplied by as many countries there are that don't use English.

* *Internet service providers rescind many basic services.* Features like instant messaging with voice and video, multi-player online gaming, or being able to access your home computer's desktop from a cyber café are no longer offered to users except at extremely high prices. This is because Internet Protocol numbers are required to be divided up equally among all countries; France gets as many as Senegal, even though the degree of Internet use is radically different. A bustling aftermarket exists, but the high cost of obtaining numbers means that services that rely on them can only be offered for the few users willing to pay a lot extra for them. Where they are offered, it is usually off the public Internet and unreachable from some places.

Sound awful? It is. But if it sounds preposterous, it isn't. Although all three scenarios are unlikely, they are not impossible. The technology policy issues in all three situations -- technical standards, domain names and IP numbers -- fall under the rubric of Internet infrastructure management. If the institutions that keep the Net running smoothly from a technical point of view fail to work, the Internet would become less useful, too.

The Internet has emerged as a critical infrastructure for commerce, communications, government services and civil society for every country. It makes the question of who controls it -- that is, oversees its technical coordination and evolution -- of paramount importance to all nations. Currently, the US government has predominant power over the Internet's core infrastructure, the domain name system, through its oversight authority of ICANN, the Internet Corporation for Assigned Names and Numbers. Yet the US's transitional period as defined in its 1998 statement of policy (the White Paper) [1] has elapsed, and plans are being considered for a new timeframe and rubric for the US to relinquish control to ICANN. [2]

It is rare in international relations for a country that enjoys power to voluntarily cede it, though that is essentially what is happening. ICANN was established in 1998 as a form of international industry self-regulatory body. However, the policy was formed in the context of introducing market competition for selling domain names and creating intellectual property protection for trademarks -- not with broader foreign policy interests in mind. [3] Indeed, in a sign of this commercial approach, the policy is led by the Commerce Dept., not the State Dept. The issue is controversial internationally: other governments see ICANN as an instrument of US dominance of cyberspace. This went so far as to lead the United Nations to convene a working group on "Internet governance," to consider the role of governments in this regard. [4] Fittingly, its first mission is to define such an ambiguous concept, that has traditionally referred to infrastructure coordination, but is increasingly used to mean much more: any area of the Internet where governments believe they have a role, such as privacy, content controls, spam, cybersecurity, international access cost, as well as ICANN.

On its own, the question of who manages the Internet's underlying infrastructure is not a tier-one foreign policy issue for most nations, and certainly not for the United States. Though significant, there are many more serious issues that require attention. However, the importance that other countries are placing on the "Internet governance" issue, and the significant diplomatic resources they are putting towards it, raises the importance of the matter considerably for the United States, because it essentially calls into question US authority, and is an attempt to displace US control. Ironically, this is happening at a time, it bears repeating, when the US is voluntarily ceding control as a matter of policy.

This paper represents an attempt to provide an assessment of what diminished US control of ICANN means for American interests (related to national security, national power and national sovereignty). The paper first explains the Internet, Internet coordination, and ICANN, in the context of the decentralization of communications networks and innovation. Secondly, it identifies the key areas where control over the domain name system matters to national interests of all nations. Thirdly, it examines unique US interests in infrastructure coordination due to the US's oversight authority, and then assess the impact of multilateral control on specific areas of Internet infrastructure.

The paper concludes by recommending that the transition of US authority to an independent entity for Internet coordination should continue, provided the US retains control of certain Internet resources (namely, legacy generic domains, and root servers); maintains special influence on policy through its ability to shape policy due to its market size and technology firms; assures an institutional structure that embodies a multi-stakeholder approach to prevent any imposition that might ossify Internet technology with political or commercial interests; and guarantees that the openness of the Internet's architecture is preserved. Lastly, the current domain name system and any entity that oversees it should not be treated as sacrosanct and able to easily succeeded by outside interests, based on users' volition. The US should be open-minded as what institution serves this function; the paper introduces the term "XCANN" to describe this.)

Though the issue of ICANN has been well treated in numerous scholarly and policy work, there has not yet been a systematic study of the effects of the US ceding control on the Internet's capacity to encourage democratic values and continued technical innovation, which are arguably its hallmark. This paper is meant as an initial look at that vast issue. As befits the author's background -- in journalism, not academia -- this paper is an empirical examination at the issue, not a scholarly treatment of it.

Internet coordination matters to the US domestically in terms of assuring the stability of the infrastructure and imposing legal safeguards, so that citizens and industry have confidence in the network. In this way, the Internet can continue to become the platform for communications and commerce. Yet Internet coordination is also vital for promoting traditional foreign policy objectives, since the Internet as it is currently constituted – with an open architecture compared to other communications media – can export values of transparency, free expression and economic development. Moreover, the Internet is important for community-building, which is the bedrock of civil society, particularly in developing countries. There is also a human rights dimension: the domain name system is the centerpiece of personal identification online, effecting privacy, freedom of assembly online, and even freedom of thought.

Ultimately, the changes in ICANN's oversight authority may have serious repercussions worldwide for users and the future of the medium -- or, it may be barely noticed, and the Internet continue to evolve in a healthy, unfettered way. This paper represents a rough attempt to identify the possible impact of the transfer of power from the US to ICANN itself. Such an event would entail less influence by the US, and more influence to other countries (both directly and through international organizations). The paper concludes that although ceding control entails a minor loss of sovereignty, this does not harm US interests. At the same time, the US should be vigilant that the transfer happens in a manner and timeframe that preserves the openness inherent in the architecture of the network

Part I: The Internet, Internet coordination, and ICANN

The Internet's best definition is that it defies definition; its capacity for continued innovation and re-invention is its hallmark, but it's based on a principle: openness. This is established through its end-to-end design. With that as the focus of understanding, this section looks at the basic needs of Internet coordination, and then how that is accomplished through ICANN -- noting where the organization came from, its actions in its first six years, and the pressure for change.

1. What is the Internet

The Internet to most people is a plastic term, signifying something to do with computers and digital content and communications. It's often wrongly considered a synonym for the World Wide Web (which is an application, akin to instant messaging or email, that travels atop the Internet, which is the transport infrastructure). Even government regulatory policies offer only vague, at times inconsistent, definitions for the Net [5]. The fact that the Internet is typically written with a capital "I" offers a clue that it represents something quite specific (or at least once did).

In fact, the Internet is a philosophy before it is an actual network. Its fundamental characteristic are its decentralization, and thus, its openness. The Net places great autonomy at the end-points, or edge, where individual users and sub-networks are, and asks for only a basic degree of agreement in order to route packets from source to destination. Indeed, the Internet was a response to two predominant drawbacks to data communications in the 1960s: the fact that different computer makers' machines were unable to inter-communicate, and the use of centralized, telephone-based circuit-switching technology for traffic, which was less robust in case of partial failure of transmission, and less efficient because it dedicated a full circuit regardless of the actual load. The Internet Protocol, was designed as a basic common denominator to enable the interconnection of networks, i.e. the term "Internet."

One theory behind the Internet is called the end-to-end principle. [6] It says that Internet communications should be as free from any centralization as possible, so that experimentation and innovation can take place at the edges of the network. The "core" or center of the network should be open, or "stupid." (The Internet's openness in this regard has two meanings: an openness to all networks and traffic who agree to use the basic Internet protocols, and an openness to decentralized innovation. [7] The model finds its parallel in many other areas outside technology: For instance, capitalism is a decentralized system organized by an "invisible hand" as opposed to Soviet-style communism, that was centralized (described as a "control economy" and typified by five-year-plans). The ideology behind the Internet is best expressed by the title of a popular book on the topic: "Small Piece Loosely Joined." [8]

This is unlike the telephone system, which is centralized, and where power rests at the core, not the edge. In such a system, the owner or operator of the infrastructure can determine the network's uses. New services are added only at the intention of the entity in control; anything not expressly allowed is usually forbidden. A centralized system allows for easy monitoring, measuring and billing of traffic. Innovation occurs at the pace set by the center of the network, rather than the end points. Experimentation often does not happen, and there is usually an attempt to predict what users want rather than a willingness to let them decide for themselves to what purpose to put the infrastructure. It is the difference between a typewriter and a computer -- the former allows only for words to appear on paper, based on the dictates of the manufacturer; the latter enables not only word processing but a myriad of other things, since the owner of the equipment can determine its uses.

The mentality of a closed network that is centralized, like the telephone system, is to charge for each discrete unit of activity (be it a phone call, or an email, or clicking on an interactive page for information) as opposed to the mentality of an open network like the Internet, where one usually charges once, for connectivity, and then lets users decide what to do online. [9] This is one reason why the Internet approach tends to encourage low cost of access, as opposed to the telephone system that only until very recently lacked this pull. [10] As the Internet matures, there is a fear among many of its inventors and supporters that is taking in the traits of the telephony world -- such as making the infrastructure more secure and traffic more traceable, as well as the architectural model less open to commercial competition -- which would set back many of the Internet’s most valuable attributes, albeit solving some of its ills. [11]

It is useful to distinguish the Internet by what it is not, by its predecessors in the evolution of media -- here to mean communications mediums, from print and publishing to the postal system, the telegraph, telephone, radio, and television (including over-the-air, satellite and cable). In short, some media format specific (telegraph is only text) and others characterized by reach (telephones are mainly a one-to-one medium, while television is a one-to-many medium). The Internet eliminates these distinctions allowing for any sort of reach (i.e. many-to-many) and form (i.e. multimedia). In fact, because it is decentralized unlike other communications media, the Internet is able to mature in lockstep with evolution in the processing power of end-devices (like PCs and mobile phones) rather than from top-down decisions at the core of the network. This means that the marginal cost of developing a new use -- like instant messaging or Napster -- is effectively zero, because it is added to software by the user at the edge of the network.

The Internet is distinct in another way that is significant to note: in the way it was treated commercially and in terms of public policy. Communications media aren't so much shaped by their underlying technology but by the political and economic decisions that are made about them. For instance, the US Congress's mandate for inexpensive postage for publications in the late 1800s spurred the development of a diverse newspaper and magazine industry, which in turn served to unify the newly transcontinental nation with a common civitas. France’s Minitel, a primitive online teletext system, was based in a centralized architecture that enabled every activity to be metered and charged for -- it survived long after the Web became commonplace due to the disincentives of France Telecom to promote the vastly superior technology of the Web, in which revenues were less certain due to competition. [12]

Importantly, behind the development of these media was a principle: the US, unlike Europe, never endowed the owners of one generation of media technology the control of the next; so the US Postal Service didn't get the telegraph, Western Union didn't get the telephone, AT&T didn't get radio, etc. This is one reason why those services developed much faster in the US than anywhere else. [13] Cross applied to the Internet, it is useful to note that Internet was not handed over to telecom carriers -- indeed, the industry, as noted earlier, rejected it because it was so small it wasn't worth its time. That led to a cottage industry of small, privately-run data-network providers, then unknown, today boasting world-famous names like AOL, MCI and Sprint, among others. The small players had an interest in maintaining an open network in which all could compete on equal footing, which at the time preserved the open nature of the Internet. [14] Also, as noted, it helped that regulatory policy stayed clear of the Internet, so as to let that competition flourish when the industry was an infant.

Lastly, the best way to define the Internet is to let it remained undefined. To define something is to limit it, to kill its evolution into new form. However, the Internet is typified by continual re-invention, and a capacity for fast, unpredictable change based on the innovation that takes place among the decentralized actions of people at the end-points that are free to experiment. In this respect, the Internet is a free market akin to capitalism; on a spiritual level, it aggregates and gives expression to the collective intelligence, talents and potential for progress of humanity. Again, this is due to its decentralized nature, which although is something that many parties see drawbacks from -- be it the difficulty of tracking down spammers to upholding music copyright -- leads to a low-cost, easy-to-use network undergoing constant innovation.

2. What is Internet ~~Governance~~ Coordination **(sic)**

The term "Internet governance" is undergoing a change in its meaning; it is now so ambiguous that it confuses more than clarifies. The expression generates so much misunderstanding that it should probably not be used in any serious way except as a sort of informal shorthand among policy people. Even then, the term is a useless catch-all, and should be avoided in favor of identifying issues precisely. (As such, this paper disdains it, and refers to "Internet coordination.")

There are, obviously, many aspects of the Internet where it is useful to have international, and intergovernmental agreement or harmonization. The inherently cross-border nature of the medium begs for cooperation among different jurisdictions, on matters like cybercrime, consumer protection, viruses, etc. These issues, in their offline equivalents, are dealt with by governments. It is rightly done so as well in an online setting. Yet the difficulty in addressing these challenges also seem to require the cooperation of many stakeholders, not just government, but industry and civil society. Furthermore, these issues regard the content and usage of the Internet. Below the surface of the network is the infrastructure layer, and here, the role of government has traditionally been much less pronounced. [15]

How that substrata of the Internet was administered was traditionally the purview of the network's designers, the technical community. They referred to it as "Internet governance," and it encompassed issues like allocating Internet Protocol numbers, assigning networking parameters, managing root servers, approving standards and delegating top-level domain names. In fact, in the late 1980s and early 1990s, it was actually called "Internet self-governance" because the so-called "Internet community" (then, a somewhat homogenous group of researchers and technical engineers), collectively made the decisions over how the Internet technology would evolve.

Today, as the Internet has grown, many of these same questions have emerged, rightfully, as matters of public policy, Moreover, as new voices have come to the debate from around the world, the meaning and history of the term has been divorced from its original context. This has been the source of misunderstanding. In some instances, people use or shun the term to promote an agenda; be it to bring government closer in to Internet matters, or keep it away. It is important to keep in mind the history of the term, since the very semantics unduly polarizes the debate due to its lack of clear meaning. (I return to this point at the end of this section.)

A. Classic Internet Coordination Areas (Names, Numbers, Root and Standards)

Though there are many areas of the Internet where governments have a role to play, and do play it, there is another dimension -- how the network itself works, and evolves on a technical level, which also have important political, economic and societal concerns. Despite the Internet's decentralized nature, there are a few basic things that need to be coordinated centrally to ensure the Net's interoperability. They are the names, numbers, the root servers that match the two, and the protocol, or "language" of the network itself. These are mainly technical issues, but as will later become apparent, they contain important public policy considerations. The most pressing issue facing the Internet is that infrastructure coordination questions have emerged as conflicts in international relations, whose a resolution is unclear (for more on this, see: "Appendix A: Internet Infrastructure Resources as a Matter of International Politics")

* *Domain names:* These are the addresses like "economist.com" that people use to find Web pages or send emails. While traffic still works without them, they are important for making the Internet easy to use. There are two aspects to the names, the domains at the "top" (such as generic ones like .com, or ones that designate countries and territories, like. .uk for Britain) and the "second-level" names (such as "economist" in this example). The top-level domains are delegated to an administrator to accept registrations of second-level addresses. A domain can only have a single administrator; if names were duplicated, traffic would get misrouted -- and it is the responsibility of the entity managing the Net's infrastructure to ensure that the name matches the authoritative IP number in the root server system (see below). As for technical coordination problems at the second-level, they are the concern of that administrator, and is not generally considered a matter of global Internet governance unless it jeopardizes the quality of service for all users on the network, more broadly. [16] That said, trademark issues for

both sorts of domains at the second level has been addressed by ICANN, through a Uniform Dispute Resolution Procedure, though the results have been controversial. [17]

A final word on domain names: to some, names seem rather unimportant -- digital traffic can still flow without them, people may find content using search engines, and other than switching costs associated with printed matter, browser bookmarks or "favorites" and branding issues, domain names can be changed easily and for a low price. However, this is an incredibly superficial perspective that looks only at where domain names are today; it takes rudimentary foresight to see that as the Internet matures, the role of domain names as the cornerstone of all digital identity -- for paying taxes, medical records, voting, etc -- may develop in tandem. Today, the state issues birth certificates and social security numbers: why not someday issue a national domain to serve as the locus of a citizen's digital rapport with the state and civil society institutions? For these institutions both governmental, corporate and civil, domain names represent online presences that may last in perpetuity. The names are even starting to meld with the traditional, governmental telephone numbering system, in a protocol call ENUM. [18] Though the question whether domain names will always be the sole or predominant means of navigating the Internet, or if they may be supplanted over time by other systems, is an important one, to be mindful that we do not wed public policy interests to a technical architecture that is may change. Nevertheless, it is wrong to presume that the importance of names is decreasing; rather it may increase. What this points to is that either way, domain names are significant, not insignificant as some critics believe.

* *Internet Protocol Numbers:* These are the digits that, though usually invisible to users, enables the digital traffic to be routed through the network. Under the current version of Internet Protocol, there are a potential 4 billion numbers to circulate; a new version, called IPv6, will allow for a quadrillion IP number addresses. Despite the theoretical wealth of addresses, they are a finite resource and their allocation must be made carefully to prevent depletion or accidental duplication of number assignments. Three main bodies, called regional Internet registries (RIRs) allocate numbers, ARIN in North America, RIPE in Europe and APNIC in Asia; new RIRs have recently started in Latin America (LATNIC) and Africa (AfriNIC).

* *Root Servers:* These are the large computer servers match the domain names to designated IP numbers (and vice versa) so that traffic is routed correctly. The master database is called "a.root-servers.net"; it contains the authoritative data of domains and their corresponding IP numbers, which it sends regularly to 12 secondary root servers, lettered b to m. (Because of the way IP packet headers are designed, there is a limit of 13 root servers). The servers are operated by US government-related entities as well as private companies, academic institutions and technical organizations; three are outside the US, in London, Stockholm and Japan. However, due to a technical enhancement, "mirror" root servers that contain the same data are possible; roughly 50 are currently spread throughout the world. The data in root servers must be identical, or the Net will not interoperate perfectly everywhere. [19]

* *Protocols:* This is the underlying computer code, or "language" of the network. It, as well as all enhancements that are developed, must be standardized among all devices connected to the Internet, or they will not interoperate smoothly. Likewise, the network software relies on using certain agreed parameters (for example, Web traffic is handled on "port 80"), which unless universally recognized, will undermine the Internet's interoperability. These technical standards are the responsibility of the Internet Engineering Task Force, an open-membership non-governmental organization that operates as a meritocracy and eschews formal voting in favor of rough consensus. The assignment of networking parameters is handled by the Internet Assigned Numbers Authority, the name of ICANN's predecessor organization, which today is a few individuals managing these technical details. [20]

These four areas are where some centralized coordination is necessary to ensure the Internet's global interoperability. For a distributed network, it marks the rare places where control over the Internet is possible, and where some sort of institutionalization of management is required. [21]

B. Internet Balance-of-Power Considerations

Yet there are a number of factors that create a sort of balance-of-power among the central Internet coordination entity (e.g. Jon Postel or ICANN) and those whom it affects (e.g. users or sub-networks). First, the Internet is only a protocol, only an agreement; it operates on consensus among network administrators and device software programmers to adhere to the Internet standards. There is nothing to prevent any group from using their own standards, other than the disadvantages of lacking interoperability with others. In fact, many groups have sought to create "alternative" domains (e.g. .web or .sex) to compete against the ones sanctioned by the Internet's standards groups (i.e. .com, and more recently, .info), but have failed to achieve widespread support. [22]

Second, there is an inherent tension between whether the Internet is a public or private infrastructure. It has the importance of a critical public utility, and in many instances, travels over public telecommunications infrastructure. However, it is deployed by the private sector and in many countries, historically received exemption from traditional telecom regulation (though this is now winnowing in most jurisdictions, including the country with the most hands-off policy, the United States). Likewise, the Internet technical community claims a significant amount of power over how the Internet infrastructure is managed, and tends to discount the legitimacy of the US government's authority. Meanwhile, there is a tension between the degree to which the US has authority versus other countries, through the aggregated power as administrators of their country-code domains (though this balance of force remains untested).

Thirdly, the domain name system is not actually a core function of the Internet Protocol per se, but an application layered on top of it. It seems indispensable only to users; in reality, traffic can still move about using only IP numbers, not names. For some applications, this is impractical, such as email. But for other instances, such as instant messaging or peer-to-peer file sharing, the domain name system is not used.

On a final note, a reason for the friction in the debate over “Internet governance” is semantic. As already mentioned, the meaning of the term has changed from originally referring to infrastructure coordination and now is increasingly used to include more general policy issues, such as spam or content control. Secondly, people -- particularly non-native English speakers -- hear the term “governance” and intuit that the government must necessarily be involved. (In English, the term “governance” does not have such direct connotations to government; i.e. people refer to “corporate governance.”)

A short explanation of how the term came to be is thus in order. In the early days of the Internet, the engineers needed to create terms for what were then new concepts; they generally appropriated terms from other contexts. To establish a technology that let people to interconnect their own networks with others required a lot of diplomacy. Unsurprising, this became the basis of the language they chose. Thus standards documents weren’t called “rules”: that would have been too off-putting. Instead, they were named “request for comments” -- as neutered a term as imaginable, for what were broadly imposed requirements. The networking language itself was called a “protocol” -- a word taken from directly from diplomacy. “Policy” described how to prioritize engineering parameters or different technical features for certain users.

With hindsight, we can see that it didn’t help matters that in the insular world of brilliant, underdog data communications engineers, there was a prize placed on being able to dress up mundane technical matters in ornate language, to humorously give it an air of intentionally *faux* importance. For instance, in 1989 Jon Postel created the Internet Assigned Numbers Authority to describe his role coordinating the infrastructure. It was meant as a joke, he said in an interview in 1997; he “made up an impressive sounding name.” [23] The idea of an “authority” over numbers would strike techies as something beautifully silly -- akin to a “Port Authority” referring to a person responsible for pouring a round of aged wine from Portugal, rather than overseeing a coastal border entry point for ships.

Likewise, the notion of coordinating Internet infrastructure was termed “Internet governance.” It followed in the tradition of “protocol” and “policy” and “authority.” But its meaning had nothing to do with governments. This, in the same way as the term “goodwill” has completely different meaning if it is used by accountants (to refer to an intangible asset that is valued above the market value of its net assets) or Santa Clause (“Peace on earth; goodwill to men.”) To presume that the expression “Internet governance” necessitates that governments handle the task would be as nonsensical as to believe that only carpenters should manage aviation issues because it involves planes. To be sure, there are numerous areas where governments ought to be involved -- but this responsibility shouldn’t be invoked on semantic grounds, as it sometimes is, at least mentally, by participants. To do so would set back the more complex task of figuring out in what ways the role of government is necessary, and in which ways it might actually undermine the very goals it aims to achieve.

3. What is ICANN

These four aspects of the Internet require some centralized coordination so that the network is completely interoperable for users everywhere. For instance, without a single entity handing out names, there may be more than one "apple.com" and email and web traffic would get misrouted. If the same happened with the numbering system, traffic would also be disrupted. If the protocol isn't agreed upon by all parties, users from one part of the network would not be able to communicate with users on another, and the result is that the benefit of the network for all would be diminished. If root-severs don't contain identical data, then the universality of the network may be broken. [24]

Prior to 1998, the task of coordinating these aspects of the Internet fell upon a single individual, Dr. Jon Postel, a computer science professor at the University of Southern California. His role -- he called the task the "Internet Assigned Numbers Authority" (IANA) was funded by the Defense Dept's Advanced Research Projects Agency (DARPA), and the role was cited in a National Science Foundation agreement to outsource the registrations in com, net and org. Between 1996 and 1998, responding to attempts by the Internet technical community to institutionalize Dr. Postel's role, the US government became involved. [25] US officials met with stakeholders from industry, academia as well as other governments, and solicited comments from users worldwide, before forming a policy known as the White Paper.

It called for industry to establish a private-sector-based group to manage the domain name system, with transparent and accountable procedures and a globally diverse board of directors. It would introduce competition for registrations in generic domains like .com, and create a process to introduce new domains. The US would have oversight authority for a transitional period, set at five years. In October 1998, the Internet Corporation for Assigned Names and Numbers was formed; on the eve of its birth, Dr. Postel passed away.

Today, ICANN holds three or four board of directors meetings each year, that are held on different continents and open to the public. Its 18-person board is comprised from ICANN's three "supporting organizations" (representing IP addresses, generic domains and country-code domains), as well as non-voting members from its four "advisory committees" (representing government, at-large members, security, and root-server administrators), a technical liaison, an ombudsman and ICANN's chief executive. Controversially, ICANN's proposed 2004-05 budget envisions expenses of $15.8 million, almost double of $8.3 million the year earlier; it also calls for a staff of 59 people, again, almost twice as much as the 33 staff from the previous year's budget. [26]

In fact, there is very little about ICANN that as not been controversial. In five years of operation, ICANN has had many eras, and has suffered substantial criticism at each step, some of it well-deserved, some of it not. The first two years were mainly devoted to opening up competition for selling domain names and establishing its own procedures and mandate; in that time, it had to overcome objections to initially holding closed board meetings and proposing an ill-conceived $1 surcharge on all domain name registrations to raise revenues. Congress held hearings annually in this time, when it felt ICANN was overstepping its bounds. In 2000, ICANN selected new top level domains in a chaotic process that lacked responsible procedures; also, it held an election for three at-large board members that teemed with voting irregularities. In 2001 it sought to attain support the Internet community of country-code domain administrators and the regional Internet registries, who balked from agreeing to ICANN's excessively stringent contracts, at a time when the organization failed to adhere to its own standards of transparency, accountability and process. ICANN for a time actually refused to respond to requests for technical changes by county-code domain administrators as a way to induce them to sign the contracts with which they disapproved.

After 9/11, security obviously became a major focus. In 2002, realizing that it failed to achieve the support of Internet stakeholders, ICANN introduced a reform process that centralized power slightly, yet spread board membership to a wider group. The reform also eliminated directors elected among Internet users at large, the one cohort of the board that came from outside the ICANN establishment, and which in practice had voted differently than the near unanimity of board decision until then. [27] In 2003, it lost a court case by a director who complained that ICANN failed to provide adequate transparency of information to which he was not only legally entitled, but legally bound to inspect. In its first five years, its budget and staff swelled. The US government, across two administrations, kept a vigilant watch on ICANN but a relatively hands-off approach to its day-to-day operations. It used its contracting procedures to demand improvements from the organization. [28] In 2004, the United Nations appointed a Working Group on Internet Governance to consider the role governments should play in both managing the domain name system, as well as broader areas of Internet policy. [29]

During this time, the US has remained supportive of ICANN as a concept, but expressed dissatisfaction with certain ways that it operated and requested numerous substantial changes. It has declined to comment publicly other than through occasional press statements, leading some observers to speculate that the US is rethinking its 1998 policy on handing over control to ICANN. That the Bush administration has backed away from other international agreements, such as the Kyoto Protocol on the environment, the Anti-Ballistic Missile treaty and the International Criminal Court, has fueled the perception that the US, on Internet coordination as the war on terrorism, will follow a unilateral course.

Part II: Internet Infrastructure and National Interests

In terms of the Internet issues that the US and other governments most want to address -- cybersecurity. spam, content restrictions, e-commerce taxation, intellectual property, etc. -- the control of Internet standards and the domain name system infrastructure as it exist today means very little. Authority over ICANN doesn't help resolve the problem, or there are better ways to treat it. But if one wanted to change the architecture of the Internet to address these matters, then control over standards and the underlying infrastructure means quite a lot. This section treats the national interests all countries share concerning Interment management, before turning to the areas where the US has unique interests by dint of its currently authority over ICANN.

All countries benefit from, and have an interest in the Internet, yet for different reasons. For instance, trademarks are more important in the West than in the developing world, where the Internet is making an important impact more as a communications medium than for retail e-commerce, for which branding is essential. Sectors have different interests, such as supply-chain management operations for manufacturers in Asia, to entrepreneurs who use Internet telephony in Africa. As such, every country has an interest in the smooth running of the Internet, for economic wellbeing on a national level, and ordinary convenience on an individual level.

However, in certain instances, one country's use of Internet resources may interfere with another country's use: IP numbers need to be allocated frugally, without accidental duplication, with transparent processes, and equal access to them; domains in the root servers must be authoritative; delegations must be made openly and competitively; etc. If number allocation favored one country over another, it could have commercial implications -- for example, if Japan's Sony Playstation videogame console had its own IP number due to favorable IP number allocation, but US's Microsoft X-Box did not, because of unequal treatment. Likewise, if a valuable domain (for instance, .xxx for adult content) was allocated to one company or country due to an unaccountable process, which denied the same opportunity to others. Thus, some sort of legitimate, recognized international body needs to exists as a forum for dialogue, negotiation and decision-making authority. [30] This is not unlike other communications media; international coordination of information and communications technologies have a long history.

The difficulty for governments is encapsulated by a number of paradoxes: the Internet was deployed on mainly private infrastructure (leased lines for data communications) which has often been exempt from much traditional telecom regulation, though the Net often rides atop of the public telephone network. [31] Additionally, the Internet's technology was principally designed by a large group of researchers that spanned the globe in a open-source process, yet at the same time, the central functions of Internet coordination was funded by the US government, which on a legal level (albeit untested), the US government retains ultimate authority over Internet infrastructure policies. [32] Finally, it is not clear to what degree Internet coordination institutions should prioritize certain stakeholders, such as governments, industry, academia, not-for-profit organizations, etc. [33] History is an imperfect guild, for although the US government initially sponsored Internet development, its success is largely credited to the hands-off approach that it took.[34]

The notion of what constitutes a national interest has a long provenance, and is much debated. This paper, in a nod to simplification, will focus on a few broad interests that relate to the Internet, first looking at common interests of all nations, and then at ones that are specific to the United States, which could be affected by its decrease in influence over ICANN if it grants the organization autonomy.

1. Common National Interests

The Internet affects the national interest of all countries. This is true even of countries such as Burma, that feel threatened by the Internet, and seek to block it within its borders. Though many countries place restrictions on Internet content and use, this is mainly for political speech, pornography and to preserve the revenues of state-run telecom carriers from Internet phone calls. [35] Significantly, the Internet's main benefit, particularly in the developing world, is not in the content that is created and viewed but the community that it engenders, which is the bedrock of civil society institutions, intellectual dialogue and exchange beyond mere information transfer (web pages), transparency, and the community discourse that is a prerequisite for establishing a civitas and, hopefully, democratic governance. [36] This power of the Internet for community rather than content is also a hallmark of how the Internet is taking hold in developed countries as well, though the content is often more noticeable than the slower, more subtle changes in how the technology shapes group formation and behavior. [37] With that in mind, a look at common national interests in the realms of security, economy and the socio-political dimension.

1. Security

Communications and media resources have long been a matter of national security for all nations. The reason is generally three-fold, First, the use of the system is vital for protecting the country (indeed, the Internet itself was created in part as a means to assure continuous communications in the event that the network was partially destroyed). [38] The role of the Internet in this respect was made apparent to all nations on September 11, 2001, when the telephone system malfunctioned under calling strain, but email messages continued to pass through [39] Second, it is a national security matter due to the physical need for communications infrastructure from one nation to be present on foreign soil (the so-called "landing rights" of telecommunications cables). [40] Third, and more significant, is the content of media itself; the control of information is one of the most important powers of modern states, from the ability to control broadcasting on one hand [41] (through ownership of "state-run" media, or regulation of radio spectrum), to the potential ceding of certain amounts of sovereignty due to unauthorized broadcast or satellite transmission on the other. [42] For instance, Warsaw Bloc governments were miffed by the transmission of Radio Free Europe (though their people weren't), just as the Chinese government was concerned about Western television infiltrating from satellites overhead (again, though their people weren't). Eastern Europe unsuccessfully blocked the former using technology; the Chinese very successfully blocked the later, using commercial law.

The Internet in some respects represents a new iteration of these concerns; there is both a hard infrastructure component to the Internet, the transmission network (for instance, the cables or less tangibly, radio spectrum), as well as a media component, that is, the content that is transported over the network. There is much to be said in these aspects of the Internet related to national security, but the issues are fairly well understood, since it's simply a question of extending the challenges of earlier technologies, from telegram to television to fax machine, and applying it to the new medium.

More interesting is how the infrastructural coordination component of the Internet itself relates to national security concerns. The question of control of Internet infrastructure affects the national security of all nations, both on a discrete, national level as well as at a global level. (This, in the same way that the environment can have domestic implications but due to the interdependent nature of the issues, the global situation have national stakes involved.) To be sure, national security is far from the most dominant aspect of the network -- the Net means much more on an economic and social level (treated in the sub-sections below) -- however, it would be incorrect to say that there are no implications on national security.

A. National Control of Country-Code Domains

First, is communications and content reliability and confidentiality. Many governmental institutions are online and use the Internet to send important information, much of it considered classified. Thus, countries have an interest, on one level, on having control, indeed sovereignty, over their two-letter designated domain, for the stability and assurance this provides them as users of the network themselves. Lack of sovereignty over one's country-code domain does not necessarily give a third party the ability to eavesdrop on conversations [43] but it could be used to disrupt traffic flow, by intentionally or accidentally misdirecting it to another address, or intercepting it.

Moreover, countries have an interest in using this control over their country code domain on a domestic level as leverage to assure the proper order, functioning and stability of the system as a whole; that is from the internal or national level, to the systemic level, of the global Internet itself. [44] This is relevant because, controversially, countries do not have sovereignty over their country-code domains today, as they do, for example, over telephone country-code and their national numbering plan; also, they have only minor influence over the domain name system as a whole due to ICANN's private-sector structure, on one hand, and the US's preponderance of oversight authority, on the other. (For more on this, see "Appendix B: Country-Code Domains and National Control.")

B. Stability of Root and Security in Standards

Likewise, countries have a national security interest in the management of the root-server system, to ensure that the data indicating the administrator of the domain is authoritative.

If the data were not authoritative by accident or intention, the universality of the Internet - whereby any user can reach any other -- would break, as traffic would not be routed correctly. Furthermore, if the root-server system failed to operate due to technical or security reasons, it would disrupt the traffic flow of the Internet globally. The root server system is completely redundant; if one fails there are many, many more with spare capacity to take up the slack. [45] Many root servers themselves have come under attack by hackers in recent years, and though the system has withstood these assaults [46], the matter underscores the extreme seriousness of the issue and the need for proper technical and security management. Lastly, it is feasible (though extremely impractical) to identify who is communicating to whom using detailed logs from the root servers, however grossly imperfectly. [47] Thus, the root-server system needs to be under trusted management.

The development of the protocols for the Internet also matters for national security, since it can further political objectives. The values that the network embodies can be established by the computer code. [48] As such, the technical standards that are adopted can affect many social and political dimensions of the medium that is generally considered the purview of governments, such as the degree to which citizens can exercise freedom of speech and the amount of privacy protection that exists. Countries may find that their national security can be effected by decisions over Internet protocols, such as ensuring anonymity of traffic flows, or building in strong identify and authentication features, as well as wiretap capabilities, possibly for law enforcement purposes. [49] Additionally, as the Internet becomes a potential vehicle for attack (that is, not attacked itself, but the method of attacking the information technology systems of others), the issue of the tradeoffs between freedom and security in the computer code of the network itself becomes a serious matter for which governments will see national security interests. [50] Three of the four so-called “ICANN functions” -- names, root servers and protocol standards -- therefore relate to national security. The fourth area, IP numbering, is not central to security issues, though have critical economic interests, treated in the next sub-section.

2. Economy

The second half of the 20th century has seen most prominently the issue of the national economy emerge as a vital national interest, concomitant with national security. Indeed, in some instances, it is not easy to tell the two apart. For example, in the case of oil, it is a natural resource that affects both national security and the economy. In the allocation of other shared international resources, for instance geo-stationary satellite orbital space, national security and national economic welfare are inherently linked. Elsewhere, so-called “soft issues” of international relations are being understood in the framework of economic interests, such as health, the environment and human rights. For example, the National Intelligence Council in 2000 called infectious diseases in the developing world a matter of US interest due to the negative spill-over effects if could have on the US economy. [51] Second, human rights is managed by the State Dept. with an ambassador-level official, managing the “Bureau of Democracy, Human Rights, and Labor” -- a name highly evocative of the interplay between foreign policy and economic interests. These examples signify the degree to which transnational “soft-issue” concerns are being understood in the context of their impact on national economics.

Likewise, the Internet. Though it represents matters of national security in the ways identified above, it holds its greatest importance to national interest in the economic sphere, by among other things, lowering transaction and switching costs, and boosting productivity. Much can be said about this (and already has, elsewhere) so this discussion will focus on identifying the degree to which infrastructure coordination, rather than the use of the Internet more broadly, affects economic interests.

The Internet is a resource, both non-rivalrous and at times rivalrous, in its allocation and use. It is non-rivalrous -- in that the use of it doesn’t deplete the resource or impinge on others’ use of it -- in areas of the operation of the root servers, or technical standards; indeed, in these examples, all users of the network need to use the same root system, and incorporate the same technical specifications. However, some infrastructure coordination resources are rivalrous. For example, IP numbers: one entity’s use of a block of addresses space denies others the opportunity to use those numbers. Meanwhile, in other instances, the infrastructure coordination area is both non-rivalrous and rivalrous, such as in the creation of a top-level domains. Creating the domain .aero, for example, denies all other entities a domain with those exact letters -- there can only be one. Yet at the same time, it is relatively easy to generate other domains technically. [52] Still, because the number of meaningful and valuable character-strings are limited -- though the extent of which is an open debate -- it is essentially the case that domains are rivalrous. [53] This context is helpful in understanding how Internet infrastructure coordination issues affect the economic interests of all nations.

A. Commercial Innovation and Standards

The first area where countries have an interest is in technical standards. This has been a fertile area of intergovernmental dispute for centuries, over many technical iterations. In fact, it was the need to resolve international standardization disputes that led to some of the earliest intergovernmental organizations [54] -- an important historical reminder that the issues we face today are not so novel, and the degree to which countries willing cede small degrees of sovereignty to obtain the benefits of cooperation has a long lineage in international relations. Standards have often been used as commercial weapons; the lack of interoperability has been a means for the entities like a state or a company to retain control or maximize profits (as anyone who has traveled across Europe with a suitcase filled with different phone and electrical adaptors can attest). In the case of data communications, Countries often stump for the standards of their companies, be it Europeans for the inferior OSI data networking protocol in the 1980s, which was defeated by the Internet, to the current drive by the US to support San Diego-based Qualcomm’s wireless standard for third-generation mobile phones.

Out of this history came the Internet, which bypassed all the politics and commercial fuss. The reason for this is manifold: it was driven by techies not politicians or businesspeople; the protocol, as earlier noted, was a base-line system so was kept simple and gave great autonomy to sub-networks; it was made freely available on a non-propriety basis; it was developed in an open source style process, relying on the decentralized activities of technical engineers worldwide. As a result, Internet standards are free to use, developed openly and non-politically (albeit with fierce commercial interests), and universally accepted -- leading to complete interoperability so any user of the Internet can interact with any other. (The same cannot be said for applications atop the Net, such as instant messaging, among other things.) Development is faster and possibly better than proprietary protocols because the open source system harnesses the engineering talent from around the world, and operates as a complete technical meritocracy. The Internet's standards body, the Internet Engineering Task Force, is open to all. This is in contrast with how international standards are generally made and maintained. For instance, consider the approach taken with telephone standards, which relied on an intergovernmental treaty organization, the ITU, whose members were from governments, and which was costly to join for corporate members and the standards themselves until recently were costly.

The Internet's technical standards provide universal connectivity, low cost of access, and low barrier of entry for firm entering any area of the market that relies on Internet specifications. Moreover, the technical specifications themselves specifically design a network whose characteristics are open and decentralized, due to its end-to-end approach (as described in Part I). And this, in turn, leads to the Internet's hallmark: a network where the users define the purposes to which it's put, and is capable of continued re-invention or revolution. As an open medium, with little centralized control at the core, the network itself requires no pre-approval for experimentation and makes no presumption about what applications run over it.

This network design has made the Internet the motor of technical innovation that it is, and has led to many benefits for users -- but is it extremely unsettling to large commercial interests that become vested in one technical approach and then seek to preserve that status quo for commercial gain. Thus, there is an inherent tension between the interests of large, wealthy actors (companies, and the states that are responsive to organized interests, and financial interests) and the disaggregated interests of individual users and start-up companies who claim the benefits of the Internet's decentralized design. As such, where some countries will find that maintaining the Internet's current openness is in their economic interests, other countries will not. For instance, today, the West generally seeks to preserve the open character of the Internet, many developing countries try to filter or block the Internet to preserve the revenues of their state-run telecom operator from competition by Internet telephony, or to retain their hold on information. [55]

B. Services and Devices Related to IP Numbers

Another area of economic interest is Internet Protocol address space. IP numbers affect the types of services and number of devices that can be deployed. There is a way for companies to create their own numbering system that would then interface with IP numbers -- called network address translations -- but this breaks the end-to-end nature of the Internet. The reason is that IP numbers are import is because they allow devices to connect directly to other devices, without the need of an intermediary, such as a telecom operator or technology service provider (which could then charge more for it, lock-in customers, or add features that make it not fully interoperable with rest of the Internet for competitive interests).

Access to IP numbers are important to countries and companies; as noted above, IP numbers are a rivalrous good. Mobile phone manufacturers lose a degree of technical freedom if they are unable to embed an IP number into each handset. This changes the commercial dynamics of the communications medium, by either making phone makers and thus users independent of the wireless operator who provides coverage and service, or making phone makers and users dependent on the wireless providers by dint of their supplying their own network routing number rather than an IP number if the latter is difficult to obtain. (A telephone number in this example isn't analogous, since it is more like a domain name, the superficial wrapper used by people, above the underlying routing number used by the infrastructure itself to establish the communications.) This affects the competitive structure of the Internet, the cost of access and ability for innovation to take place.

To show the political stakes involved in IP numbers consider a real incident: At an ICANN board meeting in Marina del Rey in November 2001, two months after 9/11 when the world was focused on terrorism, a senior Japanese official flew 20 hours for a two-hour visit to meet board members and speak publicly, only to fly 20 hours back to Japan. The reason: IP numbers are considered a critical resource for Japan's national economy because of the country's consumer electronics industry. [56] As devices like cameras, televisions, stereos, dishwashers, cars -- and eventually watches, pens, eyeglasses and probably someday medical prostheses -- start to interact with each other over networks, access to IP numbers is essential. IP number allocation policy is, ultimately, ICANN's remit, and thus a priority for governments; Japan was just one of the first to recognize this, and at the highest levels. (China understands this also, and formerly complained that the allocation process was inequitable. In early days of the network when the Internet was used mainly for data-communications research, enormous blocks of IPv4 address space were allocated to US companies and organizations; in the mid 1990s, Chinese officials noted that there were more IP addresses at Stanford University than in the entire Middle Kingdom. As China has deployed the Internet nationally at one of the fastest paces of any country, it was able to obtain the IP number allocation it has required, under policies set by the regional Internet registry, APNIC.) [57]

The importance of IP number policy for national economic interests is that the policy process, in formation and substance, must be fair, open, transparent, accountable, handled in a technically competent manner, adaptable to changing circumstances and independent of short-term political or commercial pressure or interests. The move from IPv4 to IPv6, which offers many orders of magnitude more addresses, may alleviate many of the tensions over access to numbers, but it does not change the underlying economic reality that IP numbers are finite and rivalrous, and require some sort of centralized management. On a political level, a concern among engineers is that IP number allocation will be politicized and social objectives rather than technical ones will determine their distribution (i.e. instead of being based on the topology of the network as technical experts recommend, it be based on factors like geographic size or population. This examination does not want to address the argument, but simply explain how IP numbers are a matter of national economic interest.

C. Online Identity and Domain Names

After standards and IP numbers, a third area of Internet infrastructure coordination with an important economic impact are also the most apparent: domain names. The Internet can function without the use of domain names, in terms of the infrastructure of the network, but they represent an essential element of the Internet to make the medium accessible by users, who rely on for things like Web pages, email, and grace of new technical standards, soon telephone calls and -- of course -- other applications not yet dreamt up. As such, the stability and reliability of the domain name system, and particularly the names themselves, are of paramount concern to business and government. As names are used for personal communication as well as automated computer-to-computer communications, and the Internet becomes the platform for global supply-chains, the smooth functioning of domains are critical.

There are two levels with which to consider the importance: for top-level domains (that is, the .edu in “harvard.edu”) and the second-level names (the “harvard” part). National management of top-level domains provide governments the ability to shape how the Internet is used. For instance, it can be a means to promote or restrict freedom of speech (by legally allowing, for example, “companysucks.tld” or banning, for instance, “religiousgroup.cctld”). This power over language is enormous, insofar as it enables governments to impact freedom of assembly through how Web sites can be used as virtual forums, as well as freedom of thought, since language is the bedrock of memory and discourse, and only in totalitarian regimes is it the purview of the state. [58]

Moreover, domain provide governments a means to impose public policy objectives, such as to protect intellectual property rights (by requiring digital tagging of content and certifiable domain ownership) as well as to collect e-commerce tax revenue (by requiring registrants to identify if the Web site is a commercial venture, which Australia does). Policies also impact privacy and free expression, insofar as whether anonymous communications are permitted or if all registrants must accurately identify themselves, as is the case with .com and .us registrants, under US law. [59]

For names, at the second level, governments have an interest in trademark protection, so users have predictability in the infrastructure and companies have a rational legal regime to invest in branding sites. One of ICANN’s first tasks after it was created in 1998 was to establish a globally applicable Uniform Dispute Resolution Procedure (UDRP), to streamline trademark disputes internationally and cut down on the incidents of cybersquatting, that is, the bad-faith registration and subsequent ransoming of domain names. ICANN deferred to the World Intellectual Property Organization, which oversees the UDRP. The system is highly controversial, due to inconsistent rulings by panels, particularly depending on size and region, [60] and a bias that many experts believe grossly favors established trademark interests against the individual and public good. [61] Still, there has been a move by ICANN to encourage country-code domains to apply the UDRP to name disputes in their territory. Without taking a position on the UDRP specifically or the state of intellectual property for domain names generally, it is clear that some sort of balanced rules must exist to protect the interest of consumers, businesses, and individual freedom and expression.

D. Universality of Communications and Root Servers

Finally, root server deployment is a matter of economic interest. To return to the formulation at the start of this section, root server deployment is in an ambiguous state of being both rivalrous and non-rivalrous. This precarious description is explained because on one level, root server deployment used to be rivalrous, As noted in Part I, due to technical reasons their number once was limited to 13 servers. However, that limitation has been overcome over the past few years with the use of mirror servers and so-called "anycast" technology that enables a root-server query to identify the closest mirror root-server -- an important factor for quality of service of Internet traffic and cost of bandwidth, in cases where root queries were going to servers outside the country or region.

Now, it is almost fair to say that root server deployment is no longer rivalrous except for symbolically (i.e. the desire of a country to operate its own root server, for reasons of national prestige, though no tangible benefits accrues from it). This is placed in the conditional because there it a slight rivalrous advantage to be had by managing one of the 12 secondary, or "slave" root servers. It is the possibility of establishing a coalition to deviate from the sanctioned "a.root-servers.net" master database to delete a domain, add a domain or change the administrator of a domain outside of established Internet coordination procedures, in the hopes of generating a critical mass that would encourage the rest of the network to do the same to maintain its universality. This, in the unforeseeable case that an entity or group wanted to do that. It would, of course, risk fracturing the interoperability of the Internet that has been one of the key reasons for the Net's success. (This issue is developed in Part III, section 3.)

Taken together, all four of the core Internet management functions -- protocol standards, numbers, names and root servers -- are a matter of economic interest to all nations. It bears repeating that the chief importance of the Internet isn't in these things at all -- it's in the usage, the content, community and business processes that happens over the network that this infrastructure enables, not the infrastructure itself. That said, the system of management for the infrastructure must be recognized as a common economic interest.

3. Socio-Political

The third area where the coordination of the Internet infrastructure is a matter of common national interest is in political society. This encompasses interests that don't properly fit into the previous two categories, because here, the issue is more on an informal social or political dimension rather than the formal structural realm of security or economy. In this instance, it concerns a society's culture, values and mores. It is also where other stakeholders than governments or industry feel they have particular relevance, and certainly more influence, than in the previous two areas of national interest.

Of course, the Internet is used for education, health care, community-building, religion, politics and entertainment, among a myriad other things -- but these refer to usage of the Internet. Additionally, the role of information and communications technologies broadly have been identified, appropriately, as matters of human rights [62] This examination will go beyond these aspects and specifically look at how the management of the infrastructure is a socio-political interests shared by all nations. In some cases, this is for symbolic reasons (i.e. a sense of equal responsibility to oversee the network to which we are all affected, whose very defining characteristic is interconnectedness); in other cases, it is for practical reasons: to shape the direction of the technology to ensure it aligns with a society's community values. [63] Four main areas are considered: First, domain names (including personal privacy, name terms themselves, internationalized domains and funding mechanisms). Then, IP numbers; thirdly, standards; and lastly, the "soft issues" of societal concerns: empowerment and symbolism.

A. Privacy, Freedom, Globalism, Innovation: Domain Names

Domain names have security interests and economic interests; they also have social interests, which although less easy to measure than economic interests, is nevertheless important. There are roughly 65 million domain names registered, of which almost 60% are under generic domains, .com, .net and .org -- the remainder are under country-code domains. [64] The use of generic domains tells a paradox: both completely global in use, while at the same time de facto US national domains. Current figures are hard to obtain, but as of 1998, over 75% of registrants were from outside the United States. [65] This makes their importance all the more considerable for everyone.

The first area where domain names are important is privacy. The world's most popular generic domains, .com, .net and .org, require registrants to identify themselves in a public database, called WHOIS. Failure to do so contravenes ICANN regulations [66] and may violate US law if legislation considered in 2004, called Fraudulent Online Identity Sanctions Act, is enacted. For the moment, inaccurate or misleading data can be cause for a domain name to be revoked, especially in cases of a name dispute brought under the UDRP. [67] The reason for this is the predominance of intellectual property interests in the ICANN process. It was one of the earliest interests groups to organize and has helped frame the agenda since before ICANN's creation; indeed, the early documents concerning Internet management by the US government [68] identified trademark issues as central to the debate, and among the first acts of ICANN was the establishment of the UDRP, based on WIPO's policy.

However, the WHOIS issue is controversial on privacy grounds, and has been the subject of many studies and reports. [69] Originally, WHOIS was to help network operators identify the managers of other sites online, when there was little different between the person running the domain and the person overseeing the network or computer lab. This of course is no longer the case -- though the requirement for public disclosure of name, address, telephone number and other data remains obligatory. Why didn't the policy change as the Internet went mainstream? On one hand, it was a part of the Internet's ethos for openness; here, perhaps too much. On the other hand, there was considerable pressure from intellectual property lawyers wanted to ensure an accurate WHOIS system because it makes identifying the source of potentially infringing material online easier. However, there is good reason to believe that the policy, reaffirmed by ICANN, violates European privacy and data-protection laws. The ICANN's policy requirements has global ramifications, and if the US legislation is enacted, it will have extra-territorial effects, though is not unlawful per se. ICANN is well aware of the matter, and has set up a process to study it and make policy recommendations. [70]

The identification and public disclosure of domain names effects privacy and anonymity online, which in turn affects other social values such as free speech, assembly, worship, etc. For example, people may not feel at ease in creating a web site to share opinions on a topic if one's name is known. It is a timeless question of liberty versus authority -- in short, the degree to which criticism is permitted to promote progress in an open society. Throughout history, anonymous and pseudonymous speech have been important cornerstones of dissent and freedom, from the graffiti scrawled on the walls of La Sorbonne in the Paris student demonstrations in May 1968, to Hamilton and others' Federalist Papers (signed "Publius" among other names) that helped found the American government, to persecuted Catholics throughout the Roman empire prior to 250 AD, who secretly used the sign of a fish to communicate their faith to others. Domain names are the foundation for the equivalent digital forms of communication online.

In addition to privacy concerns of domain names are interests related to the content of the names themselves, the words used. There are three dimensions: restrictions imposed by trademarks (particularly concerning unflattering names used for protest), the responsible evolution of new top-level domains, and internationalized domain names). The ability to chose names is a critical component of economic value, as mentioned in the previous section. This is for branding and commerce online, though the process of settling name disputes seems to favor large trademark holders. In the case of names used for to express protest -- the infamous "companynameSUCKS.com -- authorities have ruled that it creates trademark dilution and causes confusion in the market. In other instances, names that are similar to well known names have not been permitted on grounds of violating trademarks, customer confusion or bad-faith registration (a basis for revoking a domain under the UDRP). [71] It is clear that a reasonable balance must be struck between the permissibility of domain name words and the rights of trademark holders. To defer to corporate interests above individual or societal interests, as critics say currently happens, due to the degree that these interests are organized, institutionalized and the economic clout they posses, may suggest a need for readjustment as the Internet develops.

The issues that appear at the second-level names also matter for the top-level domains. The terms chosen for domains initially had little true meaning; for instance prior to our being flooded with references to .com, it would not be apparent that the three-letter abbreviation refers to "commercial" -- in fact, most users today would probably not know this. Others like .org, .net, edu, .mil and .gov are semantically relevant, yet as the Internet evolves, they will likely become more so, as decisions are based not on engineering efficiency among a homogenous group of people, as they had been, but among a broader number of stakeholders with more diverse backgrounds, nationalities and values. Any entity that coordinates Internet infrastructure will have responsibility over establishing new domains, and that means choosing the actual terms and, possibly, their purpose. (This latter, because "closed" domains are designated for a special purpose, such as the current .museum; or because the term itself will serve to identify the sort of content that can be expected to be placed within that domain, such as the current .name or .pro, for individuals and professionals).

That role of selecting the names represents an enormous responsibility, since the name will be globally visible online. It requires an enlightened appreciation of the responsibility this confers, to assure a dignified evolution of the network which encompasses the values of different cultures. Moreover, great care is needed to ensure that, on one hand, a term does not offend others, and on the other hand, that choosing a term doesn't restrict free expression or free thought, or attempt to "zone" cyberspace. This matter has come up in two instances when ICANN selected new domains at a board meeting in November 2000. In one case, during the debate over granting .air to an applicant representing the aviation industry, the Societe Internationale de Telecommunications Aeronautiques (SITA), one non-English speaking board member at the last minute argued that it was unconscionable to delegate the term "air" to anyone, since the air belongs to everyone. Other board members did not object, and as a result, .aero was allocated instead. [72] At another moment during the same meeting, the board considered adopting as a top-level domain the proposed term .sucks. Beyond the trademark issues at stake (companies arguing that any such suffix to their name being an injury to the value their brand) the board of directors appeared unaware that the word might be offensive to some people, particularly non-English speakers who could be exposed to translations based on etymological denotation rather than current connotation of the word (see note). [73] A third incident, concerning the idea for the domain .sex, raised in an intergovernmental meeting, is discussed in the next section. The point here is that terms involved with name selection is a social and political interest to nations.

Yet the content of the name selection doesn't have to be in English, or using the Roman alphabet. So called "internationalized domain names" -- names that are written in scripts of different languages, not just the Latin characters, which the domain name system once used exclusively -- is an emerging development. It is necessary, in order to bring the information society to all people around the world. Agreed standards are necessary, or the internet will not be interoperable, and the inevitable cleaving off of greats swaths of the

Internet based on language would happen also on a technical level, which is far worse -- language translation can always happen if sites and emails are retrievable; if they are not even reachable, the single communications platform that is the Internet will be balkanized and of less utility for all. (This is of particular concern for national economic interests as well: in cases where the domain names are not merely used for human-to-human communications, but for machines and automating business processes, where seamless and assured interoperability is essential.)

All nations, on a governmental and societal level, have an interest in how internationalized domain names are chosen, especially when they are not under the two-letter country-code domains, but if or when domains must be selected in local scripts, that are entered into the root server system and are globally visible across the Internet. For example, will there be a .chinese (representing the language) or a .china (representing the country)? If the latter, will the registry be managed by a (presumably) an entity such as a Chinese academy of arts and letters, or by the Communist Party?, considering that the choice of administrator may effect the registration policies, which in turn affect free expression. Likewise, in the case where the language, not country, is represented by the top-level domain (i.e. .chinese), the question still arises over who administers the domain; for example would the entity be based in China, or outside the country where tens of millions of Chinese speakers live (notably Singapore, Malaysia, and the United States -- not to mention Hong Kong and Taiwan), and who have an interest in the registration policies regarding how their language migrates online. These are the social and political challenges that internationalized domain names pose, which is a matter than falls under ICANN's remit. It is important to note that Internet coordination institutions have previously done a poor job of incorporating the interests of the least powerful or economically developed nations into its practices, though there are encouraging signs that this is changing. [74]

The final area where domain names are a social and political concern is in the funding mechanism that ICANN determines for operating a domain, as a way to finance ICANN's budget requirements. Currently, ICANN receives a small proportion of revenue from generic top-level domain administrators based on the number of domain registrations that take place. However, this approach, though seemingly rational, actually has a shortcoming that is only just becoming apparent: It bolts financial interests and political power to one model of domain name registrations, with the unintended consequence that it presumptively forecloses other possible models and indeed uses of the domain name system. The role and use of domain names have changed in the past 20 years since they were first introduced; the quantitative change has led to a qualitative one, just as the Internet itself changes as it continues to scale upwards.

From 1985 when the domain name system was created to 1992, domain names mainly identified users associated with sub-networks, academic computing centers, large corporations and organizations; under 20,000 were in use. [75] From 1992 to 2002, as the Internet grew into a mainstream medium, the names identified Web sites and email accounts for individuals as well (in 1995, the year Netscape went public, there were 120,000 names; by September 2004 the number was almost 65 million. [76] Yet they now serve as telephone numbers for some applications; they are used as passwords for many Web sites; and they are often relied on as the most efficient and permanent means of communications for people, when traveling, changing jobs, etc. Today, we often take this for granted, but it is important to realize that 15 years ago, this was not the case. Their role is still undergoing change and will continue in the future -- for instance, there is a serious attempt by the .aero registry to use domain names to identify every airplane flight in the world every day, as a service for aviation professionals and travelers -- but this sort of innovation is affected by ICANN's financing model. (For a fuller discussion on this point, see "Appendix C: ICANN's Registry Funding and Domain Name Innovation.")

B. Services and Ease-of-Use: IP Numbers and Standards

Beyond the role that domain names play for social and political values of privacy, free expression, local languages and internationalization, and innovation, other areas of Internet infrastructure coordination also have socio-political interests, namely, with IP numbers and technical standards. Moreover, there are interests on the level of individual and collective empowerment, as well as the symbolism associated with globally shared governance.

Regarding IP numbers, the policies governing their allocation and maintenance can either make the Internet more or less useful to people, and effect the prices people pay for services and access. This is because not all numbers are equal, for so to speak -- there is a difference between numbers that are "static" (that is, the same at all time) versus those that are "dynamic" (that is, different and changing because it is designated by the network providers each time a users logs on to an Internet). The latter system allows an ISP to have more customers than it has numbers, under the presumption that not all customers will be logged on at once -- a presumption that is increasingly incorrect in the emerging world of ubiquitous always-on broadband access and wireless connectivity. Static IP addresses are more valuable than dynamic ones because many applications rely on the user having an IP numbers that is constant, such as accessing one's computer from a remote location.

Yet, IP numbers are considered non-portable. They are the property of the ISP and individuals are not allowed to keep them when they change service providers. There are two reasons for this: first, because the current batch of IPv4 numbers are relatively scarce, at 4 billion, compared to the number of users and network-enabled devices today and in the future. Second, due to the current state of network routing efficiency. To let users retain their IP numbers would be to disrupt the way that IP numbers are aggregated, or subsumed, into large blocks of IP address space. This is important because it lets routers do less work in looking-up where each packet of data should be directed as they flow through the network, which in turn means faster speeds and better quality of service. Today, engineers say there is little way around this -- but must it always be so?

Access to IP numbers and portability for individuals is a useful objective. It would allow users to be independent of service providers while still retain high-function services that may require static IP numbers. While today this may seem arcane and technical rather than a mainstream socio-political interest, it is useful (and humbling) to consider that the idea of personal computers being a general interest concern and international development priority was also considered overly-technical matter and bizarre, a mere 30 years ago. [77] Today, these matters are common place and important at the highest levels of public policy, as the UN's World Summit on the Information Society makes clear. This, like the previous discussion on the future of domain names usage, points to the need for longer time horizons than we currently have when considering Internet coordination matters. Thus, there are social stakes involved in how IP numbers are handled.

Socio-political interests are also affected by Internet standards, although usually not directly. Most of what affects social interests are outside standards issues. Nevertheless, standards play a role regarding freedom of experimentation, cost of access, barrier to entry to provide services, and ease of use of Internet technology itself. Often, these values are achieved through software interfaces that build upon or make useful the networking standards that are developed -- one case in point is the Web; a second is the Web browser, Still, the development of technical standards can make the Internet easier for ordinary people, not engineering experts or even literate people, to use. Internationalized domain names, discussed above, is one clear example. The domain name system itself is a standard, without which the Internet would be a less friendly and manageable medium.

Standards bodies are aware of the role they play, straddling technology, public policy and usability. For many years, the IETF had a User Services Area run by Joyce Reynolds of the University of Southern California's Information Sciences Institute, and a longtime associate of Dr. Postel's, who was sensitive to this exact issue of ease-of-use, herself working in the technical community but not an engineer by training. Technology embeds values. [78] Looking ahead, some standards are bound to be offensive to different cultures or values. For instance, a proposed Web standard by the World Wide Web Consortium in the mid 1990s, called PICS, that allowed content to be tagged with a rating system, outraged free speech advocates who argued that it made censorship easier. [79] Internet standards bodies have had to decide on the degree to which the protocol was open to law-enforcement surveillance (an issue considered more in the next section). More such conflicts will surely arise in ways we cannot anticipate, other than to acknowledge that the development of technical standards for the Internet is a common socio-political interest for nations.

C. Empowerment and Symbolism

The final area of socio-political interest related to the Internet's infrastructure coordination is in less concrete areas: the role that Internet management plays in promoting individual and collective empowerment, as well as the symbolism of shared control over a global resource. While these may be considered “sentimental” matters relative to, say, economic interests, they should not be dismissed.

The way in which the Internet’s infrastructure is managed affects the degree to which individuals are able to exercise autonomy, and groups able to form. These values are the bedrock of civitas. At the same time, the openness or closeness of the medium impacts the amount of transparency and accountability to which the Internet can be put towards. This is the basis of a democratic ethos. While these traits of the Internet, autonomy and transparency (and their effects, civitas and democracy) are usually viewed as resulting from the use of the Internet rather than its underlying infrastructure, it can rightly be included here, since the technical architecture of the Internet inherently allows for these values, which would be thrown into jeopardy under any other sort of network design.

The Internet, as it is currently designed, inherently furthers the cause of human freedom; its decentralized and open nature provides for easy, widespread and low-cost access, and difficulty in imposing centralized control relative to other communications media (discussed in Part I). Like with the Internet’s end-to-end architecture, so too with its users: the autonomy and control generally rests at the edge of the network, with the people, not the center of the network, whether the authority is a service provider or government. Consider the ease or difficulty of censoring content: in a centralized network like the telephone system, where numbers are the purview of the state, carriers are licensed, and all traffic flows over a specific route with an entity at the center monitoring it (usually for billing purposes), censoring content like a mobile phone text message is relatively easy -- in fact, the Chinese authorities did so during the SARS epidemic in 2003. [80] Trying to do the same sort of content-based censorship over the Internet is also possible, but more complicated, because names are not necessarily managed by the government (though laws still apply), ISPs are not licensed (though, again, are under legal obligations), and the traffic does not follow a set path or be monitored (though they pass through access points and gateways where censorship can take place). The ability of the Internet to bypass censorship attempts is a distinguishing aspect of the technology. But the point is not about censorship; it is that similar to the issue of censorship, in many other seeming mundane areas, the Internet’s openness -- grace of the way its infrastructure is coordinated -- the network furthers individual and collective empowerment.

Importantly, this is not to argue that governments are impotent or ought keep clear of the medium -- on the contrary, governments have a role to play, in many cases are already playing it, and have many instruments at their disposal to do so. The issue, however, is that the management of the Internet’s infrastructure can either advance or set back values of freedom, both technical and political. This should be obvious, but the naïve idolatry that many of the Internet’s early proponents invested in the medium has led to a sort of backlash whereby it is fashionable to naysay the Internet’s ability in this regard. Today’s cyber-dyspeptics, like yesterday’s cyber-utopists, extol an extreme view; they are two sides of the same coin. What is needed is a balanced view. [81]

Lastly, the Internet coordination is a common national interest for symbolic reasons -- that the control of a global resource should happen on a global scale, with all stakeholders. For the moment, many governments are expressing a position that Internet infrastructure is insufficiently represented by government in general, and on a multilateral footing in particular, [82] requiring a dilution of the influence of the US government. The reason has more to do with symbolic representation of Internet management as an example of global interconnectedness, solidarity and common destiny than of any specific power that would accrue to other nations by placing Internet infrastructure coordination on an equal, intergovernmental footing. [83] In short: other countries don't want this power to actually do something with it, but because the US's position of dominance, here as in other areas, is unsettling to them. It doesn't help matters that the US's willingness to act unilaterally in other areas of international affairs gives rise to suspicions that it could do so in terms of Internet infrastructure as well. For example, a fear expressed privately by officials from governments that are allies with the US [84] is that in the same way that the US may invade a country or render moot a treaty, it might decide to revoke a country-code domain from the root system. This discussion is not to meant to indicate merit for those fears, only to aknowledge them.

Two factors are important in this respect. First, the internationalization of the management of Internet infrastructure is actually formal US policy, initiated by the US government. Other countries object to the way it is established (on a primarily, though not exclusively, private-sector basis) and the timeframe (without clear indication when the US will end its transitional oversight role). Second, the objection of other nations to the current dominance of the US and the interest for a shared structure for Internet infrastructure coordination itself is wanting from an internationalist perspective, because the multilateral principle that is advocated effectively privileges one set of stakeholders -- nation-states and their governmental representatives -- while ignoring other stakeholders that have similar and at times competing interests. (Ironically, some of the countries that are most vocal in seeking more influence over Internet infrastructure matters are the same ones that most restrict the Internet within their borders, be it controlling content or forbidding Internet telephony.) [85] All sets of stakeholders can speak for the communities and interests they represent, though obviously with different degrees of representation and legitimacy.

The multilateralism that is vaunted as the apex of the internationalist approach, which encompasses the global diversity of peoples and cultures, itself does not go far enough. It is rooted in the past, the Westphalian state-system whereby peoples' representation is the sole responsibility of the state [86] (akin to the nation's monopoly on the legitimate use of force, in the sociologist Max Weber's formulation). It misses a broader trend in foreign policy, whereby other stakeholders, particularly from industry, academic, religion and civil society are influencing international affairs. [87] To advocate a system that ignores these stakeholders is only a partial globalist approach, and bound not to endure. Ultimately, the common national interest in shared Internet management may promote the symbolic goal of international solidarity, but an argument can be made that it should encompass stakeholders from outside of government if it is to truly reach the objective to which it aspires.

This concludes the discussion on how coordination of Internet infrastructure is a matter of common national interest in regards to political society. On a final note, it is significant to remember that this list is not comprehensive and more interests will surely emerge, that are either entirely new, or are issues that will be identified tomorrow which we take for granted today.

Part III: US Interests and Potential Effects of International Control

The interests noted in the previous section matter to all countries, including the United States. But the US has additional national interests that are unique to the country due to its oversight authority of ICANN, which it is responsible for as a legacy of having initially funded and managed the network through its 35-year history. These interests include matters of national security, economy and political society, as well as national power (that is, US influence abroad), and national sovereignty (conducting unfettered domestic policy). This section first examines these interests as they pertain to the current state of Internet management. Then, it analyzes what the impact of diminished US control and a multi-stakeholder -- particularly multilateral, intergovernmental -- approach may mean for US interests.

The US Dept. of Commerce has the ultimate authority to approve or deny actions and decisions made by ICANN. [88] The way the current authority structure works, in regards to any substantive decisions, the ICANN board simply makes recommendations to the US Dept. of Commerce for authorization. Moreover, the Dept. of Commerce has informal "hot-line" control of ICANN activities; the ability to directly and immediately set the agenda or turn the attention of ICANN to matters, or demand reforms of ICANN [89] It has exercised this authority on rare occasions (notably an incident over root-server placement, discussed below).

This power is significant and unique to the United States. It is noteworthy that the US has never exercised its ability to formally disapprove any ICANN board decision. It has, however, used its ability to shape ICANN's decisions (such as when it used Congressional hearings to dissuade ICANN from establishing a $1 fee for each domain name registration, among other instances). Since almost any action the US would take regarding Internet infrastructure at the level of ICANN would have global ramifications, the US's "management role" (as it is called in the White Paper), [90] effectively represents a stewardship of the resource for the global Internet community. This has not required to the US to set aside its own interests for the sake of other stakeholders or nations because, at least for now, the interests of the US and the international community in regards to Internet infrastructure are neatly aligned.

1. US Interests Related to US Control

The United States government's authority over ICANN means that the country can act according to its sole interests without outside hindrance. Empirically, this has never been tested. And pragmatically, with good reason -- though the US could *in theory* make unilateral decisions, it might not amount to much: other networks, software and hardware developers and countries that comprise the Internet *in practice* could equally chose not to follow along. This is a crucial point, and one that this paper will return to in the conclusion. The autonomy that the Internet affords, by being a decentralized network, creates a balance-of-power among stakeholders (as discussed in Part I), and this appears on an international governmental level, not simply at the device or user level. The end-to-end, bottom-up design of the Internet architecture is mirrored in the institutional framework of its infrastructural coordination. It is a two-way street: it essentially restrains US power (and ICANN's authority), as well as limits the risk that the US would be constrained if Internet infrastructure decisions were to be adverse to US interests. (This is an unintended byproduct of the current institutional arrangement, not a premeditated feature.) Though US influence over Internet infrastructure would be diluted if ICANN is given autonomy, the central question is whether that would have any tangible impact on the US's ability to achieve its interests.

For the moment, US oversight of Internet infrastructure coordination has been exercised in a relatively benign form. It has meant that the US can make decisions faster and arguably more efficiently than if it had to act in a fully coordinated way with other stakeholders, particularly other governments, which tend to work at a slower pace than non-governmental entities. It has also served as a way to prevent ICANN and its subsidiary bodies from acting in a hostile or erratic manner, though it is important to stress that the US's mostly hands-off approach from ICANN's operations has also meant that the organization has been free to make poor decision based on dubious process and act incoherently, to which the US government even distances itself. [91]. It is relevant that when the registry of .com, VeriSign Inc., implemented a service in 2003 called SiteFinder that made subtle-but-serious changes to the routing of errant domain name traffic globally, the US government did not seem to intervene but let ICANN respond (though the US may have taken undisclosed actions privately). [92]

From an American perspective, the reasons for retaining power over Internet infrastructure coordination seems compelling: US government control can help ensure that the Internet operates smoothly. This may be on a technical level, that the infrastructure receives the proper maintenance and technically competent decisions. Or, on a political level, it can help ensure that Internet infrastructure does not fall under unfriendly legal regimes or be used as a pawn in state-to-state relations, [93] where the chance of a consensus on matters is far less than when one political entity has to decide policies that may be divisive, even on a domestic level.

On a proactive level, the US is able to assert its interests by legislating policies that effectively apply to all users of the network regardless of the jurisdiction where they reside. On a reactive level, the US can prevent actions that would otherwise happen, that would be against its interests. Mostly, however, the US has opted not to exercise any of its potential power at all. Rather, it has continued along the path set in motion in 1998 to share control of Internet infrastructure with other stakeholders globally, from government and the private sector -- the so-called "ICANN experiment." [94]

Of course, even if US power remains unexercised, the fact that it exists serves US interests, since it enables a form of policy suasion that no other country enjoys. The use of this management authority in regards to national security, power and sovereignty is considered below.

A. National Security, Economic & Socio-Political Interests

There are no vital national security interests related to the control and operation of Internet infrastructure, as it exists today. This immediately requires two qualifications. First, on a fundamental level, Internet infrastructure coordination does not pose any risk to US interests that threaten the safety and security of the country, its government and people, or way of life. Thus, there are no interests that can be considered vital, as the term is commonly understood. Second, this assessment refers to how Internet management exists today, not how it might function in the future -- a significant distinction.

Today, Internet coordination has within it the autonomy of its users, and the seeds of its own evolution or demise: any country is free to deviate from established standards, just as any user is free to develop new applications; and the institutional edifice of the domain name system is open to being succeeded in the course of technological progress. If this openness were jeopardized so that technical coordination policies became entrenched in place on an intergovernmental level, or if the current institutional model were to radically change in a way that was directly hostile to the US, it could constitute a deeper threat to US national security. Although possible, these situations are so improbable that it can be relegated an extremely remote factor in policy consideration. [95]

With these qualifications, this assessment should help place Internet infrastructure issues in a humble context -- it is a significant matter, but obviously far from the most pressing in international affairs today. To this, it is probably revealing that in the US government's landmark report "The National Strategy to Secure Cyberspace" in February 2003, the name ICANN did not appear once, and in the section where it mentioned the domain name system, the report did not recommend any action other than to encourage the use of IPv6. [96] ICANN is important to the US and the way its citizens, business, civil society institutions and government use the Internet -- but it's not vital.

Though US's oversight of Internet infrastructure management does not represent a vital national security interest, it is not unimportant, either. The "positive" or "active power that it begets is little, that is, the ability to proactively do something. On the other hand, the "negative" or "reactive" power -- the ability to prevent adverse policies -- is much greater, at least in terms of providing a degree of certainty and comfort. There are five main areas where the US government's authority over ICANN provides it with special national security interests, which are considered in this section:

i. reliability due to domains;
ii. stability due to the root servers;
iii. security and surveillance due to standards;
iv. US military interests in Internet infrastructure coordination;
v. predictability due to institutional design.

At the same time, key areas where the US accrues special advantages from its oversight authority are not just in security but economic and socio-political dimensions -- though, it must be added, the practical benefit of this control is far less than it theoretically seems. The section is further broken down considering:

vi. intellectual property and standards

vii. the economics of names and numbers

Importantly, while there are many limits of US power despite its control over ICANN, this can be considered as two sides of the same coin. It has a positive dimension: provided that Internet management happens in a similar way after ICANN is independent as it does today, this inherent limitation of power will prevent any harm of US interests if actions are taken that are unfriendly to the US. (It is raised here, but developed in the final section.)

i. Reliability and Domains

The US government's oversight of ICANN gives it special interests related to national security. First, it ensures the stability and reliability of the infrastructure of its national domains. This, importantly, does not merely include its two-letter country-code domain (.us). It also includes its three-letter generic top-level domains, such as restricted domains .gov, .mil and .edu, which are closed to general registration except for qualified entities, as well as open domains like .com, .net and .org, which accept registrations from anyone able to pay. These final three domains, though open for registrations from around the world -- and count many non-US registrants -- can nevertheless be considered de facto US domains. The high proportion of US registrants, in addition to their status as being the original and most influential domains (created by US government contractors, as well), gives the US special interest over them. These so-called "legacy domains" are under the responsibility of ICANN, not the US -- in the same way that the generic domains ICANN established in 2000, like .info, .biz, are under ICANN's remit. This lack of direct authority over .com, .net and .org is one reason why the US imposes national law on them (as discussed more fully, below).

It also marks an area where US oversight of ICANN accrues specific benefit to the US. In this instance, it ensures that operational control of the registries do not get reassigned to a foreign entity where it would no longer be under US jurisdiction, or that decisions adverse to US citizens and consumers take place (such as the US Congress's ability to stop the $1 fee on generic domain name registrations in 1999). There is historical precedent to treat the three open, generic domains as a special US asset. In 1998, when the pricing mechanism for domain registrations was declared illegal due to a $15 surcharge imposed by the US National Science Foundation (for a so-called "Intellectual Infrastructure Fund") was ruled an illegal tax, Congress authorized its ex post facto collection in a supplemental appropriations bill and allocated the monies, then $56 million, to the NSF, even though roughly 30% of it was collected from non-US registrants.

As for the US's control of its country-code domain .us, the country's authority over ICANN serves its interests in this area, as well. For instance, when the US underwent a legislative process to reassign .us in 2000, the issue was placed on a fast-track and addressed outside customary ICANN procedures, due to country's ability to make direct demands on ICANN. It is notable that the US didn't actually need authority over ICANN for it to attain the same result -- however, critically, the process would not have gone as fast, and the outcome would not have been as completely certain. This is because other countries have not been formally granted sovereignty over their country-code domains; as discussed in the previous section, the matter remains inconclusive. It may be fair to say that the US does not have actual sovereignty over its country-code domain either -- but that does not matter so much since it obtains the same degree of autonomy by dint of its authority over ICANN.

ii. Stability and the Root Servers

On another level, the US's authority over ICANN provides it special national security interests in terms of the stability and security of the infrastructure, through the root server system. US control means it can more directly ensure that the contents of the root are predictable and reliable. Moreover, US control means that it can ascertain that the security of the domain name system is protected at home and worldwide. For instance, authority over ICANN enabled the US, after 9/11, to directly insist that the organization make security issues a more urgent priority. At the ICANN board meeting in November 2001 in Marina del Rey, the entire ICANN agenda was suspended and replaced by security issues. The US uses this power in a number of ways: it is able to communicate directly with ICANN; it was instrumental in pushing ICANN to quickly establish a standing "Security and Stability Advisory Committee" [97] which includes a number of members who hold US security clearances; and it is able to enforce changes on root server administrators (who are organized in the "DNS Root Server System Advisory Committee") by subtly threatening to take away their operational responsibilities, using such expressions as wanting to place it on more "professional management." [98]

Furthermore, the US has disproportionate influence over the root server system because, in addition to controlling the A root server, the country controls the majority of 12 secondary servers both directly and indirectly. Though there are now many mirror servers deployed outside the US, the content is replica of the secondary servers, so accrues no balance-of-power interest. (For more on this, and its implications, see "Appendix D: Control of the Root Servers and Policy Evolution".) The US's authority in this area has been used: in 2002, the US bypassed normal ICANN procedures to see that a root server's location was changed for security reasons, a potent example of how US control provides it with special interests it wouldn't have in a different institutional arrangement. [99]

iii. Security and Surveillance with Standards

On another dimension, US control of ICANN provides it with unique power to shape -- at least try to shape -- security as well as surveillance techniques for law enforcement access to communications. This taken place since the very beginning of the Internet. For instance, the co-author of the Internet Protocol specification and current ICANN chairman, Vint Cerf, was asked to build more robust security into the protocol by the US National Security Agency in 1975, at the very start of the network, which he did. [100] Cerf, as with most of the original Internet pioneers, were contractors with the Dept. of Defense which funded initial work, so it is not surprising that these informal contacts would yield fruit -- particularly because, in this instance, it was to build a stronger protocol, not a weaker one (i.e. with backdoors).

The days when the US could wield its influence successfully may be over. The creation of Internet standards are performed by the IETF, which comprise engineers who are notoriously independent-minded. [101] In three instances, where the US sought to influence the development of technologies and standards for its public policy goals, it was rebuffed. In the mid 1980s, the cryptographic scientists at many software vendors were contacted by the NSA and asked to build back-doors for intelligence access into their products; nearly all did not comply, though some did, such as by weakening the strength of their cryptographic products sold overseas. [102] In 1999, the US tried to persuade the IETF to build wiretap capabilities into the protocol of the Internet. It became a public controversy, and the IETF's governing bodies issued a statement saying that though an understandable public goal, it recommended not doing so because providing that feature made the protocol less secure for all users. [103] In a third instance, after 9/11, the US Defense Dept. Advanced Research Project Agency (DARPA) funded an early-stage discussion by Internet security experts on the idea for a way to upgrade the Internet protocol so that each packed would be identified with a specific user. One participant at the meeting said that with the exception of a few government officials and one former official at the meeting, the idea was roundly ridiculed as both unworkable and against basic freedom. [104]

iv. US Military Interests in Internet Infrastructure Coordination

This raises an important adjacent question concerning the US military as a user of the Internet, and what a diminished US control over ICANN would mean for national security in this context. A full assessment of this question would require a complete picture of the US military's Internet use, which is classified. Yet there are indications that it would not matter very much, provided that the system operated much as it does today.

In terms of names, the US continues to use the .mil address for publicly reachable sites and users, which relies on dependable name resolution from the root, as any other domain does. As for the .arpa domain, it is used for infrastructural operations like "reverse look-ups," and more recently, as the operational domain for the ENUM protocol that melds the domain name system with the traditional telephone numbering plan. (This has been the subject of controversy internationally, who point to the name to argue that the US military still runs the Internet.) [105] As regards the root, the US military either does or could use name servers on its internal network, so any instability in the root would not jeopardize higher-priority military communications, particularly battlefield-related. Moreover, the US military directly controls three of the 12 secondary root servers; provided a future institutional framework is established that enables the US military to retain control of one or more machines, the independent management of Internet infrastructure would not pose a problem in this regard.

The US military today has control of enormous blocks of IPv4 address space: of 255 so-called "Class A" address blocks that exist, the military currently has 12 blocks. [106]

Though useful, it is migrating to IPv6 address space by the end of 2008. [107] Provided that it is able to obtain suitable access to the number blocks, this should not pose a problem; there is even good argument for the military to deploy its own numbering system for internal communications, which is off of the public Internet without the need for secure public gateways.

In terms of standards, DARPA has sought to influence protocol development, as mentioned above, as well as through its technology grants. It has in some instance sought to bring more accountability to Internet traffic by making it more "deterministic." [108] Though whether it will be able to influence IETF standards is unsure; importantly, the military can always deploy its own specification -- like any user, it never needs IETF standardization, unless it wants the application to be universally interoperable. At the same time, the domain name system may fade in importance for the US military; one DARPA official believes that ad hoc mesh networks relying on peer-to-peer principles are more efficient than end-to-end topologies. [109]

This all points to the idea that a decrease in US control of Internet infrastructure might not harm US interests in terms of the military. During the debate over the creation of ICANN in the US government, there was never an assessment by an intelligence agency over what this transition of power meant for the military or US national interests, according to a ranking Congressmen close to the matter [110] Though this may be due to omission, it could also be because it was judged not sufficiently important to warrant such. It may be a fitting testament to how far the Internet has gone, that the network originally created for the Defense Dept.'s use no longer has much impact when it flies away from its nest; the father is child of the man.

v. Predictability in Institutional Design

The US has a unique interest in the current institutional structure because, obviously, it provides a degree of certainty and predictability by dint of US control. Though the Internet means a lot to all countries, it may mean more to the US itself. The US has one of the highest levels of Internet penetration for a country of its geographic size and population. The largest companies that depend on the Internet are based in the US or its is their largest market -- companies that supply services through the Internet (like retail e-commerce); technology products that relate to using the Internet (such as computer hardware, software and integration services); backbone network providers; and companies that are incorporating Internet technologies into their business operations. A greater proportion of research and development investment is made by US companies or foreign countries operating in the US. More business and individuals have incorporated networking technologies into their activities, because of the US's early lead. Moreover, US entities have registered more domain names and have been allocated more IP numbers than any other. [111] Four of every five IETF meetings are held in the US; slightly over 50% of attendees at all meetings are from the United States. [112]

All stakeholders depend on the stability of the infrastructure, its predictable coordination and its responsible evolution, which is what Internet management provides. But because the consequences of possible failure are greater for US firms and people than from elsewhere, the US has a special interest in maintaining the existing system, however imperfect, because there is less uncertainty. There is a fundamentally conservative pressure on the US, even if not openly articulated, to resist change to the Internet's institutional design. It is only natural, in terms of risk avoidance. Of course, the current trends will not remain -- the percentage of Internet users is already greater outside the US than in it; China and India invest heavily in the Internet to develop technology centers and so their companies can be competitive globally -- but the current factors help explain a US hesitation before relinquishing its oversight authority.

Much of the reforms that the US government requested of ICANN though the MOU process involved assuring the constancy of ICANN's institutional design. [113] In fact, in the heat of debate over whether the creation of the United Nation's Working Group on Internet Governance would indirectly usurp ICANN's authority, during summer 2004, ICANN took pains to issue a statement that it had accomplished seven of the Dept. of Commerce's requested reforms -- all dealing with institutional structure. [114] One can treat the history of ICANN as a long attempt to get its institutional structure right: from the dispute over open board meetings in the first year; to "board squatters" who remained after their initial term expired in year two; to the ganglion of studies and reports on membership issues in year three; to major reform process initiated by ICANN President Stuart Lynn throughout year four; to the Dept. of Commerce's major reporting requirements during year five; to the structure of ICANN compared to the UN, where we are today.

ICANN and the US perceive a threat from the UN's World Summit on the Information Society (which established the Working Group on Internet Governance), because it seems to call into question the underlying principle behind ICANN's creation: its model of bottom-up, private-sector-led self-regulation, as opposed to more formal governmental regulation, which unsurprisingly, some UN member states call for. [115] This is the biggest threat that ICANN and the US faces, for if the institutional design should change radically, it would undermine all other aspects of Internet coordination. One could devise many worst-case scenarios; the more threatening they sound, the more unlikely it is that they would actually occur. Nevertheless, the very unpredictability makes it a legitimate worry. The uncertainty is all the greater because other countries seem to be changing their positions, and the idea of Internet coordination happening as a public-private sector partnership, with an emphasis on the private sector, is being called into serious doubt. This is not only happening by the developing world [116] but, surprisingly, also by developed countries, like Norway and Japan. [117]

If the institutional framework were to shift, and the influence of the US were to be severely and irreparably impaired by a power (be it commercial or political) that sought to enforce decisions adverse to the US interests, it would create major problems and threaten the global interoperability on which the US, as others, depend. (More on this is treated below.) It is notable that the UN's WGIG process can serve a useful function as a means to force countries to establish formal national positions on these issues, and provide an occasion for the US to make its case for private sector-led management, and the limits of intergovernmental control. Only with an international consensus for Internet management can the US attain the predictability it needs that the institutional structure won't change radically after a transition takes place.

vi. intellectual property and standards

US oversight of infrastructure coordination could provide it a means to influence what standards are adopted -- in practice, however, it does not. A concern is if Internet coordination were to move into a more multilateral footing, that governments would use the standards process to give its companies advantage; it could start a sort of standards arms race that would threaten the interoperability of the Internet. This, counter-intuitively, is at bigger risk of being set-off by the United States (due to pressure from narrow interests in domestic politics) than by other countries, with the exception of upcoming large technology-intensive countries. [118] In such a case, the US's authority over Internet infrastructure can be said to potentially set back America's broader interests, if the question of standards became politicized within the country, and the US proposed specifications that other countries rejected. [119]

At the moment, there is little risk of the IETF becoming the shill for one country's or company's standards. The protocol TCP/IP, like almost all Internet standards, are free of any intellectual property restrictions -- they are open standards: open to freely use, and open to freely build upon and redevelop. [120] In rare (though increasingly occurring) cases where there is intellectual property attached to a specification, it is disclosed prior to standardization and is usually "unencumbered," that is, made available for license on transparent, non-discriminatory, and easy-going financial terms. The history of Internet standards is replete with examples of technologies being rejected due to intellectual property claims; for instance, in 1998 with the Netscape's secure online transaction technology that relied on the RSA cryptographic algorithm that was patented in the US (but not patented elsewhere). Another public dispute took place in the summer and fall of 2004 with Microsoft's technology to reduce spam, called "Sender-ID," which was rejected by the IETF due to its proprietary nature. [121] The IETF has established formal guidelines on how it handles intellectual property issues. [122]

These trends suggest that standards development belongs to no one but the techies, so that it can belong to everyone. It seems like a sweet nirvana, and like all such stories, there is usually a sour reality it doesn't take into account. In this instance, the concern is two-fold. First, what if the standards process where to change and become politicized (for instance, there is already work on a sort of "successor" to the Internet at the ITU referred to as the "Next Generation Network" that has a lot of input from governments not just techies). Governments have used standards for their advantage; in the case of the Internet, there was a real risk in the mid 1990s that the European Union would deviate from established Internet routing protocols as a way to remain independent of Cisco, which dominated the market for routers, and give a boost to European companies. [123] Second, and contrarywise, the IETF's independence from governments might be problematic since standards embed values, and the public interest as they are expressed by governments might be appropriate.

The US has a special interest in the current system of Internet coordination because, for the moment, it embodies American principles of market competition. Though antitrust suits against technology firms are not unheard of in the United States, Internet standards have largely been founded on interoperability, not commercial advantage. Engineers are told to attend IETF meetings representing the interests of the Internet community, not their companies. [124]

Though there is a certain degree of unilateral benefit to the US from this, since US industry has a lead in developing many technologies, it also leads to an open market for competitors who can catch up and surpass existing companies (for instance, France's Alcatel is a world leader for fixed-line broadband technology, called DSL). Moreover, whereas the Intenret protocols serve as an open platform, it enables a raft of opportunities for competition among technologies that ride atop basic access. Consider: the Web was created by an Englishman living in Geneva; instant messaging was pioneered by an Israeli firm; and WiFi was devised in a research lab in Zurich. All three of these technologies utilized the openness of Internet protocols to emerge.

The US receives special advantages, on an preventative level, due to its dominance in standards development (due to its high number of engineers and the culture they have established). However, these benefits are not due to the broader issue of Internet management per se, that is, authority over ICANN. Rather, the US oversight could act as a preventative stop in case standards-setting became politicized in a way that was adverse to US interests, or if it threatened the interoperability of the Internet or required costly licensing of intellectual property, which would be averse to all interests. Furthermore, the US can act to ensure that Internet protocols maintain the Internet's fundamental openness, which is both an economic and socio-political interest.

vii. the economics of names and numbers

The US, because of its oversight role in Internet coordination, has a unique interest in how the economics of domain names and IP numbers evolve -- and on first blush, has less to gain and more to lose from a change in the status quo (though this paper will argue in the next section that this is an oversimplification, and unless the US remedies the tension brought about by the inequality of influence over the Internet coordination, the US will set back its own broader interests).

Due to its role as the first country online because it invented the Internet, the US has special control over certain names and numbers. As alluded to earlier, the US has a dominant position in IP address number space in the current version of Internet Protocol, version 4. American entities controls roughly 85 percent of the allocated "Class A" IP address blocks. However, the dominance is even more pronounced: only about 35% of the available blocks are allocated, the rest are reserved by ICANN's quasi-separate division, IANA [125] (essentially, controlled by the US government through contractual agreement). It must be immediately noted that the benefit of the IPv4 number blocks becomes much less meaningful over time as the world migrates to successor technology, called IPv6. Additionally, the US controls its own closed generic domains (.gov, .mil, .arpa, and to a lesser extent, .edu), though not its open ones (.com, .net and .org).

A change in the nature of Internet coordination could create problems if it were to disturb the current way that names and numbers are accounted for as a resource. In the area of domain names, any funding mechanism that imposes extra cost on the use of domain names, akin to a tax, would disproportionately hurt American users more than users elsewhere; the increase cost would likely decrease demand for names, which would harm the economic interests of the companies that register them, again, predominantly American. This is not to say that funding ICANN through domain name registrations isn't viable; it is. Rather, it is to say that the current structure to a certain extent already takes into account the delicate business factors involved. This could be altered when the institutional model changes. Bad-case scenarios would include actions that artificially disturb the economics of names for policy objectives rather than technical ones. For example, one can imagine adding a surcharge on all generic domain name registrations to finance a program to address the digital divide, akin to a universal service tax. Though a worthy goal, there may be less a intrusive way to achieve it than to bolt economic development issues and Internet infrastructure management together. In this case, the cost of encouraging the use of technology in developing nations comes at the expense of inexpensive access in developed ones; were it a policy goal, it would likely make more sense for it to be financed through aide programs, not infrastructure administration.

Another example where a change in Internet coordination could harm US economic interests is if a non-US company won the rights to operate the legacy .com, .net or .org registry. This would mean less revenues for US firms who operates these registries (and could jeopardize the free-expression values that they embody, permitting religious tolerance, political dissent and consumer satisfaction (though the final element is already under threat from the UDRP and US trademark rulings). Moreover, one could imagine policies that encourage the delegation of new top-level domains outside the US, and particularly non-Western countries; while this would harm US interests in a shallow sense, it should be added that this is already ICANN policy and also helps American broader interests in global economic development. This would certainly be controversial in the case of extremely valuable new domains (such as .xxx, .web, .law, .tel, etc.) granted to non-US registries. Mitigating this, of course, is the fact that such semantically good domains may not be in English though still in ASCII, or in foreign scripts as top-level internationalized domains.

The economics of domain names also has a socio-political dimension, not just a commercial one: the low cost of registering a name serves the social goal of encouraging online participation, free expression, media diversity and community-building. The US's generic domains are the least expensive open domain name registration costs in the world, due to the private-sector nature of the system and competition. [126] This low cost (and unregulated access) allows for its broad use. If the economics were to change due to different Internet management, it could set back US interests in his regard. Likewise, if policies were put into place that used domain names to restrict content -- which is the classic bugaboo of placing Internet management on a multilateral footing, where the notion of national sovereignty is usually invoked as a diplomatic codeword for censorship. This is a potential outcome, including by Western countries normally closer to the US position on free expression. [127]

The bad-case scenario for IP numbers is that their distribution will be based on other criteria than network topology, such as global population. This, predictably, has been suggested by developing nations and populous ones, who do not have the network infrastructure to justify receiving IP number allocations, so use their ability to have equal standing in international forums as a basis to request equal distribution of numbering resources on social justice grounds that it is merited. [128] (The issue basing Internet resource access on geopolitical rather than technical grounds is also hinted at by the infographic in the 2003 report on ICANN for European Commission, in Appendix A.) International media resources have often played this role as a political football by states in intergovernmental forums, to be arbitraged for financial gain. For instance, the Pacific Ocean island-republic of Tuvalu, which leases its semantically lucky two-letter country-code .tv to a US registration company, is considering renting out its share of satellite orbital slots it was allocated by the ITU. [129] It would be following the lead of Tonga 20 years earlier, which controversially exploited the lax ITU rules to resell its slots. [130] There is a real possibility that the same sort of politicization may occur with Internet resources, manipulated for national economic gain by developing countries, but with increased costs to genuine users of the resources -- and that this is more likely in a multinational, intergovernmental setting than under the current framework of Internet management. [131] The United States -- equally dependent on IP numbers as a resource as other nations but with more at stake due to its current position of abundance -- has an important economic interest in ensuring that any new institutional framework does not seek to revise the current IP number allocation policies. It is relevant to note that while some countries are arguing that IP numbers be allocated using different rules than the current procedures based on justified technical need, the US is not countering these proposals by arguing that IPv6 allocations should match the current distribution of IPv4 allocations in which it has so much -- underlining the different degrees of good-faith motives among the parties involved.

This section has been long. It has traced the ways that US has intrinsic national interests in Internet coordination beyond those common to all countries, because of its current role regarding Internet management, and its history. These interests impact national security as well as the economy and political society. The benefits the US accrues due to its influence over ICANN would be jeopardized if the assumptions underlying the current system of Internet management were to shift due to shared control. We now turn to how this would effect US power abroad and sovereignty at home.

B. National Power (Influence Abroad)

Power is the ability to impose one's will on another, regardless of the propriety of that action. Forcing others to do something they wouldn't ordinarily do on their own can be both good or bad, depending on the specific circumstances and outcome. Indeed, much of the international order after World War II has been about using multilateral institutions to compel states to achieve their broader long term interests rather than lean towards satisfying their more short term ones, upon which most domestic politics are based. The very basis of the United Nations system is that states must work together to ensure global peace and stability. It is an underlying principle of all multi-lateral, intergovernmental organizations, with different degrees of power and enforcement.

The World Trade Organization, for instance, can enforce the level playing field among states with regard to trade. Without a certain degree of international force, states are victims to their short term interests -- for instance, designing the rules of national trade around one small politically-active interests, that might undermine wider interests that are less politically active. The European Union, for example, entails the loss of some sovereignty by its members, but in return they gain a harmonized and stable continent-wide economic and political system. On an institutional level in terms of the global economy, international institutions that bind countries to cooperate have what has been called "sticky power" -- something situated between the "hard power" of military muscle and the "soft power "of influential ideas, from popular culture to public diplomacy to the Internet. [132]

ICANN serves as a sort of "sticky power," too. It effectively binds stakeholders to cooperate (in this case, in agreeing to use Internet standards and a common root for the domain name system), even though any entity is free to deviate at any time. ICANN keeps nations in to a single coordinated system for Internet infrastructure: the benefits of standardization due to network effects outweigh the advantages for countries to exercise their sovereignty and devise their own system for data-communications traffic exchange. This helps explain why although some countries wish to better control the Internet within their borders through the notion of a nation-wide intranet, that hasn't happened; nor, why countries keen to denounce US control are not prepared to renounce their country-code domain or IP numbers and establish their own naming and numbering plan.

ICANN is an expression of US power abroad, and furthers American interests. It is able to export American socio-political principles (such as free expression and bottom-up self-governance); economic approach (private-sector-led, market-based approaches); legal institutional mechanisms (transparency, accountability and due process); and cultural values. Importantly, this is a secondary effect of ICANN's actions; it is not because of any pre-designed goal on the part of the US government or ICANN. From the perspective of ICANN, it simply is trying to coordinate Internet infrastructure on a private-sector basis, uniting fractious parties with divergent interests, and governments that endow ICANN with powers more imaginary than real. (It helps matters little that ICANN itself made a startling large number of truly terrible errors of substance, process and principle.) From the perspective of the US government, it is devolving its authority over Internet coordination but seeks to do so in a responsible manner to ensure the stability of the infrastructure. For both ICANN and the US government, forefront in the minds of the men and women in charge are not larger geopolitical consequences of American control, but small day-to-day operational issues.

This is testified by the weight accorded to it within the power-structures where they reside. ICANN's Governmental Advisory Committee is comprised of low-level officials from the standing bureaucracy; the ICANN board are unknown outside of technology circles with the exception of Dr. Cerf, and policy in the US is managed from a small division of the Commerce Dept., not the higher-profile State Dept., or the White House. This all points to the importance of ICANN as a means to promote American power is not due to intention or as an explicit goal, but is an unavoidable effect of the otherwise low-level operation that the ICANN project, viewed narrowly, entails.

As ICANN enables the US to influence affairs globally, it should be noted the ways in which this has a beneficial effect on the spread of the Internet internationally, which in turn, helps other countries for economic development, political culture, civil-society institution-building, and in some cases, human rights. The United States' private-sector approach to Internet coordination -- specifically, country-code domain administration, Internet service provision and non-proprietary protocols standards -- is responsible for low-cost access, which increases the ability of users to participate in the medium. It also led to a faster deployment of Internet infrastructure resources. Additionally, it has traditionally placed technical matters before political ones, which freed the medium from being encumbered in bureaucratic wrangling. Often, the Internet's private-sector footing is one way the medium can still make inroads into these countries, despite the obstacles that their governments place in its way.

It is noteworthy that many of the governments most vocal against the current system of Internet management are unable to articulate how it has jeopardized the development of the Internet, other than basing their argument as an appeal on symbolic grounds. This list includes China, Brazil, India, South Africa, Zimbabwe, Syria, Vietnam and Cuba. Moreover, many of these same countries are also the ones that impose the greatest restrictions on Internet use, by banning content, blocking Internet telephony or refusing to open up competition in their national telecom markets. This should rightfully give pause to officials involved in Internet policy matters -- not just from the US but from around the world -- about what this may portend once control of Internet coordination is shared rather than under US oversight. It also helps justify US cautiousness before it grants ICANN autonomy.

To put a point on it, at the UN's WSIS summit in Geneva in December 2003, Zimbabwe's president Robert Mugabe criticized what he described as a conspiracy by the West to use the Internet as a form of neo-colonialism, and specifically called for respecting "a sovereign national government that manages 'top-level domains' within its borders" [133] -- he, responsible for violent civil unrest, media restrictions, mismanaging the economy and accused of assassinations of political opponents. Indeed, US control over Internet infrastructure has arguably done more to encourage the spread and use of the Internet around the would than would have happened if national governments had been given political control initially.

For the US, ceding control of Internet infrastructure impacts the degree to which it can influence issues related to the domain name system internationally, as well as how it could use Internet coordination to achieve foreign policy goals, either discreetly or overtly. One can imagine many ways this could happen: for example, creating a domain that offered free registration for anyone in the world -- it would fit into the tradition of Radio Free Europe, but give people (by analogy) the means to be the broadcaster, not just the receiver. What is relevant is that while there are many ways in which control of ICANN could aid US policy objectives, the government has chosen not to use it. The effects of US control of Internet coordination in terms of US power abroad is due to subtle, implicit consequences of technical management, not explicit initiatives to serve discrete foreign policy aims.

In terms of socio-political principles, US control of Internet infrastructure enables it to export its values abroad. The openness of the architecture leads to low cost and easy access to naming resources, which encourages free expression. Internet use promotes transparency and accountability, which are the bedrocks of a democratic culture. The lack of regulations on use means that anonymous speech remains possible. The decentralization and unregulated nature enables the Internet to act as a platform for subsequent technical innovation -- and this can be exploited by all countries. (One example is the file-sharing software company KaZaa, which is accused of abetting online music piracy; the Estonian firm applied the same technical approach to phone calls and created the company Skype, which offers near-free phone calling.) This sort of innovation that can disrupt multibillion-dollar industries is due to the values inherent in the network, which is concomitant with US control.

Another way in which the current arrangement enables US values to be imposed a broad is in the policies of names and numbers. Consider the case of adding new domains. An informal recommendation by an official at the Organization for Economic Cooperation and Development in 1997 (prior to ICANN) for governments to consider creating the domain .sex as a way to establish a “red-light” district in cyberspace to protect minors from adult content was swiftly rejected by US officials present; their knee-jerk reaction was that it would set off a diplomatic fracas from countries with cultures where sexual matters were treated more intimately. The differences of what it permissible between Sweden and Saudi Arabia would make a single global standard impossible. [134]

In addition to values, US control enables America to impose its legal mechanisms abroad. Complains over generic domain name issues, if they make it to court, go to US courts. This gives American companies a slight advantage in that they can seek local representation. Yet it is also in some instances good for other countries, since US law, despite its many flaws, marks a better judicial mechanism than exists many of the world’s other jurisdictions, notably in developing countries (though the corollary is that a reliance on the American judicial system might disfavor non-US parties, particularly from developing countries, on economic grounds among others). [135] Furthermore, re-delegation procedures require other countries to follow transparent processes of documenting claims, which detracts some countries from changing domain registrars anytime the government changes. This, it should be noted, was an intentional reason why Postel and others sought to encourage the private-sector model of Internet coordination (and the dual-responsibility to the “global” Internet community, not just the local one, which gave Postel and others the standing to weigh requests on re-delegations). It was a means to prevent the infrastructure from being threatened by civil political disputes, and possibly for economic gain.

In terms of cultural approach, US influence over Internet coordination is a means to promote the American cultural values of bottom-up self-governance, which is a foundation of the democratic ethos. Often, this is done via the private sector, which is decentralized relative to many developing country's political culture, which is centralized on major cities and government bureaucracy. In many countries, even ones where monopoly state-run telecom operator are present, Internet access is furnished through a private-sector model: independently-owned cyber cafes. Its use for communications develops communities and is quickly embraced by institutions of civil society. (It is with this in mind that one of the first things the US government did in the reconstruction of Iraq was establish Internet access infrastructure.) The private-sector model of Internet coordination is a means to encourage this goal of bottom-up self-governance that relies on other stakeholders than the state.

On a final note, this approach must be understood more broadly, in the context of the American democratic experience. The political culture of the United States was shaped by its overthrow of centralized authority in favor of a form of democratic self-governance that was highly decentralized, providing most powers to the states, not federal government. (This was the Articles of Confederation, whose very name embodies the values that underlied it; this shifted, of course, with the Constitution, yet the central debates in American politics to this day is one of federalism. Even the controversy in 2003 over media diversity is an echo of this, as a dispute over national versus local news.) The self-governing ethos is fundamental to America; de Tocqueville believed the new nation's hallmark was its open participatory civic-engagement and associations. Later, when settlers expanded across the continent, before they set out they elected a police chief among their ranks to keep order and punish crime. [136] To this day, sheriffs are locally elected. The Internet is a natural extension for this bottom-up, private-sector-based, self-governing approach.

Yet it is a uniquely American phenomenon, and cannot be so readily universalized -- though this is the implicit consequences of the ICANN model. Though it is viewed as a foreign policy interest, like democracy and freedom, holding universal appeal, it is in fact particular to the American political culture. Other countries come from vastly different political traditions and are content with them. France has had a predominantly centralized control in most areas of society, government and the economy since before the days of Louis XIV; one 19th century education minister boasted he could look at his pocket watch and know what every French schoolchild was learning at that precise moment. A policy that disintermediates the state and its ethos for centralized coordination, as ICANN to some extent does, is a direct affront to national authority. Moreover, China's history has been one of avoiding the perils of anarchy and disorder, and achieving peace and stability in times of order. [137] Its history is punctuated by eras with names like "Period of Warring States." Decentralization has never been a good thing; in such a vast land, it has usually meant a breakdown of order, and ushered in great strife, famine, war and poverty. In such context, the notion of harnessing the forces of chaos and anarchy, which is the commercial ideology of Silicon Valley smacks as not only inappropriate but dangerous.

ICANN holds in creative tension these forces: decentralization (multi-stakeholder interests through supporting organizations) and centralization (a single, inviolable root). However, it is the progenitor of a bottom-up approach that flies against the political culture and national experience of other peoples and countries that participate in the system of Internet coordination. This is a critical source of inherent conflict within the ICANN structure that has never been explicitly recognized (and is difficult to see because is so subtle). Yet as Internet coordination becomes more internationalized, unless addressed, this aspect with grow more discordant and be an invisible underpinning of many disputes.

C. National Sovereignty (Domestic Autonomy)

National sovereignty is the ability for a government to control all that happens within its boarders without interference, be it domestic or foreign. The Internet has long been named the culprit for weakening national sovereignty of all countries. [138] Indeed, many nations see in ICANN the power over infrastructure that they, governments, ought to have but do not. In terms of the United States, on a purely formal policy basis, the US is able to translate authority over ICANN into unilateral, direct control over the Internet's names, numbers, root servers and standards. This control, in turn, would allow the US an immediate and unfettered way to promote American domestic and foreign policy interests through the infrastructure. However, this has not happened. For the most part, this is because the US has not tried to manipulate Internet infrastructure in this way. In other cases, it isn't for lack of trying.

Examples of how the US could potentially use its control include adding new domains to the root and delegating their operation to US registries; establishing three-letter country-code domains and auctioning them to private companies to operate; allocating blocks of IP address space to US companies (or simply setting policies over IP numbers that inherently favor allocation requests from US firms); mandating features in Internet protocols that meet American interests, be it in terms of traceability of communications, intellectual property protection, or propriety standards owned by US firms. Moreover, the US could rescind the non-proprietary nature of the Internet Protocol itself and demand that all non-US users pay licensing fees to use any element of Internet technology that relies on those standards, such as the domain name system.

This list, of course, is preposterous. While the US could theoretically try any of these things, its chance of success is low, and the probability of success distant. The US wouldn't be even prone to try to manipulate the system to its advantage. To cite just a few reasons: the creation of new domains isn't such a cash-cow and fostering a government-backed industrial policy isn't considered the most appropriate use of state power; US firms don't have too much difficulty acquiring IP address space under the current rules if they can justify need; the US would like to modify Internet standards for security reasons, but this would still require the adoption of those standards by implementers around the world for it to take hold, which is uncertain to happen; etc.

Yet the US, in a number of instances, did try to translate its oversight authority into policy action, and was unsuccessful. Noted already, for example, is in the issue of wiretap capability written into IETF standards in 1999, which was rebuffed. Instead, the US police and spy agencies perform surveillance by directing their efforts at other points of eavesdropping than within the basic protocol itself. Though it would undoubtedly have been easier to enable this in the technology, it wasn't indispensable, and law enforcement simply devised ways to accomplish the same goal through other means. Likewise, tracing traffic to its source; though DARPA was unable to impose its vision of "eDNA" to identify each packet with its sender (as discussed above), this does not mean that traffic is untraceable -- it just takes much more effort and is much more costly. That three of the most notorious virus writers in the past few years have been captured -- the "Melissa" virus to man in New Jersey, "ILOVEYOU" to a youth in the Philippines, and a variant of "My Doom" to a hacker in Germany -- not to mention the proliferation of lawsuits by large US companies against oft-considered untraceable spammers, shows that although identifying Internet traffic to a specific individual or machine is difficult, it is not impossible. When the pictures of the American journalist Daniel Pearl held in captivity in Pakistan in 2002 was sent to media from the email "kidnapperguy@hotmail.com," the FBI was able to swiftly locate the machine it was sent from, starting the process of apprehending the journalist's murders. [139]

In other instances, the US sought to use its authority over ICANN to meet national interests, only to find it could more easily achieve a comparable result through national law rather than by modifying the global infrastructure. Consider three examples:

* *Prevention of Cybersquatting* -- In 1998 the US charged WIPO with devising a global policy to prevent speculators from ransoming domain names associated with trademarks in .com, .net and .org. Impatient with WIPO's pace and an uncertain outcome, the country enacted legislation to address this on a national level. The "AntiCybersquatting Consumer Protection Act" was signed into law on November 29, 1999.

* *Creating a child-safe online zone* -- US policy makers wanted to establish an area on the Internet that was guaranteed to have content safe for children. It debated creating a .kids top-level domain for this purpose. However, it was unable to dictate this due to having to respect ICANN's process on adding new domains which the US government itself set up. The process was cumbersome, and the private company that submitted an application to manage the domain wasn't successful in obtaining it. Subsequently, Congress created the same area under its two-letter county-code domain, .us. The "Dot Kids Implementation and Efficiency Act" was signed into law on December 4, 2002.

* *Prohibiting mislabeled adult content* -- US policy makers, frustrated at the propensity of misleading domain names that dupe users into visiting innocuous-seeming sites that in fact has adult content (such as, in the 1990s, bambi.com, and as recently as 2003,

whitehouse.com, as opposed to the executive branch's .gov), officials did not try to use ICANN to set a policy to protect minors from bait-and-switch domains that housed adult content. Congress achieved the same goal in domestic legislation. The "Truth in Domain Names Act" was signed into law on April 30, 2003.

In other areas, the US has applied pressure on ICANN to assure the validity of WHOIS data of name registrants in generic domains, which ICANN does through its contractual agreements with accredited registrars. However, despite this, the data is rife with erroneous information and there is lax enforcement. [140]. As a result, the US Congress in 2004 considered legislation, called the "Fraudulent Online Identity Sanctions Act" that would mandate this information me accurate and impose penalties if it were not. The legislation is controversial since while it promotes the US interest in accountability of content and traffic, particularly for reason of preventing intellectual property piracy, it at the same time jeopardizes American interests in promoting anonymous speech and free expression domestically and globally.

The US also has found ways exert sovereignty over the domain name system without exercising its control of ICANN but instead through basic national law enforcement powers. In cases where Internet sites are suspected of being a locus of criminal activity, the Federal Bureau of Investigation has seized the domain names. [141] As in the previous examples, this shows how the US is able to assert its interests through domestic law and ICANN processes, rather than rely on its authority over the Internet coordination policy at the global level.

Much of US sovereignty related to ICANN is a preventive power to block action rather than an affirmative power to impose actions, as has been noted above (with the exception controlling the agenda, such as the case of security after 9./11 or root server relocation). For instance, in 1999 when ICANN proposed a $1 annual charge for every open generic top-level domain name sold (.com, .net and .org), to be paid by the domain name registries from their customers, the US Congress held hearings in which politicians criticized the proposal, which was quickly dropped. [142]

Moreover, as law enforcement penalties move directly into code-based punishment rather than offline-to-online processes, as is predicted, [143] such so-called "Lex Informatica" approaches may rely on interfacing with Internet infrastructure such as domain names or IP numbers. Here, the US has an interest in preserving its sovereignty from the possible misuse of that power by retaining its control over Internet coordination, in the same way as it has rejected in 2001 the creation of the International Criminal Court in The Hague to assure its officials were never encumbered by a bastardized, overzealous judicial process. That said, the scenario that Internet infrastructure is the most useful line of defense against this sort of action against US interests is highly unlikely.

These examples of US authority over ICANN relative to US sovereignty points to a single observation: the power that ICANN provides the US to achieve its will is somewhat illusory; in most cases, it is through domestic law that the US influences how the Internet operates in the country, not via ICANN. In other instances, the US uses ICANN's own processes but does not depend on them. The conclusion here is that though the US seems to have power over Internet coordination, either it didn't exercise it to the fullest to be successful, or its power is less than perceived. From the perspective of countries outside the US, America has complete control over everything that happens regarding Internet infrastructure coordination; but from the point of view of US government officials, they are bound to act in accordance with the rules of ICANN that they helped establish -- which relies on process, transparency, and independent decision-making. Though this obviously takes place within the framework of a prominence of US influence, it is clearly far less than if Dr. Postel's IANA operation was to have been put out for rebids as a function of the Federal Communications Commission (as one US government informal proposal at the time suggested), or made a function of the US military -- both plausible options at the time.

It is hard for people of different political and legal traditions to understand, but US oversight authority of ICANN actually constrains US power over Internet coordination as much as gives it privileged means to influence it. The US must act under the rule of law. The US government is accountable to administrative rules [144] and its agencies are held under tight scrutiny by Congress. There are burdens of transparency and documented due process it must adhere to. US's authority must be exercised under ICANN's established procedures. As examples of this, consider the case of the root server redeployment discussed above and in note 99; though it revealed a more assertive approach by the US than is often publicly seen, the incident was made known after Freedom of Information Act request, and the US officials took pains to follow the ICANN process, at least superficially, rather than impose its will directly. There are few other jurisdictions in the world where government power is itself so held in check by the very same laws that the government itself creates.

Furthermore, the US's authority must be exercised gently. It cannot be so great as to upset the delicate balance of power among stakeholders, which if disrupted, and parties decide to deviate from the IANA-sanctioned domain name system and IETF standards, would risk fracturing the universal interoperability of the Internet. This would set back broader US interests in a single, seamless platform that preserves the end-to-end connectivity of the network, which is its hallmark, and is responsible for the key benefits the US derives from the infrastructure. The interconnectedness of the Internet relies on cooperation, which if jeopardized, would undermine the very thing US oversight authority seeks to maintain. As such, the US has not assertively exercised national sovereignty over Internet infrastructure coordination notwithstanding its oversight authority of ICANN.

2. Possible Effects of Shared, Multilateral Control

The previous discussion has set the groundwork for attempting to answer the central question: what is the impact on American interests if the country has less direct control over Internet coordination, and the influence of other stakeholders were to increase, notably by other governments and international organizations? Where the analysis leading up this has been somewhat long, this section is kept intentionally short. (That said, readers who skip to this section will be disappointed; it does not address the particulars of each dimension where Internet infrastructure is impacted -- to so would be to repeat much of what has been discussed already -- rather, it draws on the previous analysis to identify policy points that warrant consideration. I will summarize my analysis in another form.)

The Internet is decentralized and is devoid of institutionalized intergovernmental obligations. The Internet is a protocol -- an agreement -- and as such, any party can agree to do otherwise at any time; the IANA root and IETF standards, as administered by ICANN, is convenient, but not mandatory. It should not be sacrosanct. Likewise, the Internet's lack of institutional political structure allows it to defy definition and evolve in a manner that places a premium on technical progress rather than risking stasis due to commercial or governmental interested that are wedded to it, like in other communications media. Provided that the Internet's underlying decentralized architectural character is preserved so that new technical innovations can succeed the old; and its multi-stakeholder procedural structure is maintained so that no one party among industry, technologists, civil society or government (to name but a few) has dominate control; the effects of a diminished US authority is likely to be minimal to non-existent.

The US must safeguard these two central policy objectives -- decentralized architecture and multi-stakeholder control -- since these aspects are most placed at risk by increased intergovernmental influence. The US should develop contingency plans, as it does for many such areas marked by low-probablity, high-impact risk. But it does not on its face require the US reassess its policy of transitioning its oversight of Internet coordination to an independent entity that realizes these principles. Furthermore, the actual institution that performs these functions is less important so long as US interests are met. It may be ICANN; or some other; or possibly a combination of institutions. This agnostic approach towards the current organization is referred to below as "XCANN."

A. Classic Coordination Areas

The US is likely to retain special influence over Internet coordination matters even with an independent entity managing Internet infrastructure, due to the country's large commercial prowess, as it does in many other international setting. In 1998, when the US government settled on a policy to devolve its control, the initiative fit squarely with American interests because a private-sector-led approach meant that control didn't actually go very far away -- from one Bill to another, for so to speak (i.e. from Bill Clinton to Bill Gates). US technology companies -- Microsoft, AOL, Cisco, Intel, Dell -- for the most part *are* the Internet and have the responsibility of devising and then adhering to IETF standards. The tier-one US backbone networks have the vast majority of "routes," or end-user connections, such that any network that is not connected to the US backbone can scarcely be considered to be on the Internet at all. Though this will surely change, it will not diminish in any abruptness that should make US policy makers uneasy with less formal control over ICANN. That said, there are a number of issues that must be taken into account.

* ***Generic Domains*** -- Other countries will seek to operate registries, just as there is a competition to receive UN secretariats or the Olympic Games. The US should encourage the spread of non-US domain registries, provided that legal safeguards for US users are ensured in those jurisdictions. There may be calls to rebid the .com, ,net and .org registries, and for symbolic reasons, delegate their administration to companies outside the US, to show the degree of internationalization. This, however, represents a degree of policy instability and risk to the interests of US users. The legacy open domains of .com, .net and .org, can essentially be considered as US national domains that are available to non-US registrants. If the registries were to move outside of US jurisdiction, there is a degree of uncertainty in how they would be managed. The US should establish a means to maintain oversight of them, which probably means rescinding ICANN's control and having the Dept. of Commerce act as the agent to delegate operational control to private sector firms to administer (as it does today with .us and .edu). The US may be able to assert rights to them, considering they were devised in 1985 under US funding (though a cooperative agreement in 1992 with Network Solutions Inc. left the matter of intellectual property rights unclear).

* ***Country-Code Domains*** -- Countries will press for sovereignty over their two-letter country-code domains as a matter of international law. It should be granted, but in a responsible manner than protects the institutional design of the Internet coordination system itself. For instance, the management of country-code domains should take place in a forum that is associated but independent of ICANN, so that ICANN is distanced from the politics. The ITU may be an appropriate body, so long as it acts in association with ICANN and its multi-stakeholder design -- this relationship would need to be formally established. The country-code domains would also have separate rapports with the root server system, so that it bypasses ICANN's process of managing the root. ICANN's responsibilities, under this approach, would be focused on new generic domains.

* ***IP Numbers*** -- There will be calls to place IP number allocation procedures on a footing other than technological need, since the West under such a system will always have a predominant amount of blocks relative to other countries. The migration to IPv6 relieves some of the concerns over the degree to which numbers are scarce (though still finite), so will not cause problems so long as technical criteria is used to make allocations, and the process is non-discriminatory and transparent. The US should encourage a migration to IPv6 by US entities. The issues here have not been as political as in other areas of Internet management; due to its technical rather than legal or social nature, it is extremely remote that IP numbering will be at risk from a transfer of US to independent control of Internet coordination; if US interests were threatened, the US has the means to remedy the situation technically [145]

* ***A Root Server*** -- There will be calls for the A Root Server to be placed up for rebid regarding its management, which could be won by a non-US company. Overtime, this

operation from other countries is poses little risk, but in the immediate term and foreseeable future, the A Root Server should remain in the US, to prevent against any policy instability and for the physical security of the machine. Today, its power is almost completely symbolic and not real, though that does not prevent other governments from endowing it with significance. Still, the US should wait until the stability of the new institution is assured before any transition of physical control is made.

* ***Secondary root servers*** -- There will pressure from other counties to change the placement of root servers so that they are re-located to their countries or continents, on technical grounds, for symbolic purposes, and for balance-of-power reasons to ensure that Internet management is suitably shared that no one entity has too much control. This should be implemented, but in a way that assures root server management does not harden in place due to political interests, and that the system retains protections for US users. For example, a new system can be instituted whereby a fraction of root servers are based in different regions of the world and its technical control is regularly rotated through countries in the region, perhaps on an annual basis. This is mainly for symbolic purposes, though it does further security interests as well. Alongside this, a number of permanently-placed root servers should exist (akin to permanent member of the UN security council); the US should retain control of at least two servers.

* ***Standards*** -- Provided that there are no explicit attempts to capture control of Internet standards from the IETF by a political or commercial entity, there is probably no risk to American interests from a diminished US control of Internet coordination. The US can't even control the IETF -- even the IETF can't control itself! -- it's unlikely another entity can. That said, the US should ensure that the IETF does not have a monopoly on Internet specifications by allowing technologies to emerge from other forums and be deployed, though they may not carry their title of an Internet standard. The Internet's end-to-end design approach makes this especially possible, and attractive.

B. Policy Formation and Scope ("*XCANN*," GAC, Institutional Model)

In addition to the technical functions of Internet coordination, a new concern emerges: the political functions, and how they are addressed in an international, multi-stakeholder setting.

* ***XCANN* --** Countries should not be dogmatic on what institution is used as the locus of Internet coordination. However, the institutional design will require international legitimacy; states can become involved if only to identify in what ways they agree not to become involved. The US should make it a diplomatic priority to ensure that XCANN receives governmental backing (though perhaps not formal recognition). The body should not be held sacrosanct -- its mandate should make clear that it is not to be considered the one principle forum where Internet management takes place. Also, the group's remit should make clear that it mustn't treat the Internet in a way that precludes technologies that wil succeed its institutional scope.

* *Governmental Advisory Committee* -- Governments will want to establish a more formal body ti discuss Internet management matters, and with sovereignty over their country-codes, will be inclined to use ICANN's GAC to serve that purpose. This would be a mistake, because it would establish formal governmental control close to the heart of ICANN's mutli-stakeholder process. Rather, a diversity of forums should be considered. For instance, GAC should remain an advisory committee to ICANN for the purposes it plays now. Government standing on ICANN matters should take place in a separate forum, that relates to, but is outside of, ICANN's structure. The control over Internet infrastructure that nations have by dint of sovereignty over their country-code domains should not extend to control over the system at a global level, since this would jeopardize the multi-stakeholder model.

* ***Institutional Model*** -- The key attributes of the Internet management structure include: decentralization of authority, openness, flexibility, multi-stakeholder process, internationally legitimate, no one organization to manage but many, as well as classic values of transparency, accountability and prevention of capture. The participation of all stakeholders is the key. [146] These qualities fits the needs of Internet management. [147] Yet they clearly do not speak simply to ICANN but to other issues where international cooperation is needed and is institutionalized. In that respect, ICANN can serve as a model for other global approaches. This should be kept in mind as policy and institutional design choices are made. It is important that the system remains open to its own demise -- that this approach to coordination does not harden in place the existing architecture of the Internet. While it serves to ensure the interoperability of the Internet, it should not prevent other mechanism that challenge its control from forming.

* ***Internet Governance*** -- Many countries will naturally try to endow the new institutional setting with additional responsibilities or take problems or political squabbles to it. This is a particular risk with such a cross-jurisdictional medium like the Internet. As we've seen, the notion of "Internet governance" is increasingly used to mean any area where governments want to be involved with the Internet. At the same time, this paper has shown, they are and should continue to be. One way to establish a means to handle this matters is to create a forum where Internet issues can be formally discussed among governments. It can take on a similar structure to the OECD. It can be treaty-based but not treaty-making (a critical distinction); it can exercise soft-law in compelling informally agreed upon best practices. It can act as a centreal hub that documents the work going on at other intergovernmental forums, but not try to compete with them. It can do the all important task of providing neutral, intellectually rigorous statistical measurement and policy advice on issues that governments bring to it. It could have a light-weight secretariat and meet twice-yearly. In this way, Internet issues can be discussed at the bureaucratic level of national administrations, and not the political level, yet still provide a forum for discussion, issue identification and negotiation.

Conclusion

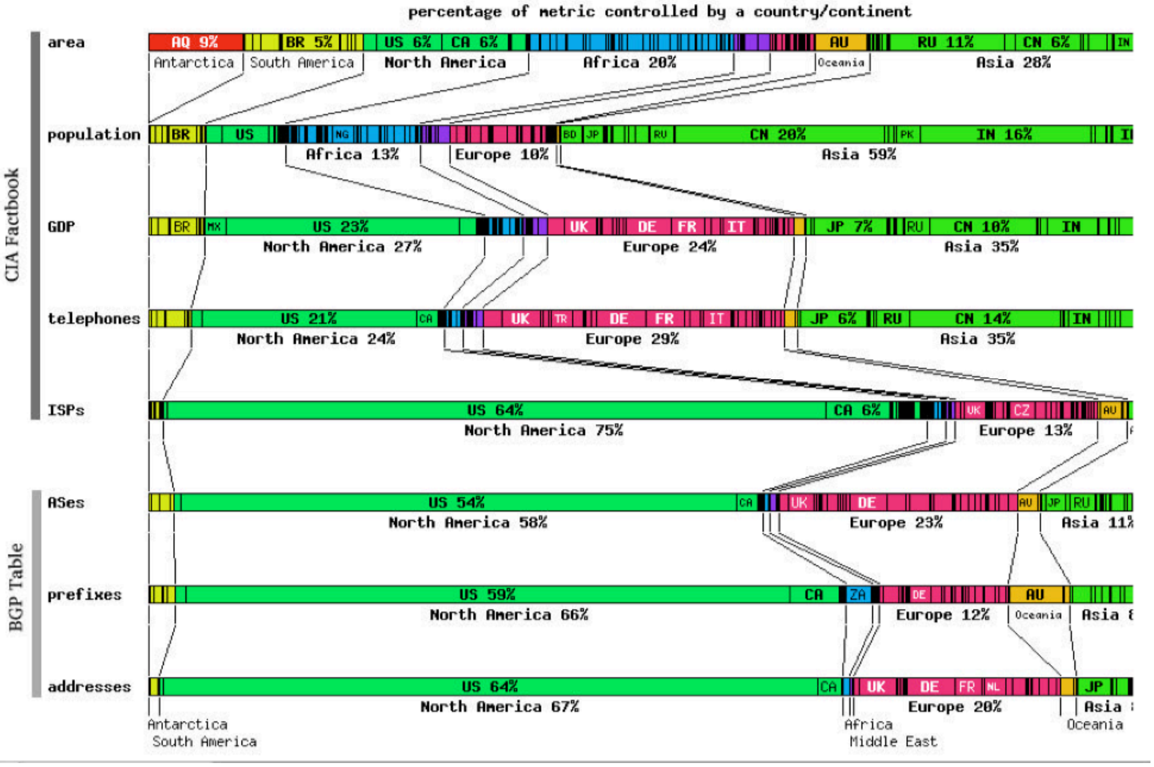
Internet infrastructure coordination matters greatly to all countries, but it is only a vial interest if it is done badly, deviously, or not at all. The power it represents is largely symbolic or illusory. That said, those without control (other countries) for the most part don't recognize this, and the country with the authority doesn't appreciate the degree to which the outsiders want in.

The reality is more banal: the US only has power so long as it remains unused; nothing prevents other parties deciding to deviate from ICANN standards and what the US might propose, if they object to it. Moreover, any benefit that the US could derive from its control, the country can achieve elsewhere, usually more easily and efficiently. For instance, if it wants to regulate WHOIS accuracy or impose content controls to block adult material from minors. Lastly, over time, there will be more problems for the US from retaining control than ceding it.

It is important to remember the serious shortcomings of the Internet. There is so many ways it is still unwieldy, with spam, security vulnerabilities privacy-eroding spyware, and hackers intercepting our communications. The question is how to overcome these problems that are partially due to concerns at the infrastructural level, without jeopardizing the openness of the network for innovation and renewal. And the preserve the openness of the network that makes it a vital means for human betterment and individual freedom that is the rightful aim of public policy for an enlightened, interconnected age.

Appendix A: Internet Infrastructure Resources as a Matter of International Politics

The following chart appeared in a report prepared for the European Union. The findings, while interesting, belie the more pertinent point that the chart itself sheds insight into what international policy makers are thinking about regarding Internet coordination and the impact of US control. Internet resource issues are being considered alongside classic metrics in international relations; the question of equal distribution is explicitly raised.



Source: Jacques H.J. Bourgeois, Jacques Crémer, and Pierre Marsal. "A Study on the Internet Corporation for Assigned Names and Numbers -- Annex." College of Europe; European Legal Studies. Report to the European Commission. November 2003. (Page 12) (http://europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/studies_ext_consult /ICANN_Study_Col_Europe_Nov_2003_Annex.pdf)

From the text of the report:

> "Imbalance in address distribution:
>
> Figure 4 shows the situation of address distribution and its imbalance.
>
> Developing continents in terms of Internet (e.g. Asia, Latin America, and above all Africa) do not get a proper share of the available resource worldwide.
>
> IPv6 could assist in solving this problem."

Appendix B: Country-Code Domains and National Control

The countries and territories that the two-letter codes designate do not actually have sovereignty over their prefixes -- something different than the ITU system of sovereignty of phone numbers under the E.164 international telephone numbering plan. [1] Though granting national sovereignty over country-code domains was clearly specified in the US government's 1998 statement of policy, the White Paper, [2] ICANN has implemented a peculiar interpretation of that. First, it updated Jon Postel's formal but non-legalistic policy that relied on two burdens of accountability of domain managers, to the local and global communities [3] to a sort of joint control that strengthened the role of ICANN and governments, particularly to set the stage for domain name re-delegations [4). Yet in one instance when national control was empirically tested, with something so anodyne as a trademark application by the government of Singapore at the Singapore trademark office for its country-code .SG, ICANN claimed that it held rights to it [5]

A brief word on the motivation and advantages of Postel's private-sector approach is relevant. [6] Postel created this dual accountability system -- that managers must uphold the interests of both the local internet community and the global internet community -- very intentionally; it created a sort of balance-of-power. It allowed for there to be local control and accountability (so that Internet management was decentralized, like the network architecture itself…), while permitting some degree of oversight centrally, since the operation of a domain is visible globally. Here is where the tension between the public and private network causes the most friction, what one scholar of Internet coordination issues, Jeanette Hofmann, has called "the poisoned chalice of Internet governance"; by creating national names rather than sticking with generic ones, the Internet community opened up a door for governments that it would never be able to close. [7]

The two-letter codes signify nations, so governments would naturally have an interest. Postel deferred to an internationally-approved list of countries and territories, called the ISO 3166 list for two-letter country-codes. [8] Postel delegated country-codes to people who where active in the Internet community as a way to see the network grow globally. These people where private individuals, mainly technical experts associated with universities rather than governments. Postel explained that he did this because it was the quickest way to get the Internet deployed internationally with the least fuss -- otherwise, he'd have to track down the right person in each government, probably someone at the foreign ministry or state-run telecom operator, who would have never heard of the Internet and not cared because it was so small and relatively unimportant. [9]

Postel had nothing against government; though a young man during the 1960s, he wasn't a hippie or counter-cultural. He was a techie; he had been an eagle scout. [10] It must be recalled that he not only worked for the government, but the Defense Dept. He voted in every election, usually closely examining all the questions and the candidates positions on issues. In short: he was of the establishment, and not anti-government.

Postel delegated country-codes to private organizations because the Internet was small, technical and arcane -- but mainly out of necessity. It wasn’t even clear what was the relevant government authority; for instance, who speaks for a country: the academy of sciences, the telecom ministry, the national university or the defense ministry, or the prime minister’s office (all which may be jockeying for control)? This is an issue that ICANN still faces, that the early Internet pioneers clearly foresaw, like Postel, Vint Cerf, John Klensin, as well as Scott Brander. It is one reason why the accountability of the “global Internet community” exists, to give Postel’s IANA a sort of “standing” to decide among different groups claiming to represent the interests of the local community. Likewise, it is also why ICANN’s ICP-1 strengthens the influence of government to speak for itself over which agency it wants to manage the domain.

Yet an implication of the technical administrators, and private-sector management of the country-code is that it preserved the informal character of Internet’s operation. These groups are faster moving and more technically competent that governments, many of whose monopoly telephone companies at the time were seeking to undermine the Internet at the ITU among other forums. Besides, managing a domain seemed to be merely a technical function in the eyes of the Internet community; only later were the political dimensions so apparent (and a case can be made that many people still don’t recognize this).

Obviously, the role that governments play in country-code administration is changing. The ITU has been an important catalyst to this, and has hosted well-attended workshops on the matter. [11] Governments are becoming more assertive over their two-letter domains. In a survey of all 189 ITU member states, 56 countries responded, with 47% saying they retain ultimate control over their national domain. An additional 45% said that they are, or are considering, placing the domain on more formal governmental footing. [12]

Notes:

[1] see: ITU. “Overall network operation, telephone service, service operation and human factors.” (http://www.itu.int/itudoc/itu-t/rec/e/e164.html).

[2] See: White Paper, 1998; op. cit. (section: “4. Creation of the New Corporation and Management of the DNS. Response”): “Of course, national governments now have, and will continue to have, authority to manage or establish policy for their own ccTLDs.” It is highly relevant to note that the actual term “sovereignty” was never mentioned once in the White Paper. This can be attributed to the tension surrounding the matter at the time: the US policy needed to be palatable to two difficult-to-please and opposing stakeholders: other countries who wanted more control, and domestic political interests, who wanted the US to retain it. Similarly, it was a time when the notion of government involvement with the Internet was considered anathema. Still, sovereignty was clearly implied.

[3] Jon Postel. “Domain Name System Structure and Delegation / RFC 1591.” IETF. March 1994. (http://www.faqs.org/rfcs/rfc1591.html)

[4] ICANN ICP-1; op. cit.

[5] ICANN. “ICANN Inquiry Regarding .sg Trademark Application.” Email Message from Louis Touton to SGNIC General Manager. January 16, 2003. (http://www.icann.org/correspondence/touton-letter-to-tarmizi-10feb03.htm#Attachment1). It reads, in part: “The IANA has established ccTLDs to facilitate and promote the spread of the Internet globally and has designated managers from time to time to operate them, with the delegated duty to serve the Internet community during the period of that operation.” The incident underscores the degree to which ICANN sought to centralize control, and lacked international political sophistication; a senior government official involved in the matter said the country was surprised by the letter, but withdrew its application knowing that the place to win its position was in the ICANN Government Advisory Committee, not in correspondence with the organization’s general counsel in California. (Interview with author.)

[6] See also: John Klensin. “Reflections on the DNS, RFC 1591, and Categories of Domains / RFC 3071.” IETF. February 2001. (http://www.faqs.org/rfcs/rfc3071.html).

[7] In conversion with author.

[8] ISO. “English country names and code elements.” International Organization for Standardization. (http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/list-en1.html).

[9] Interview author.

[10] Biographical information based on interviews with Postel’s family and friends.

[11] See: “ITU Internet Governance Resources.” (http://www.itu.int/osg/spu/intgov/)

[12] Michael Geist. “Governments and Country-Code Top Level Domains: A Global Survey.” Version 2.0; February 2004. (page 1). “Only seven percent of respondents indicated no formal governmental role in their ccTLD with no plans to alter the present situation.” (www.itu.int/osg/spu/forum/intgov04/contributions/governmentsandcctldsfeb04.pdf)

Appendix C: ICANN's Registry Funding and Domain Name Innovation

Domain names are important since they make the Internet friendly for non-technical people to use; fittingly their administration goes beyond technology, too, and touches upon many social, policy and economic issues. [1] The role and use of domain names have changed since 1985 when the system was created -- but this innovation can be promoted or jeopardized by any financing model imposed on the system. To be fair, this is a notion that wasn't foreseen when ICANN was considering different funding approaches. Domain names were used by machines (Web sites) and people (like email addresses and personal homepages); once registered, and used, they generally remained. A problem was speculators. Few at the time imagined that domain names could be used in much different ways, such as to identify geography, discrete items if information, a business process; a moment in time. The following is a brief discussion to develop this point.

Prior to 1990, domain names identified networks and major host sites on the Internet. Today, they are used mainly for Web sites (human-to-machine multimedia communications) and email addresses (human-to-human text-based communications). The future will surely be different. [2] As mentioned in Part I, domain names are starting to serve for real-time voice communications; as such, they may someday overtake the amount of telephone numbers in the world. And as mobile phone use evolves for Internet-like uses, these sorts of domain names may also emerge [3]

Moreover, when we think of other identifiers that are being incorporated into how we live and interact offline, [4] such as birth certificates, drivers licenses, social security numbers -- things which are migrating online -- the number of possible domain names increases dramatically. A second-level domain for every person today would be 6.5 billion -- and in some of our lifetimes, 20 billion. If the use of names are to evolve just as other aspects of the Internet have progressed over time, it is clear that basing funding mechanisms on the current usage is inappropriate. As more Internet use relies on machine-to-machine communication, the use of names may soar. (An objection to this quandary, that registries could chose to adopt third-level names, not second-level ones, is a moot point: they shouldn't have to adapt what they believe to be the most technically and architecturally efficient way of delegating names simply because of an artificial funding system devised under an earlier set of conditions for how domain names might be used.)

Why should domain names only signify a human, or a machine? Why not geography? Consider that if one were to try to delegate a name for every cubic millimeter on Earth, a mile high, it would be technically feasible to do, but maybe financially impossible under ICANN funding mechanisms. Though this sort of naming initiative may sound strange, there was a proposal before ICANN in November 2000 for a .geo, submitted by SRI International, the renowned Silicon Valley research lab that played a role in the very creation of the Internet, [5], which wasn't very different than this. [6] Why restrict domain names to tangible things -- a slight jump in imagination suggests that domain names can be used to identify pieces of information, such as a song file or a document, in the same way that systems like Digital Object Identifiers are today. [7] To jump again, why should domain names only represent on piece of discrete information like a digital file online -- why not an “incident” of information as it is replicated and flows through the network? Such names may be generated by the hundreds in milliseconds, akin to some approaches to continuous multiple session keys in cryptographic exchanges. And what if the system was such that these domain names expired on a regular basis?

This may sound like science fiction, but it is not -- it is a real, ongoing issue at ICANN: At the Rome board meeting in March 2004, SITA made a presentation to the board on the status if .aero. The organization noted that it would be necessary to re-look at the policy over funding since it was establishing a domain name look-up system for every flight that takes off from every airport every day, retrievable from any sort of device. The service, to provide information on departure time and other things, is undoubtedly a useful and innovative service for travelers, but it is infeasible due to the current funding system. It also would be unable to evolve -- the imaginative techies at SITA can envision having every aircraft part being given its own domain, so that sensors can continuously monitor it. [8] But would funding models prevent this from happening -- and if so, how can we devise a structure so that innovation is preserved? This is an economic interest, but it is above all a societal one, because the bigger implications are what it means for human freedom and progress.

Notes:

[1] For a comprehensive overview of the topic if naming and numbering in communications, see: Joe McNamee, Tiina Satuli. “Policy Implications of Convergence of Naming, Numbering and Addressing: An Orientation.” Final Report for the European Commission. Political Intelligence. September 2003. (http://europa.eu.int/information_society/topics/telecoms/regulatory/studies/documents/nna_final_15sept.pdf)

[2] For an excellent look at the present and future of naming systems online, see: Esther Dyson. "Online Registries: The DNS and Beyond...", Release 1.0, Esther Dyson's Monthly Report, New York. September 2003. (http://www.edventure.com/release1/abstracts.cfm?Counter=6805767).

[3] There has even been application to ICANN for a new domain for the mobile phone industry, See: Mobi JV. “New sTLD RFP Application .mobi Part B. Application Form” Mobi JV (venture among Nokia Corp, Vodafone Group Services Ltd and Microsoft Corp.) March 19, 2004. (http://www.icann.org/tlds/stld-apps-19mar04/mobi.htm).

[4] A good discussion of comparing domain names to other identifiers appears in Mueller “Ruling the Root” 2002.

[5] Additionally, SRI, ironically, for a year in the early 1970s employed Jon Postel while he managed the parameters of the Internet, which eventually became the IANA function, and today, ICANN.

[6] See: SRI. “TLD Application for .geo” October 11, 2000. (http://www.icann.org/tlds/geo1/)

[7] The Digital Object Identifier System (http://www.doi.org/) is led by Robert Kahn, the co-author with Vint Cerf (currently ICANN chairman) of the Internet Protocol.

[8] Andrew Charlton “.aero Update.” (Presentation to the ICANN General Assembly.) SITA. March 5, 2004. (www.icann.org/presentations/charlton-forum-rome-05mar04.pdf). Also, interview with author.

Appendix D: Control of the Root Servers and Policy Evolution

How much power does controlling a root server actually wield? It depends. Today, the root server operators take great pains to say they are only "publishers" of the information that the A ROOT SERVER supplies them, and that where content of the zone file is a political matter, they merely deal with the technical aspects. That said, there is a certain degree of power from running a root server: the issue comes down to control over the system itself, service quality and cost of access, and national vanity.

After A, which is managed VeriSign on behalf of the Dept. of Commerce, 3 servers are under direct US military command (E, G and H); an additional 5 are under US government contract (B, D, J and L); a further 2 are managed independently but inside US jurisdiction (C, by a commercial entity; F, by a hybrid corporate and nonprofit group). The remaining 3 root servers are outside the US: I, in Sweden, run by a company; K, in the UK, run by a nonprofit association of network providers); and M in Japan, at an academic research institution. See table below:

NAME	ADMINISTRATOR	LOCATION .
A.ROOT-SERVERS.NET	Verisign Global Registry Services	Herndon, VA, US
B.ROOT-SERVERS.NET	Information Sciences Institute	Marina del Rey, CA, US
* C.ROOT-SERVERS.NET	Cogent Communications	Herndon, VA, US
D.ROOT-SERVERS.NET	University of Maryland	College Park, MD, US
E.ROOT-SERVERS.NET	NASA Ames Research Centre	Mountain View, CA, US
* F.ROOT-SERVERS.NET	Internet Software Consortium	Various Places
G.ROOT-SERVERS.NET	US Department of Defence	Vienna, VA, US
H.ROOT-SERVERS.NET	US Army Research Lab	Aberdeen, MD, US
** I.ROOT-SERVERS.NET	Autonomica	Stockholm, SE
J.ROOT-SERVERS.NET	Verisign Global Registry Services	Herndon, VA, US
** K.ROOT-SERVERS.NET	RIPE	London, UK
L.ROOT-SERVERS.NET	IANA	Los Angeles, CA, US
** M.ROOT-SERVERS.NET	WIDE Project	Tokyo, JP

** US non-government related*
*** Overseas non-government related*
All other root servers are run either directly or indirectly by the US government

Root server operators today are trustworthy technical experts who see their role as stewards of the Internet, and independent of the contents. What if this were to change? There is little to prevent a single root server administrator from deleting a name from the zone file (rendering all the sites under that domain "invisible" in cases of queries that go to that root); it wouldn't affect all Internet traffic but would disrupt a large bit of it. Likewise, there is nothing to prevent a single root server administrator from adding a new domain to the zone file that the other root servers do not have. The advantage would that the new domain is theoretically visible everywhere, but as in the previous example, in practice it wouldn't be: only queries that go to that particular server would render the rogue domain visible; look-up queries going to other roots would find no such domain.

Thus, while there is potential power in managing a root server on influencing the course of domain name system policy, in reality that power is very meager. (In both cases, the root server that acts unilaterally is no longer "authoritative" -- not longer an exact replica of the A ROOT SERVER.) If political advantages of administering a root server are small other than for a peculiar sort of national prestige among states and bragging rights among techies, there are nevertheless a few technical and economic advantages. Having a root server based close to where users are means that domain name look-ups don't have to be carried over a long distance -- such as across oceans -- which costs money for bandwidth, and degrades the quality of service for users because of the delay. However, the recent "anycast" technology has eliminated this problem; there are now more root servers deployed outside the United States than in it.

Still, some countries want root servers; for instance, government officials from China and France have requested that the country administer one. Some see the US's majority of servers as a mechanism of control. Even Jon Postel was aware of this, and fretted what the US government might do regarding Internet coordination, that he sought to intentionally internationalize the system by deploying the K ROOT SERVER to London in 1997, in the midst of the debate over what institution would coordinate Internet infrastructure (based on author interviews at the time with Internet experts close to Postel.) Some countries fear that the current system opens the opportunity for the US to possibly take a unilateral step and delete a country-code domain, in the same way is it can impose an economic embargo or a declarations of war. Greater distribution of root servers around the world would minimize the chance of this happening. Since it would create a more equal balance-of-power; no one would control the system, so no one could manipulate it to their advantage at the detriment of others, goes the logic.

However, one hole in this argument is that most other countries do not have the same degree of infrastructure that makes operating a root server viable in a networking sense. Some may not have the technical expertise to do so. Moreover, most other nations do not have a sufficient rule of law and predictable legal environment that deploying a root server there makes sense. Even the US has drawbacks in this regard; but the issue has been settled and the sanctity of the root as an administrative function of the government has been established by the courts (See: PG Media v. Network Solutions Inc 1998). What would prevent a court from ordering a root server to remove or add an entry, since it is under that jurisdiction, in the same way as a Paris judge in 2000 ordered Yahoo in the US to block certain content from users in France by way of IP addresses?

A formal structure will need to be established, so that the current root server system -- which is secretive and lacks a process for evolution -- can mature, with intergovernmental legitimacy. That will open the next controversy: whether root servers are deployed on a rotating basis so control is continually shared, like membership in the UN security council by non-permanent members. If so, what percentage of servers should always remain on US soil, and under US military command, to provide the US with adequate confidence in the security, stability and predictability of the system? One can imagine one server in each of the world's four non-US regions, on bi-annual rotation. Yet this would need to take into account the prevention of possible coalitions forming that have an anti-US bias, among other things, to ensure the root-server balance-of-power is stable, and the universality of the Internet's domain name system could never be held hostage.

Notes:

[1] US Dept. of Commerce. “Management of Internet Domain Names and Addresses.” Washington, DC. June 5, 1998. (http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm)

[2] Senior US government officials say that US policy has not changed since 1998 and that the US supports the transition to an independent, private-sector organization to eventually replace US management. (Interviews with author in August and September 2004.) However, the US government has given mixed messages about its intent over time. The uncertainty has been noticed by other governments. A report for the European Commission in 2003 wrote: “History of amendments to the MOU suggests that, while reaffirming the objective of privatising the DNS, DOC has backed away from its initial intention to transfer the management of the DNS to ICANN entirely. Third countries governments have been keen to point to DOC’s failure to live up to its objective of a full privatization.” (Jacques H.J. Bourgeois, Jacques Crémer, and Pierre Marsal. “A Study on the Internet Corporation for Assigned Names and Numbers.” College of Europe; European Legal Studies. Report to the European Commission. November 2003. Page 95. (http://europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/studies_ext_consult/ICANN_Study_Col_Europe_Nov_2003.pdf) Most recently, the Dept. of Commerce stated its desire to “complete the transition to independent, private sector management of the Internet Domain Name System.” (Dept. of Commerce. “Statement by Assistant Secretary Michael D. Gallagher on ICANN's July meeting In Kuala Lumpur.” July 19, 2004. (http://www.ntia.doc.gov/ntiahome/press/2004/icann_07192004.htm).) US government officials point to the three-year MOU with ICANN and suggest that if ICANN completes all the reforms requested, it will be given autonomy. (US MOU with ICANN; 2002, op. cit.) Yet the issue remains cloudy: a GAO report in 2002 stated: “In summary, we found that the timing and eventual outcome of the transition remains highly uncertain.” (US General Accounting Office. “Internet Management: Limited Progress on Privatization Project Makes Outcome Uncertain” Statement of Peter Guerrero Director, Physical Infrastructure Issues. Testimony Before the Subcommittee on Science, Technology, and Space, Committee on Commerce, Science, and Transportation, U.S. Senate. June 12, 2002; p. 3).)

[3] Milton L. Mueller. “Ruling the Root: Internet Governance and the Taming of Cyberspace.” MIT Press. Cambridge, Mass. 2002.

[4] See: UN World Summit on the Information Society “Declaration of Principles” (Point 50) and “Plan of Action” (Section C6, point 13, b), Geneva. December 12, 2003. (http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160).

[5] Robert Cannon. "Will the Real Internet Please Stand Up: An Attorney's Quest to Define the Internet" (March 2004). Telecommunications Policy Research Conference 2002. http://ssrn.com/abstract=516603

[6] J. Saltzer, Reed, D., and Clark, D.D.. "End-to-End Arguments in System Design." ACM Transactions on Computer Systems, Vol. 2, No. 4, November, 1984; pp. 277-288. (http://mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf) A modern look at this is provided in: David Isenberg. “Rise of the Stupid Network.” Computer Telephony. August 1997. pages 16-26. (www.isen.com/stupid.html)

[7] Because when the Internet was first conceived, the transmission infrastructure was secured, and the network itself was closed to only a select group of users, the actual protocol itself was left relatively open. It is only today that we are trying to build in elements of security, identity and accountability in the network. In short, the Net’s openness is the cause of its biggest headaches, from spam to spoofing.

[8] David Weinberger. “Small Piece Loosely Joined: A Unified Theory of the Web.” Perseus Books, April 2002.

[9] The author owes this summary to Scott Bradner, a longtime senior member of the Internet’s standards body the IETF, in conversation

[10] This is not a purely mythic understanding; two historical examples support this image. First, France's Minitel system was a closed, centralized system; though widely adopted, it was expensive to use since everything a user did was billed for. When the Web emerged, the Minitel died a fast death, despite France Telecom's attempts to keep it alive to preserve its revenues. Secondly. the difference in approach can be seen in email. In closed, centralized networks such as CompuServe, a popular network service provider in the 1980s and early 1990s, emails where charged for individually -- like phone calls -- as opposed to the more open Internet, where email was considered a relatively free a service that was not charged for per unit. We are witnessing a similar sort of approach crop up today with mobile telephone companies approach to wireless data applications: because they control the infrastructure, they are metering and billing per use, rather than a near unlimited use policy which is the philosophy behind the Internet's charging model. .

[11] For more on this, see: David D. Clark, Marjory S. Blumenthal. "Rethinking the design of the Internet: The end to end arguments vs. the brave new world." Telecommunication Policy and Research Conference (TPRC). Arlington, VA. August 10, 2000. ONLINE CITE. Aslo, see: Hans Kruse, William Yurcik, Lawrence Lessig. "The InterNAT: Policy Implications of the Internet Architecture Debate." Telecommunication Policy and Research Conference (TPRC). Arlington, VA. 2000. (www.tprc.org/abstracts00/internatpap.pdf). There has even been talk of "e2e's" demise. See: Mark A. Lemley and Lawrence Lessig. "The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era" (October 2000). UC Berkeley Law & Econ Research Paper No. 2000-19; Stanford Law & Economics Olin Working Paper No. 207; UC Berkeley Public Law Research Paper No. 37. (http://ssrn.com/abstract=247737).

[12] For a good examination of the US and European approaches to the Internet and their consequences, see: Raymund Werle. "Lessons learnt from the Internet. Hands off, hands on, or what role of public policy in Europe?" Max Planck Institute for the Study of Societies, Cologne, Germany. 2001. For a look at how this has affected International telecommunications regulation, see:

[13] Paul Starr. "The Creation of the Media: Political Origins of Modern Communications" New York: Basic Books, 2004.

[14] This is not to idolize the early days of the Internet; serious competitive disagreements risked fracturing the Internet or jeopardizing its openness on a number of occasions. One good reference of these disputes appears in: Jay P. Kesan, Rajiv Shah, "Fool Us Once Shame on You; Fool Us Twice Shame on Us: What We Can Learn From the Privatizations of the Internet Backbone Network and the Domain Name System." 79 Wash. U. .L.Q. 89 (2001).

[15] A number of people have made this point, including William Drake, Milton Mueller, Larry Lessig, and Yochai Benkler, as well as the International Chamber of Commerce. See also: Kenneth Neil Cukier. "Internet Governance and the Ancien Regime." Swiss Political Science Review, Spring 1999. (http://www.ib.ethz.ch/spsr/debates/debat_net/art-1-3.html) One of the best references for how the Internet has been coordinated, particularly in reference to its decentralized design is: Sharon Eisner Gillett, Mitch Kapor. "The Self-Governing Internet: Coordination by Design." In: Coordinating the Internet (Brian Kahin and James Keller eds). Cambridge: MIT Press. 1997.

[16] ICANN. "ICP-1: Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation)" Internet Corporation For Assigned Names and Numbers. Marina del Rey, Calif. May 1999. (http://www.icann.org/icp/icp-1.htm).

[17]: Milton Mueller. "Rough Justice: A statistical assessment of ICANN's Uniform Dispute Resolution Policy." The Information Society 17 (3). 2001. (http://dcc.syr.edu/miscarticles/roughjustice.pdf). Also, see: Michael Geist. "Fair.com?: An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP" August 2001. (http://aix1.uottawa.ca/~geist/geistudrp.pdf).

[18] For an excellent description, see: Craig McTaggart. “E PLURIBUS ENUM: Unifying International Telecommunications Networks and Governance.” Telecommunication Policy and Research Conference (TPRC). Arlington, VA. October 2001. (http://arxiv.org/abs/cs.CY/0109091).

[19] This view is not universally accepted, though is a principle among leading Internet engineers; see: Internet Architecture Board. “IAB Technical Comment on the Unique DNS Root.” RFC 2826, Internet Society, May 2000. (www.faqs.org/rfcs/rfc2826.html). For an extremely well argued opposing view, see; Milton L. Mueller. “Competing DNS Roots: Creative Destruction or Just Plain Destruction?” Telecommunication Policy and Research Conference (TPRC). Arlington, VA. October 2001. (dcc.syr.edu/miscarticles/competing-roots.pdf). A second view in favor of multiple roots comes from a former ICANN director; see: Karl Auerbach. “What I would say to the House Commerce Committee were I invited to testify.” Section: 2. Multiple Roots are ‘a good thing’. Personal Web site. July 17, 1999. (http://www.cavebear.com/cavebear/growl/issue_2.htm#multiple_roots). Though I agree with Mueller that the market can remedy coordination issues, I defer to the IAB on the sanctity of a base-line of universal connectivity as an imperative, which the IANA-sanctioned root provides. The Internet is a critical public infrastructure in all but regulatory policy.

[20] Importantly, the “IANA functions” is the legal term used to describe “Internet coordination” or management of the domain name system; if the US were to rescind support for ICANN and assume complete responsibility for Internet infrastructure coordination, they would do so via their authority over IANA, which is established by a Cooperative Research and Development Agreement (CRADA) between ICANN and the US Dept. of Commerce.

[21] For an excellent summary of how to conceptualize governance and institutions of Internet policy issues, see: “Reframing Internet Governance Discourse: Fifteen Baseline Propositions” Memo #2 for the Social Science Research Council’s Research Network on IT and Governance. 2004. (http://www.ssrc.org/programs/itic/publications/Drake2.pdf).

[22] Many tried; attempts include: Alternic.net, UltraDNS, eDNS, Alternative DNS, UCANN, Open Root Server Confederation, and New.net (this latter receiving millions of dollars in venture capital funding by IdeaLab, a noteworthy private equity fund.) Because ISPs defer to the IANA-sanctioned root to preserve global interoperability, there has never been critical mass for the alternative domains to be used. More serious is whether an entity with formal power were to attempt to deviate from the IANA-sanctioned root; that is, a domain registry or a country. This danger has been anticipated in two respects. First, in the 1998 agreement between the US government, ICANN and Network Solutions Inc. (now VeriSign) to manage the domain name system, NSI is forbid from deploying an alternate root system (Note point 4.E.: “In the interest of the smooth, reliable and consistent functioning of the Internet, for so long as the Cooperative Agreement is in effect, NSI agrees not to deploy alternative DNS root server systems.” Dept. of Commerce. “Tentative Agreements among ICANN, the U.S. Department of Commerce, and Network Solutions, Inc.” Amendment 19 to Cooperative Agreement # NCR 92-18742. US Dept. of Commerce, Washington, DC. September 28, 1999. (http://www.ntia.doc.gov/ntiahome/domainname/agreements/amendment19.htm). Second, when non-Roman lettered “internationalized” domain names were starting to gather pace in 2000 and 2001, there was a great effort to bring China into the formal standards process for fear that the country would otherwise develop its own naming system, and have the scale to launch a de facto second root system.

[23] Kenneth Neil Cukier. “You Gotta Believe.” WorldLink: The magazine of the World Economic Forum. Euromoney. London. Nov.-Dec. 1997.

[24]: For the contrary to this, cf. Mueller 2001, idem.

[25] It is a long, ugly history. See: Mueller “Ruling the Root.”

[26]: ICANN. “Revised Proposed Budget -- Fiscal Year 2004-2005” ICANN. Marina Del Rey. July 2004. (http://www.icann.org/financials/budget-fy04-05-21jul04.html)

[27] “Of the 723 resolutions passed by ICANN, 597 were passed without a dissenting vote. Only ten of the 42 people to sit on the Board cast a single nay vote during their tenure.” From: John Palfrey. ”Public Participation in ICANN:A Preliminary Study (Sidebar: Analysis: The Board Votes)” Working paper of the Berkman Center for Internet & Society, Harvard Law School. Fall 2003. (http://cyber.law.harvard.edu/icann/publicparticipation/board-votes.html) The data, undated, is more useful as being evocative of a broader trend rather than for making a concrete point because of shortcomings in the methodology, which Palfrey acknowledges. It treats all resolutions equally without accounting for symbolic resolutions (e.g. thanking a city for hosting a board meeting), which occur frequently, versus substantial ones (e.g. changing bylaws). The data was not used in the final version of the study, which appeared as “The End Of The Experiment: How ICANN’s Foray Into Global Internet Democracy Failed” in the Harvard Journal of Law & Technology; Volume 17, Number 2, Spring 2004.

[28] In 2001 and 2002, with a new US administration, the Dept. of Commerce expressed dissatisfaction with ICANN and demanded a number of reforms and regular progress reports. See Dept. of Commerce. “MOU Between US Dept of Commerce and ICANN, Amendment 5.” Dept. of Commerce. Washington, DC. September 20, 2002. (http://www.ntia.doc.gov/ntiahome/domainname/agreements/amend5_09192002.htm). A Dept. of Commerce statement said: “ICANN has been troubled by internal and external difficulties that have slowed its completion of the transition tasks and hampered its ability to garner the full support and confidence of the global Internet community. […] The Department has frankly been disappointed that ICANN's progress on the MOU tasks has moved so slowly.” Dept. of Commerce. “Dept. of Commerce Statement Regarding Extension of MOU with ICANN.” Dept. of Commerce. Washington, DC. September 20, 2002. Section C and E. (http://www.ntia.doc.gov/ntiahome/domainname/agreements/docstatement_09192002.htm).

[29] Adam Peake. “Internet Governance and the World Summit on the Information Society.” Association for Progressive Communications. June 2004. (http://rights.apc.org/documents/governance.pdf). See also: Audrey Selian and Kenneth Neil Cukier. “The World vs. The Web: The UN's Politicization of the Information Society. Report on the World Summit on the Information Society; Geneva, Dec. 2003.” In Information Technology and International Development (ITID); special issue. MIT Press. (Forthcoming 2005).

[30] Some people in the technology community would disagree with this statement, saying that there is very little conflict of resources, that when it occurs it could be smoothed out by market forces, and that the process of coordination can be automated rather than rely on humans, which confers power by dependence on individual judgment. However, this view is marginal and inherently contradictory (i.e. no authority is needed if the process were automated using technology -- but the technical systems are designed by people based on their values) that it can be dismissed. Examples of this technical nirvana approach is the Open Root Server Confederation (http://www.open-rsc.org/).

[31] Kevin Werbach. “Digital Tornado: The Internet and Telecommunications Policy.” OPP Working Paper Series no. 29. Federal Communications Commission, Office of Plans and Policy. Washington, DC. March 1997. (http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp29.pdf).

[32] White Paper, 1998

[33] This is a controversial matter, particularly diplomatically. It came into the open at an ITU workshop in March 2004 by China, which formally stated: “The working group should be open and inclusive to all stakeholders, whereas the governments and intergovernmental organizations should play the leading role in the whole process, both on the issues of domestic and international internet governance. The reason is that the focus of this issue is of special interests to the sovereign countries, and governments have broader representation, while the private sector and civil society only represent their respective limited groups.” From: ITU. Chairman's Report from ITU Workshop on Internet Governance. Geneva. April 2004. (p. 15) (http://www.itu.int/osg/spu/intgov//forum/intgov04/workshop-internet-governance-chairmans-report.pdf)]

[34] Katie Hafner and Mathew Lyons. “Where Wizards Stay Up Late: The Origins of the Internet.” New York: Simon and Schuster. 1996.

[35] Joshua Gordon. “Illegal Internet Networks in the Developing World.” Berkman Publication Series, Harvard Law School’s Berkman Center for Internet & Society. February 2004. (http://cyber.law.harvard.edu/home/2004-03).

[36] For an excellent discussion on the power of the Internet for development, see: Ernest J. Wilson III. “The Information Revolution and Developing Countries.” MIT Press, Cambridge, Mass. June 2004. (http://mitpress.mit.edu/catalog/item/default.asp?tid=9583&ttype=2).

[37] See: Shanthi Kalathil. “Community and Communalism in the Information Age.” Brown Journal of World Affairs, Volume IX, Issue 1. Spring 2002. (http://www.ceip.org/files/Publications/kalathil_bjwa.asp?p=5&from=pubdate). Also: Clay Shirky. “A Group Is Its Own Worst Enemy.” Networks, Economics, and Culture mailing list. July 1, 2003. (http://www.shirky.com/writings/group_enemy.html). The most impressive example of community-building for political action was the 1997 Nobel Peace Prize awarded to Jody Williams of the International Campaign to Ban Landmines, who used the Internet to rally support for the cause. See: KC Wildmoon. “Peace through E-mail: Wired activists find strength in cyberspace.” CNN Interactive. 1997. (http://www.cnn.com/SPECIALS/1997/nobel.prize/stories/internet.coalition/). An early look at the use of the Internet for community-building is in Howard Rheingold. “The Virtual Community: Homesteading on the Electronic Fronteir.” New York: Perennial. 1994. (www.rheingold.com/vc/book/). A more scholarly look at the notion of group formation online, with terrifying consequences, is: Dorothy E. Denning. “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.” In: “Networks and Netwars: The Future of Terror, Crime, and Militancy.” John Arquilla, David Ronfeldt (eds.). RAND. 2001. Chapter 8. (http://www.rand.org/publications/MR/MR1382/).

[38] See Hafner, 1996.

[39] NRC. “The Internet Under Crisis Conditions: Learning from September 11.” National Research Council. Washington, DC. 2003. (http://www.nap.edu/catalog/10569.html).

[40] Brian Winston. “Media Technology and Society, A History From the Telegraph to the Internet” Routledge. London. 1998.

[41] Anthony Smith. “The Geopolitics of Information.” Faber. London. 1980.

[42] Monroe E. Price. “Media and Sovereignty: The Global Information Revolution and its Challenge to State Power.” MIT Press. Cambridge, Mass. Sept. 2002.

[43] This should be obvious to most people familiar with the Internet, however, it is stated here because in the current environment replete with conspiracy theories, the non-US media has made this link, incorrectly. There is, however, an extremely imperfect way to surveill using the root server, discussed in a note below.

[44] The leap from domestic control of country-code domains, which may seem obvious, to influence over policy formation and operational control on the global level, which may be slightly less obvious, is based on the idea of network externalities inherent with the Internet, i.e. that actions on the network are never localized but are of an interest to all users, in this case, domain administrators. Postel clearly intuitively understood this dimension when he drafted RFC 1591 on the operation of domains, by establishing a dual responsibility for administrators to the local and global Internet communities. For more on this, see: Kenneth Neil Cukier. "Eminent Domain: Initial Policy Perspectives on Nationalizing Country-Code Internet Addresses." Presented at conference “ICANN, ccTLD, and the Legacy Root: Domain Name Lawmaking and Governance in the New Millennium.” March 17, 2003, at Benjamin N. Cardozo School of Law, Yeshiva University, New York. (http://www.cukier.com/inet02.html).

[45] This is a point made by ICANN’s Root Server System Advisory Committee and the Security and Stability Advisory Committee, at the ICANN board meeting in October 2002, a week after a large-scale attack on the roots servers on October 21. (See: ICANN. “Public Forum in Shanghai; Real-Time

Captioning – Morning Session." ICANN. 30 October 2002. (http://www.icann.org/shanghai/captioning-morning-30oct02.htm).) Yet this assessment is not independently verifiable; the secrecy of the RSSAC makes it impossible to confirm. This "security by obscurity" may offer some additional safety, and provide slight advantage or assurance to entities with inside access, like the US government. But it is unclear whether this outweighs the drawbacks that a lack of transparency often entails (i.e. absence of outside review).

[46] Withstood in the sense that users did not receive any degradation of service; in one incident, the root-server survived attack only because the attack stopped on its own; see: ICANN's Root Server System Advisory Committee Report, at the ICANN board meeting in October 2002; ibid.

[47] Control over the root server does not provide any possibility to know the content of communications whatsoever. It is simply an address-matching function, a sort of "signaling system" used by the infrastructure to match the domain name with an IP number for the traffic to be sent. However, it is not beyond possibility that some degree of low-grade surveillance could be established due to control of a root server. Before briefly explaining how, it is crucial to note that the technique is utterly inefficient and there exists far easier and more effective ways to eavesdrop that do not rely on a root server. That said how one could use the root for surveillance is to record the domain look-ups to the root and keep track of the source and destination address of every query; this provides traffic-pattern data on who is trying to reach whom. This is akin to so-called "pen register" and "trap and trace" data with outgoing and incoming phone calls. Again, this is not a very efficient technique: the vast majority of domain look-ups do not pass through the root but are retrieved on local caches, be in the user's computer or Internet service provider. For a technical description of the process, see: Simon Higgs, "IP: more on Re: Roots & Privacy Issues." Interesting People mailing list (managed by Dave Farber). April 14, 2002. (http://www.interesting-people.org/archives/interesting-people/200204/msg00135.html). For a brief, somewhat hyped view on Internet coordination and surveillance, see: Kim G. von Arx and Gregory R. Hagen, "Sovereign Domains A Declaration of Independence of ccTLDs from Foreign Control." 9 RICH. J.L. & TECH. 4 (Fall 2002) (http://www.law.richmond.edu/jolt/v9i1/article4.html).

[48] Rajiv C. Shah, Jay P. Kesan. "The Role of Institutions in the Design of Communication Technologies." TPRC. 2001. (http://www.arxiv.org/abs/cs.CY/0109109). See also: Lawrence Lessig. "Code: And Other Laws of Cyberspace." New York: Basic Books 1999.

[49] This was tried and failed, with a initiative called Raven at the IETF. See: Scott Bradner. "Tapping the 'Net." Network World. Southborough, Mass. November 29, 1999. (http://www.sobco.com/nww/1999.edited/47-tapping.the.net.html).

[50] The US is treating information infrastructure protection and network-based warfare as national security priorities, though the concerns are common to most countries. See: "Plan to Protect Cyberspace" op. cit.; NRC op. cit.

[51] John C. Gannon. "The Global Infectious Disease Threat and its Implications for the United States." National Intelligence Council. Washington, DC. January 2000. (http://www.cia.gov/nic/special_globalinfectious.html).

[52] Though easy to do in theory, it has proven difficult in practice due to the politics of ICANN and its internal disorder. This, however, is changing; the group plans to select three new domains over the next year, to add to the seven it created in 2000.

[53] "In the economic sense scarcity can be said to exist where needs and wants exceed the resources available to meet them. […] In relation to TLDs there are several potential limitations which can lead to a determination of scarcity." OECD. "Generic Top Level Domain Names: Market Development and Allocation Issues." Working Party on Telecommunication and Information Services Policies. Organization for Economic Cooperation and Development. July 13, 2004. (Page 40) (www.oecd.org/dataoecd/56/34/32996948.pdf). For those who may be unconvinced of this, consider two examples. Only one country gets to have its own closed, generic top-level domains in addition to a country-

code -- .gov, .edu and even .mil: the United States, by dint of having created the Net. Likewise, only one individual entity gets .tv (for television) .cd (for CD sales), .gm (for General Motors?), .bt (for British Telecom?) and .nu (for "naked" in French, and "now" in Swedish); of course, these are actually country-codes domains that refer to, respectively, Tuvalu, Congo, Gambia, Bhutan and the island republic of Niue. To be clear, I am in no way suggesting that this is "unfair" or should be "remedied," rather, only that it illustrates the point that domains are essentially rivalrous.

[54] The International Bureau of Weights and Measures was created by the Meter Convention, signed by 17 nations in May 1875 in Paris, during the Diplomatic Conference of the Meter. The International Telecommunication Union was founded in 1865 (when the T stood for "Telegraph") and became a United Nations agency in 1947. ISO, the International Organization for Standardization, was created in 1946 by 25 countries, as a replacement for the International Federation of the National Standardizing Associations, which was set up in 1926 and the International Electrotechnical Commission, established in 1906.

[55] Gordon, op. cit. The author predicts that a flip will occur over the next decade, whereby the more developed countries overtime will try to lock in place the Internet's technology to prevent commercial disruption to their technology industries, while the developing world, as it adopts the Internet, will strive to keep it open. It mirror a classic phenomenon of power and vested interests, as also appears today with the open source movement in the software industry.

[56] Interview by the author with Kenji Kosaka, Senior Vice-Minister for Public Management, Home Affairs, Posts and Telecommunications of Japan.]

[57] For a fuller discussion of the international politics involved with IP number allocation, see: Kenneth Neil Cukier. "Internet Governance, National Interest and International Relations." Background Paper for the United Nations Information and Communications Technology Task Force Meeting, 24-26 March 2004, New York. (http://www.unicttaskforce.org/perl/documents.pl?id=1325).

[58] For more on this point as it relates to international politics, see: Kenneth Neil Cukier. "Don't Let Governments Politicize the Internet." The Asian Wall Street Journal. Hong Kong. November 5, 2002. For a comprehensive study, see: Milton L. Mueller. "Internet Domain Names Privatization Competition and Freedom of Expression." Briefing Paper No. 33. The Cato Institute. Washington, DC. October 16, 1997. (http://www.cato.org/pubs/briefs/bp-033.html).

[59] For an excellent examination of the different policy angles to domain names, see: Stefan Bechtold. "Governance in Namespaces." Loyola of Los Angeles Law Review, Vol. 36, Spring 2003 (http://ssrn.com/abstract=413681).

[60] See: Mueller 2001; op. cit. Geist 2001; op. cit.

[61] See: A. Michael Froomkin. "ICANN's Uniform Dispute Resolution Policy, Causes and (Partial) Cures." 67 Brooklyn Law Review 608. 2002. (http://personal.law.miami.edu/%7Efroomkin/articles/udrp.pdf).

[62] See: Audrey Selian. "ICTs in Support of Human Rights, Democracy and Good Governance." International Telecommunication Union Background Paper for the World Summit on the Information Society. ITU. Geneva. August 2002. (http://www.itu.int/osg/spu/wsis-themes/humanrights/ICTs%20and%20HR.pdf) Also: Deborah Hurley. "Pole Star: Human Rights in the Information Society." Rights & Democracy. September 2003 (http://www.ichrdd.ca/english/commdoc/publications/globalization/wsis/PoleStar-Eng.html).

[63] I am sensitive that the notion of "community values" is often invoked to justify censorship and other restrictions; obviously I'm referring to its true meaning, not a bastardized one.

[64] VeriSign. "The Domain Name Industry Brief." September 2004. (https://www.verisign.com/static/015909.pdf).

[65] OECD 1997; op. cit.

[66] See: ICANN. “Steps to Improve Whois Data Accuracy.” ICANN. September 3, 2002. (http://www.icann.org/announcements/announcement-03sep02.htm).

[67] “ICANN requires domain name registration customers to keep their account information current. Outdated contact information can be grounds for domain name cancellation.” NSI. “Official Notice: Information Update Required.” Email sent to customers. Network Solutions Inc. May 25, 2004. (On file with author).

[68] “A Framework for Global Electronic Commerce” The White House. Washington, DC. July 1, 1997 (www.technology.gov/digeconomy/framewrk.htm) and Dept. of Commerce. “Proposal to Improve Technical Management of Internet Names and Addresses (Green Paper 1/30/98)” Dept. of Commerce. (http://www.ntia.doc.gov/ntiahome/domainname/dnsdrft.htm). It is relevant to note that the US government got involved in “Internet governance,” initially, not because of the highfalutin themes of national interest and geopolitics discussed in this paper, but for something seemingly much simpler: names. Though the "Framework" had sections on security and infrastructure, the domain name system appears only once, in the fourth and last paragraph of the sub-section: “Trademarks and Domain Names.” It begins, ironically: “Governance of the domain name system (DNS) raises other important issues unrelated to intellectual property.” It signals the priority in which the US government initially appreciated, or at least communicated, these matters. (The paragraph ends stating the US government will consider “how best to foster bottom-up governance of the Internet.”)

[69] See: Electronic Privacy Information Center WHOIS privacy web page (http://www.epic.org/privacy/whois/); ICANN’s Generic Names Supporting Organization (http://gnso.icann.org/issues/whois-privacy/index.shtml), and the Center for Democracy and Technology’s letter to Congress on the topic: CDT. “CDT Calls for Privacy Balance in Domain Name Database.” CDT. September 4, 2003, (http://www.cdt.org/dns/030904cdt.shtml)

[70] ICANN is letting the GNSO take the lead in its WHOIS studies. The secretariat convened a committee in 2000-01, called the “.com/.net/.org Whois Committee” (http://www.icann.org/committees/whois/)]

[71] Dan Gillmor. “We the Media: Grassroots Journalism by the People, for the People.” Sebastopol, CA: O'Reilly. July 2004. Chapter 10. Draft online at: (http://weblog.siliconvalley.com/column/dangillmor/archives/010274.shtml#010274).

[72] This is a classic example of ICANN’s dubious behavior (and the incident has been examined well already elsewhere). The dialogue, from the scribe’s notes, is below:
“*Esther Dyson*: .AIR?
Masanobu Katoh: How can we give out .AIR? (Seems like a public resource or something?) Too big. Give .AIRLINES or .AIRPLANES instead?
Vint Cerf: If the string were more precise, less concern here? A reasonable proposal except for this concern that “AIR” is too generic a word.
Hans Kraaijenbrink: A good proposal for a specific sector.
Masanobu Katoh: Would go along with that if the staff negotiates for a more specific string.
Hans Kraaijenbrink: We could think of a more generic term? “.AERO”
Alejandro Pisanty: Fewer questions here about representativeness.
[…]”
ICANN Board Meeting. Scribe's Notes. Marina del Rey, CA. November 16, 2000. Section XI, B.1. (http://cyber.law.harvard.edu/icann/la2000/archive/scribe-icann-111600.html).

[73] While the term “sucks” has entered general American vocabulary to mean some thing bad or of poor quality, its etymology refers to fellatio. This is something that Americans might not readily realize but foreigners would, when trying to understand the word’s meaning, which is not intuitive. That consideration of the domain could advance as far as it did without anyone objecting to it on grounds of proper taste in a

global setting highlights the potential problems that need to be understood, which arise from the US's disproportionate influence over infrastructure coordination. Obviously, many nations would strongly oppose this term being used, regardless of their position on trademark law or criticism in society, which the domain was meant to encourage.

[74] At an ICANN board meeting in Rome in March 2004, a French-speaking director from Africa, Mouhamet Diop, was serially told his concerns were not legitimate when he recommended that ICANN make internationalized domain names a priority. See: ICANN. "ICANN Board Meeting Captioning." March 6, 2004. (http://www.icann.org/meetings/rome/captioning-board-06mar04.htm) This was bad morality and especially bad politics, considering many governments -- vital for ICANN's legitimacy -- had been complaining about the same thing in many intergovernmental venues, from ICANN Governmental Advisory Committee meetings, to the UN's World Summit on the Information Society. Yet since then, there have been many encouraging signs that this is changing, such as ICANN deciding on opening an office in Africa. See: ICANN. "ICANN is calling on the African community to provide comments and input on appropriate modes and locations for ICANN regional presence and more significant participation in ICANN activities." ICANN. 16 September 2004. (http://www.icann.org/announcements/announcement-16sep04.htm). For an early examination of this issue, see: Kenneth Neil Cukier. "Rich Man, Poor Man: The Geopolitics of Internet Policy Making." Internet Society INET'98. Geneva. July 1998. (http://www.isoc.org/isoc/conferences/inet/98/proceedings/5a/5a_2.htm).]

[75] Data in this section comes from Robert H'obbes' Zakon. "Hobbes' Internet Timeline v7.0." Zakon Group LLC. January 2004. (http://www.zakon.org/robert/internet/timeline/).

[76] VeriSign 2004; op. cit.

[77] Even the US computer industry misjudged the issue: as the celebrated (mis)quotes go: "I think there is a world market for maybe five computers," said Thomas Watson, chairman of IBM in1943. Also: "There is no reason anyone would want a computer in their home," said Ken Olson, chairman and founder of Digital Equipment Corporation, in 1977. (See: C. Cerf and Navasky, V. "The Experts Speak: The Definitive Compendium of Authoritative Misinformation." New York: Panteon Books. 1984. Cited online at: NSBA "Exploring the History of Technology." National School Boards Association. (http://www.nsba.org/sbot/toolkit/tnc.html). To that, when the Internet was established, many engineers believed the need for numbers were limited to the hundreds since the network was only meant to connect large super computers at major universities and government sites -- the PC had yet to be invented, never mind today's use of network-enabled devices and cars connected online. See: Janet Abbate. " Inventing the Internet, Cambridge, MA: MIT Press. 1999.

[78] Lessig 1999. op. cit. Also: Ithiel de Sola Pool. "Technologies of Freedom." Cambridge, MA: Belknap Press, 1983.]

[79] On PICS, see: W3C. "Platform for Internet Content Selection (PICS)" World Wide Web Consortium. Undated. (http://www.w3.org/PICS/). On the privacy concerns, see: GILC. "GILC Submission on PICS." Global Internet Liberty Campaign. December 1997. (http://www.gilc.org/speech/ratings/gilc-pics-submission.html).

[80] Joseph Kahn. "Beijing begins censoring phone text messages." The International Herald Tribune. July 3, 2004. (http://www.iht.com/bin/print.php?file=527742.html).

[81] There is, of course, nothing inherent about the Internet that means it will be used to serve freedom or promote democracy; the Net can be used as efficiently by dictators as democrats. On that, see: Shanthi Kalathil and Taylor C. Boas. "Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule." Carnegie Endowment for International Peace, January 2003. See also: David Manasian. "Caught in the net: Instead of undermining repressive regimes, the internet might strengthen them." The Economist (Survey). January 23, 2003. (http://www.economist.com/displayStory.cfm?Story_id=1534249). These pessimistic views are akin to the gloom that suggested in 2001 that Internet stocks were worthless to overcompensate for the giddiness of

1999. The truth lies somewhere in the balance. A rebuttal to Kalathil and Boas is that if the Internet were not such a threat, those same anti-democratic regimes wouldn't be so quick to try to restrict it. A good source for the link between the Internet technologies and democratic freedom is: Christopher R Kedzie, "Communication and Democracy: Coincident Revolutions and the Emergent Dictator's Dilemma," (Section 4: Quantitative Analyses: The Empty Corner) RAND. 1997. (http://www.rand.org/publications/RGSD/RGSD127/sec4.html)

[82] Cf. Speeches by heads of state at WSIS (http://www.wsisgeneva2003.org).

[83] Cf. The comments by the South Africa delegate to the UN ICT Task Force meeting in March 2004, who argued that exercising the power was probably less important than the symbolism that power was shared. A sterilized, anonymized summary of the meeting is at: UNICTTF "Global Forum on Internet Governance - Informal Summary." United Nations Information and Communication Technologies Task Force. New York. 25-27 March 2004. (http://www.unicttaskforce.org/perl/documents.pl?do=download;id=565).

[84] Interviews with author.

[85] The countries that are asserting themselves for a diminished US role and placing Internet infrastructural matter on a more international, intergovernmental basis include China, Syria, South Africa, Vietnam, Cuba and a host of African nations. (For balance, it should be added that some Western countries also take this stance, notably France and Norway.) On countries seeking more control, see Selian and Cukier 2005; on Japan's and Norway's position, see national papers submitted for a meeting to discuss the naming of the UN Working Group on Internet Governance (http://www.itu.int/wsis/preparatory2/wgig/index.html); on countries restricting the Internet, see Gordon 2004 (idem).

[86] Wolfgang H. Reinicke. "Global Public Policy: Governing without Government?" Washington, DC: Brookings Institution Press. 1998. Pages 52-74. (http://brookings.nap.edu/books/0815773900/html/).

[87] See: Robert O. Keohane, Joseph Nye. "Power and Interdependence: World Politics in Transition." Boston: Little and Brown. 1977.

[88] MOU 1998, op. cit. US GAO 2002; op. cit. Note also ICANN lawyer statements in Auerbach v. ICANN: "[...] it [ICANN] then entered into a series of agreements with the Department of Commerce, which still to this day supervises Everything ICANN does, and many things that people assume ICANN -- that ICANN actually does, what ICANN does is make recommendations to the Department of Commerce pursuant to these agreements, and it's the Department of Commerce that ultimately makes these decisions." (Auerbach v. ICANN, July 28, 2002. Court transcript; (p. 9; lines 19-25). Jeffrey Levy of Jones, Day, Reavis & Pogue, represented ICANN before the court. (http://www.eff.org/Cases/Auerbach_v_ICANN/20020729_auerbach_court_transcript.html).

[89] This is due to the Dept. of Commerce's hold on ICANN through the Memorandum of Understanding agreement with IANA functions; and renewal procedures. See: "Management of Internet Names and Addresses," Memorandum of Understanding Between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers (including amendments). Dept. of Commerce, National Telecommunications and Information Administration. 1998-2003. (http://www.ntia.doc.gov/ntiahome/domainname/icann.htm).

[90] White Paper, 1998. Section 1; response.

[91] Such as the board elections and the selection of new top-level domains in 2000, and ICANN's refusal to make rudimentary updates to country-code domain servers even under emergency circumstances, as happened in June 2002 when a KPNQwest, a large backbone network, ceased operations in Europe, which disrupted the smooth functioning of country-code domain names. (ICANN demanded that it be allowed to obtain the entire domain databases; country-code administrators objected to this since it gave ICANN the

power to re-delegate the domains instantaneously, something that shifts the balance-of-power among ICANN and its constituent members. This arcane issue was seen as a means by ICANN to force country-code domain administrators to sign controversial contracts with the organization. The US Dept. of Commerce is said to have privately contacted ICANN to end its practices, after national administrators complained to their governments, who in turned complained to the US). See: Kim Davies. "ccTLD ICANN Meetings in Bucharest." CENTR draft statement. (www.wwtld.org/meetings/cctld/ 20020625.ICANN-AXFR-KimDavies.html).

[92] When the dispute over VeriSign's SiteFinder erupted in September 2003, officials from other countries said privately that they were very concerned that a US company could take such unilateral action which could disrupt global internet traffic, and that this underscored the degree to which ICANN's private-sector infrastructure coordination model, as well as US jurisdictional control, was insufficient to protect the interests of Internet users (and foreign citizens) globally. Ultimately, they said, this highlighted why other governments need to have more control over Internet coordination matters, most likely on a formal, intergovernmental basis. (Information based on interviews with the author.) ICANN eventually threatened legal action, and VeriSign grudgingly "suspended" (not discontinued) the service. VeriSign sued ICANN in federal and California state court for overstepping its bounds as a regulator in February 2004, citing SiteFinder; the case was dismissed in federal district court in August 2004. See "ICANN Litigation Documents. VeriSign Inc. v. ICANN" (http://www.icann.org/general/litigation-verisign.htm)

[93] Cukier AWSJ 2002. Idem.

[94] The phrase originates from Ira Magaziner, the senior advisor for policy at the White House from 1993 to 1998, who oversaw the transition from Jon Postel's IANA to the creation of ICANN.

[95] These worst-case scenarios are remote because, for one thing, they ignore US power as it can be exercised in classical dimensions of foreign policy (trade negotiations, multilateral fora), and which can act to remedy unfriendly actions at an early stage. Second, they fail to take into account the United States technology industrial power, through US firms that influence networking standards like Microsoft, IBM, Dell, Intel, Qualcomm and Cisco, among others, on a commercial basis. They, if need be, could be informally called in to play a significant role in preserving global interoperability in light of US interests and their own competitive interests.

[96] See: "The National Strategy to Secure Cyberspace." The White House. February 2003. (http://www.whitehouse.gov/pcipb/).

[97] ICANN Board meeting minutes, November 15, 2001. (http://www.icann.org/minutes/minutes-15nov01.htm).

[98] The current root-server administrators are professional and have formalized their processes and structure; however, it is unclear how the system will evolve and what role ICANN or governments will have in their operation (for instance, in relocating root-servers). They are the linchpin to the domain name system, for it to work and for new domains to be added to the root (they state that they act as publishers, simply making available what is in the root, but insisting that the decision over its content is made elsewhere). That said, the root servers are also the most effective area where the technologists can exercise their weight in the balance-of-power mentioned in Part I, so there interests are heard. For sources on the "subtle threats," see: White Paper 1998,, at "The Transition" (point 5). This is often reiterated in US government officials' remarks. It is also included, in different wording, in the most recent MOU between the Dept. of Commerce and ICANN. See MOU 2003, at I,B.6: "Continue to consult with the managers of root name servers operated by the U.S. Government […] with respect to operational and security matters of such root name servers and recommendations for improvements in those matters." Memorandum of Understanding Between The U.S. Department of Commerce and ICANN (Amendment 6). September 16, 2003. (http://www.ntia.doc.gov/ntiahome/domainname/agreements/amendment6_09162003.htm).

[99] See: Associated Press. "Lobbying pressure leads U.S. to speed approval of Internet change." December 16, 2002. (http://foi.missouri.edu/federalfoia/lobbying.html). In this case, the Commerce Dept.

approved in two days a request by VeriSign Inc., presented through ICANN, to move the location of a root-server, after the company urged the government to “declare some kind of national security threat and blow past the process,” according to a Commerce Dept. official’s e-mail obtained by the AP under the Freedom of Information Act. The normal process would have taken weeks or months. Commerce Dept. officials actually asked VeriSign to invoke the emergency procedures at a Oct. 30 meeting, because, as one official wrote, “This will allow the change to happen ASAP.”

[100] Benoît Faucon. "Le réseau vraiment sécurisé existe: il est classé secret défense." Les Echos. Pearson Group. Paris, France. November 2000. Translation of excerpt from French (which in turn was a translation of Cerf's original English): "Let me tell you a story that I haven't talked about before now. In 1975, two years after writing the specifications to TCP/IP, the NSA contacted me. They found TCP/IP interesting, but too insecure, and they wanted a version where the exchange of traffic would be more secure. So I worked for them, without ever being able to talk about it with my students. The other network ... is still classified 'top secret'," said Cerf, according to the interview.

[101] The unofficial motto of the IETF, emblazoned on T-shirts that used to be sold at meetings, was a quote from the MIT networking researcher and former chairman of the Internet Activities Board throughout the 1980s, who said in 1992: “We reject kings, presidents, and voting. We believe in rough consensus and running code.” (http://cyber.law.harvard.edu/jzfallsem/trans/clark/)

[102] Interviews with author with individuals at the meetings.

[103] “Wiretapping, even when it is not being exercised, therefore lowers the security of the system.” Internet Architecture Board & Internet Engineering Steering Group. “IETF Policy on Wiretapping / RFC: 2804.” Request for Comments series (Category: Informational). Internet Engineering Task Force. May 2000 (page 7). (http://www.ietf.org/rfc/rfc2804.txt). The scuttled IETF initiative was called Raven. On that, see: Scott Bradner. “Tapping the 'Net.” Network World. Southborough, MA. November 29, 1999. (http://www.sobco.com/nww/1999.edited/47-tapping.the.net.html)

[104] Interview with author with individual at the meeting. Also see: John Markoff. “Agency Weighed, but Discarded, Plan Reconfiguring the Internet.” The New York Times, New York. November 22, 2002.

[105]: RFC 920, “Initial Set of Top Level Domains,” in October 1984 stated: “The use of ARPA as a top level domain will eventually cease.” Like so many legacy technologies, it just stuck around. Yet it fuels conspiracy-thinking. A report for the European Commission in 2003 that mentioned .arpa, in a footnote stated: “As we now know, it did not cease: E-NUM [sic] is part of the arpanet [sic] TLD, i.e. controlled by DOD!” (Exclamation point in the original.) In addition to the style errors, the point, presented breathlessly, is factually incorrect: .arpa is not controlled by the DOD but the IANA, or ICANN/US government; it’s an important difference, and neuters the condemning tone by the authors, who clearly are unaware of the essential-yet-innocuous purpose that .arpa serves. See: Bourgeois, et al. (Annex) 2003; page 15).

[106] This should not be surprising -- they built it (though the allocations were all made in the early 1990s). Only around 20 entities other than address registries have a Class A address block, one each. No other country other than the UK has been allocated a Class A address blocks (it has two; for its military and social security department). Authoritative data on this is notoriously difficult to obtain. Sources are two-fold: Jacques H.J. Bourgeois, Jacques Crémer, and Pierre Marsal. “A Study on the Internet Corporation for Assigned Names and Numbers -- Annex.” College of Europe; European Legal Studies. Report to the European Commission. November 2003. (http://europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/studies_ext_consult/ICANN_Study_Col_Europe_Nov_2003_Annex.pdf). Also, see: OECD. “Internet Infrastructure Indicators.” Organization for Economic Cooperation and Development; Working Party on Telecommunication and Information Services Policies. October 28, 1998 (page 33). (www.oecd.org/dataoecd/11/25/2091083.pdf).

[107] Dept. of Defense. “DoD to Discuss Adoption of Next-Generation Internet” Washington, DC. June 12, 2003. (http://www.defenselink.mil/news/Jun2003/p06122003_p068-03.html).

[108] Tim Gibson (Col.). “Control Plane.” Slide presentation. Defense Advanced Research Projects Agency, Advanced Technology Office. (cleared for public release; distribution unlimited). December 5, 2003. (http://www.darpa.mil/ato/solicit/ControlPlane/proposers.htm)

[109] Rick Merritt. “Darpa looks past Ethernet, IP nets.” CommsDesign.com. CMP Electronics Group. Manhasset, NY. April 26, 2004. (http://www.commsdesign.com/news/tech_beat/showArticle.jhtml?articleID=19201035).

[110] Interview with author, November 1999.

[111] OECD 1998, op. cit.

[112] IETF. “The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force / RFC 3160” Internet Engineering Task Force; Request for Comments. August 2001. (http://www.ietf.org/tao.html).

[113] Dept. of Commerce MOU with ICANN web page; op. cit.

[114] ICANN. “ICANN Has Successfully Completed All Its Objectives under the MOU to Date.” ICANN. 19 July 2004. (http://www.icann.org/announcements/announcement-19jul04.htm).

[115] The Economist. “Internet regulation: Swiss fudge.” December 12, 2003. (http://www.economist.com/displayStory.cfm?story_ID=2288724).

[116] As expressed in the WSIS, as well as in an ITU Workshop on Internet Governance in February 2004, as well an an ITU meeting on country-code domain names in March 2003; note particularly Syria’s intervention in both ITU meetings. See: Kieren McCarthy. “Internet battle lines drawn at extraordinary Geneva meeting.” The Register. March 6, 2003. (http://www.theregister.co.uk/content/6/29612.html).

[117] See national contributions to the WGIG meeting, September 2004 in Geneva, at: (http://www.itu.int/wsis/preparatory2/wgig/index.html).

[118] For instance, China, which has shown itself newly assertive on the technical standards front on issues like WiFi encryption, microprocessor design and taking a lead, although in unison with Japan and Korea, on internationalized domain names.

[119] One area where this could be a real concern is in using Internet infrastructure for copyright protection, where the Recording Industry Association of America successfully lobbied the Dept. of Justice to make fighting the crime of music piracy a priority.

[120] Because copyright must be formally asserted in order to protect that openness from others who may wish to publish the same material for a fee, or publish them with distinct changes in their specifications, an international nonprofit organization called the Internet Society is the copyright holder, making it freely available “as is.”

[121] For an excellent report on the sender-ID controversy in the context of the Internet’s early standard-setting ethos, see: Yakov Shafranovich. “Sender ID: A Tale of Open Standards and Corporate Greed?” CircleID. September 1, 2004. (http://www.circleid.com/article/730_0_1_0_C/)

[122] See: Scott Bradner. “Intellectual Property Rights in IETF Technology / RFC: 3668” Request for Comments. Internet Engineering Task Force. February 2004. (http://www.ietf.org/rfc/rfc3668.txt).

[123] Interview by author with a senior Clinton administration official involved in discussions with the EU.

[124] “Tao of IETF,” idem; 3.3: “The IETF is about technical content, not company boosterism.”

[125] OECD 1998; op. cit.; page 33.

[126] OECD 1998, op. cit. While these figures are out of date today, the pattern is still the same: The prices of dropped across the board, but the US is the least expensive for an "open" domain. It is also often the easiest types of domains to acquire -- one reason why so many people from outside the US register them, along with the appeal of being global for a inherently global medium.

[127] For instance, France is shepherding an initiative with the Organization for Security and Cooperation in Europe, a light-weight, moribund Cold War-era international organization, to consider Internet content regulations regarding hate speech in Europe. The country has attempted to use Internet infrastructure to serve policy objectives, such as in 2000 when a court ordered Yahoo to use IP numbering filtering to prevent French users from accessing portions of its Web site. See: Joel R. Reidenberg. "The Yahoo Case and the International Democratization of the Internet." Fordham Law & Economics Research Paper No. 11. April 2001. Pages 11-13. (http://ssrn.com/abstract=267148).

[128] This issue has raised many times over the years in settings with Internet engineers as well as intergovernmental meetings; see also Appendix A.

[129] ABC. "Tuvalu: Contemplates leasing satellite space." Australia Broadcasting Corp. Radio. July 15, 2004. (http://www.abc.net.au/asiapacific/location/pacific/GAPLocPacificStories_1154482.htm).

[130] See: Lawrence D. Roberts. "A Lost Connection: Geostationary Satellite Networks and the International Telecommunication Union." Berkeley Technology Law Journal. Issue 15:3 (Fall 2000). (http://www.law.berkeley.edu/journals/btlj/articles/vol15/roberts/roberts.html).

[131] This financial manipulation of resource allocation happened with geostationary satellite orbital slots. "Developing country representatives have also stated that the present first-come-first-served system allows the industrial countries to exploit a scarce global resource that is the "common heritage of mankind" and, this being the case, developing countries should also benefit from the common heritage by using it or profiting from its use." OTA. "International Cooperation and Competition in Civilian Space Activities." U.S. Congress, Office of Technology Assessment, OTA-ISC-239. Washington, DC. July 1985 (pages 175-176). (http://www.wws.princeton.edu/~ota/disk2/1985/8513_n.html).

[132] The idea of "sticky power" comes from Walter Russell Mead. "Power, Terror, Peace, and War: America's Grand Strategy in a World at Risk." New York: Knopf. 2004. Hard power is a classic description for military might. The term "soft power," was coined in the 1980s by Joseph S. Nye, Jr. For its application to the non-technical dimensions of Internet-related policy, see: Robert O. Keohane and Joseph S. Nye, Jr. "Power and Interdependence in the Information Age." Foreign Affairs, v. 77 no. 5 New York: Council on Foreign Relations. September/October 1998. For a deeper examination of soft power, see: Joseph S. Nye, Jr. "Soft Power: The Means to Success in World Politics." New York: PublicAffairs; 2004.

[133] Robert Mugabe. "Speech by His Excellency President Robert Gabriel Mugabe of Zimbabwe on the Occasion of the World Summit on the Information Society." WSIS. Geneva, Switzerland. December 10, 2003. (www.itu.int/wsis)

[134] Interview with official present in meetings.

[135] Another problem with US law is that it is dual-edged; in areas like intellectual property some critics argue it is too strict; conversely, in the case of the public availability of WHOIS data, it is probably not strict enough and privacy-friendly rules need to be established

[136] Daniel J. Boorstin. "The Americans: The National Experience." New York: Vintage. 1967.

[137] Jonathan Spence. "The Search for Modern China." New York: W. W. Norton & Co. 1990.

[138] Henry H. Perritt Jr. “The Internet as a Threat to Sovereignty” Indiana Journal of Global Legal Studies, Spring 1998. page 551.

[139] Mariane Pearl. “A Mighty Heart: The Brave Life and Death of My Husband Danny Pearl.” New York: Scribner Book Co. 2003.]

[140] Benjamin Edelman. “Testimony before the US House of Representatives Committee on the Judiciary; Subcommittee on Courts, the Internet, and Intellectual Property.” September 4, 2003 (www.house.gov/judiciary/edelman090403.pdf)

[141] Associated Press. “Feds increasingly seizing Web addresses.” USAToday. March 5, 2003. (http://www.usatoday.com/tech/news/techpolicy/2003-03-05-web-feds_x.htm).].

[142] In that issue, Congress was probably being responsive to the incumbent domain name registrar, Network Solutions Inc,, who stood to lose some amount of potential registrations as its costs increased, and well as face a more wealthy ICANN, which would have had greater financial resources to act as a regulator of domain name registration policy and market access.]

[143] Joel R. Reidenberg. “States and Internet Enforcement.” University of Ottawa Law & Technology Journal, Vol. 1, 2004 (http://ssrn.com/abstract=487965). See also: Reidenberg. :Lex Informatica: The Formulation of Information Policy Rules through Technology.” 76 TEXAS L. REV. 553. 1998. (http://reidenberg.home.sprynet.com/lex_informatica.pdf).]

[144] - This view is contentious, and one policy observer believes ICANN’s very founding was illegal under US rules. See: A. Michael Froomkin. “Wrong Turn in Cyberspace: Using Icann to Route Around the APA and the Constitution.” .Duke Law Journal, Vol. 50, No. 1, October 2000. (http://ssrn.com/abstract=252523).]

[145] In the worse-case scenario, the remote chance of an IP number allocation freeze that is discriminatory to the US, American network providers would nevertheless be protected in two ways. First, a US entity would still be free to “self-assign” IP number space and ensure that they were routable through the enormity of the US backbone network. Second, they could institute “network address translation” from internal numbering systems for individual networks.

[146] Zoë Baird and Stefaan Verhulst. “A New Model for Global Internet Governance.” In “Governance in the 21st Century: The Partnership Principle.” Alfred Herrhausen Society for International Dialogue, 2004. (http://www.markle.org/downloadable_assets/ahs_global_internet_gov.pdf).]

[147] An interesting study of institutional choices based on policy requirements appears in: Lawrence L. Hamlet. “How States Design the Secretariats of International Organizations: Evidence from the ITU and ICANN.” March 2003. (www.internationalorganizations.org/ICANNITUPaperMarch2003_hamlet.pdf). The study is mainly intended to establish a model, with a drawback that its theoretical nature misses empirical factors that require different approaches to take into account. Specifically, Hamlet gives too much weight to intention and not enough to accident in how ICANN was created and its policy needs that may have effected its institutional framework.

# # #