

MSc The Practice of International Affairs 2005

**Dissertation submitted in partial fulfillment of the
requirements of the degree**

Candidate number 85332

**INTERNET GOVERNANCE AS A NEW DIMENSION OF
INTERNATIONAL RELATIONS: FROM AN EPISTEMIC
COMMUNITY TO A NEW INTERNATIONAL REGIME**

**Declaration Statement: I have read and understood LSE's rules
of plagiarism and related offences. All work submitted is my
own, apart from referenced sources.**

Word count: 9855

Table of Contents

<i>The Domain Name System: A Technical Overview</i>	5
<i>Why the Root Matters</i>	10
Internet Governance: Controlling the Root	10
What does Controlling the Root Mean?	11
The Need to Coordinate: The Risk of Alternative Roots	13
Controlling the Root: A Component of Sovereignty	14
<i>History of the Root and of its Governance: From an Epistemic Community to a New International Regime</i>	17
International Regimes and Multiple Stakeholders: The Need to Coordinate	17
The Epistemic Community of the “Founding Fathers”	18
Epistemic Community in the Foreground, the United States in the Background: A New International Regime in Between	20
The Domain Name Wars	24
The Late Involvement of the American Hegemon: Benign Neglect or Machiavellian Strategy? ..	27
ICANN, Flesh of the New Regime	30
<i>Glossary</i>	37
<i>Bibliography</i>	39

Table of Figures

<i>Figure 1: A hierarchical Domain Name System</i>	7
<i>Figure 2: Domain name resolution process of example.com</i>	8

“No government, no matter how powerful, can unilaterally impose or enforce its will on these issues. They embroil too many actors and interests in too many countries to be susceptible to brute, hegemonic force.” (Moises Naim, 2001, 108)

On December 2003, two-thirds of the heads of state gathered in Geneva to attend the first session of the UN-sponsored World Summit on Information Society (WSIS). For the first time in a UN “World Summit”, all stakeholders were invited to participate. Along with governments, the private sector and civil society were invited to take an active contribution into the debates (Kleinwächter, 2003). The heads of states left in a diplomatic dispute on who should control the Internet and in particular the assignment of names and numbers. While the majority of the participants were investigating multilateral and cooperative ways to rule the cyberspace, exceptions were noted. Kenneth Cukier, a research fellow at the National Center for Digital Government at Harvard University's Kennedy School of Government, gives the example of “Zimbabwe’s president Robert Mugabe [who] criticized what he described as a conspiracy by the West to use the Internet as a form of neo-colonialism” (2004b, 46). Mugabe’s speech at the conference was violent and full of political rhetoric. He notably called for “a sovereign national government that manages ‘top-level domains’ within its borders” (Mugabe, 2003). The intention to better control the Internet and to restrict its access via a nationalized management of the root was obvious.

Since the Summit, Internet governance has become a critical strategic and political matter for head of states and a new stake for international relations. As Joseph Nye once wrote:

Cyberspace will not replace geographical space and will not abolish state sovereignty, but [...] it will coexist with them and greatly complicate what it means to be a sovereign state or a powerful country. As Americans shape foreign policy for the global information age, we will have to become more aware of the importance of the

ways that information technology creates new communications, empowers individuals and non-state actors, and increases the role of soft power. (2002, 62)

As far as telecommunications are concerned, international treaties are usually defining the legal and technical environment under which these medium should evolve and function. For instance, the International Telecommunication Union (ITU) of the UN deals with telephony matters and is responsible for the coordination of international phone calls through unified rules and procedures set up by diplomats. Internet governance lacks such a framework of control. Herein lie the specificity of Internet governance and also its main problems.

Diplomats are not the only players here – they came very late into the arena – and other stakeholders such as the very first inventors of the web or private businesses want to play a decisive role by pushing their interests or convictions forward.

The following paper will engage with the aforementioned paradox and attempt to demonstrate why controlling the root of the Internet is of crucial importance for states and why it constitutes a major stake of international relations. To do so, the first part will provide the technical background to understand the specificity of the problem, the second will explain why Internet governance matters for international relations and why it is not a pure technical topic, and the last part will retrace the history of Internet governance from what was initially an epistemic community of its creators to a new international regime created along the American hegemony and embodied by an international institution of a new kind, the Internet Corporation for Assignment of Names and Numbers (ICANN). Specifically, it is argued that tools and concepts of International Relations can be utilized, albeit modified, to understand the evolution of Internet Governance. Given the short length of the document, many technical

aspects will be simplified and the historical part will only encompass major steps, ignoring many details. In the same vein, many terms will be abbreviated and the reader is invited to refer to the glossary at the end of the paper.

The Domain Name System: A Technical Overview

Technically, the Internet can be defined as “a network of networks based on the TCP/IP protocols”¹ that enables connected devices to communicate. The TCP/IP protocols allow the exchange of packets of data between machines “on” the Internet (Loshin, 1997, 3-83). When connected to the Internet, each machine is allocated a unique identifier called an Internet Protocol (IP) address consisting of a series of number like 158.143.192.210, each group of numbers ranging from 0 to 255. This configuration allows the existence of about 4.3 billion unique numbers. The IP address consists of two parts: a part identifying the network and another identifying a particular machine – or host – on this network. Each time data is sent via the Internet, it is split into little packets, which carry the IP address of the sender and the one of the receiver. As Lessig put it “a packet of data is carried “to” and “from” these addresses as it works its way across the Internet” (1999, 32). Since IP addresses are a limited resource, their allocation has become a key political factor beyond their technical function.

Although IP addresses are the core of the functioning of the Internet, they are totally useless to most of the networks users: they are difficult to remember and as Paré stresses “the range of addresses used at various organizational and individual levels is relatively unstructured [...] thus deducing which addresses apply to whom [is] rather arduous” (2003, 10). To cope with these problems, a mapping of alphanumeric character strings to IP addresses has been developed. The coordinating function between the names and numbers is fulfilled by the Domain Name System or DNS. For instance, instead of entering <http://158.143.192.210/> into a web browser, it is easier to enter <http://www.lse.ac.uk> to locate the server hosting the

¹ Refer to E. Kroll for technical definition of the Internet in the RFC of June 24, 1993: <http://mist.npl.washington.edu/internet.txt>

London School of Economics website. The DNS enables the translation – the resolution – of the “name” www.lse.ac.uk into the “number” 158.143.192.210, the IP address understood by all the devices connected to the Internet. IP addresses are designed to be unique sequences pointing to individual machines to avoid what otherwise would be confusion and chaos in the cyberspace. Likewise, an alphanumeric name can only refer to one IP address but many names can refer to the same IP address².

At the origins of the Internet, an entity called the Network Information Centre (NIC) had authority for the allocation of names. Each name was saved in a file called *hosts.txt* with its matching IP address. This file contained the global directory for mapping names to addresses; therefore every network had to download its own copy of the file and used it to resolve names locally. With the rapid expansion of the Internet and the growing number of devices connected, the file put in place at a time when only a few hundreds of computers could access the Internet showed its limits. Each name had to be approved by the NIC, each change in the resolution process had to be communicated to this authority, entered into *hosts.txt* and then downloaded by every computer on the network. With the rapid growth of the Internet, the applications for the same names were more and more frequent and it became more difficult to assign them. Moreover “the list itself became larger and larger, and the process of creating and distributing it consumed more and more resources. The list itself represented a single point of failure” (Mueller, 2002a, 41).

To cope with these problems, a new architecture was designed to replace *hosts.txt*, the DNS. The structure of the DNS was meant to be hierarchical, not linear as was the case with *hosts.txt*. The domain names reflect this multi-level structure: “When the domain name is

² For instance <http://www.wunderground.com> and <http://www.weatherunderground.com> refer to the same IP address <http://66.28.250.176>

written out, the top of the hierarchy is at the right and each segment of the naming hierarchy is separated by dots” (Mueller, 2002a, 41). Thus, in www.lse.ac.uk, the Top-Level Domain (TLD) is ‘uk’, then ‘ac’ is a Second-Level Domain (SLD) included in the TLD ‘uk’, ‘lse’ is a third-level domain, sub-domain of the SLD ‘ac’ and finally ‘www’ is a fourth-level domain. We can thus represent the DNS as a tree:

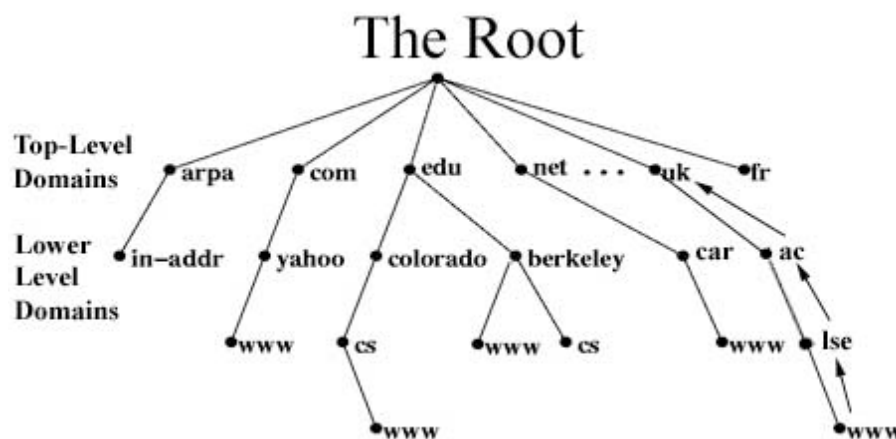


Figure 1: A hierarchical Domain Name System

*Adapted from <http://bio3d.colorado.edu/tor/sadocs/DNS/DNS-1.png>
University of Colorado, Tor Mohling’s Home Page*

As shown in Figure 1, at the top of the hierarchy is the unnamed root. The authority in charge of the root assigns the TLD names such as .com, .edu or .fr. There are three types of TLDs: the country-code TLDs or ccTLDS such as .uk, .ca or .jp; the generic TLDs or gTLDs such as .com, .net or .edu, and a category for an exclusive usage by specialists of the network: .arpa. The ccTLDS were not intended to be “official” to any particular country (Froomkin, 2000b, 40). They were associated with geographic regions based on a list of two-letter country abbreviations promulgated by the United Nations’ International Standards Organization, the ISO 3166-1 list (Mueller, 2002a, 78-79).

Once an entity has been awarded responsibility for a TLD, it has the authority to coordinate the assignment of SLD names under the TLD it is in charge of. The registrant of a second-level domain name (such as yahoo.com) has in turn the unique responsibility to assign third-level domain names (such as mail.yahoo.com); and so on down the hierarchy.

The following figure shows how the resolution process works³:

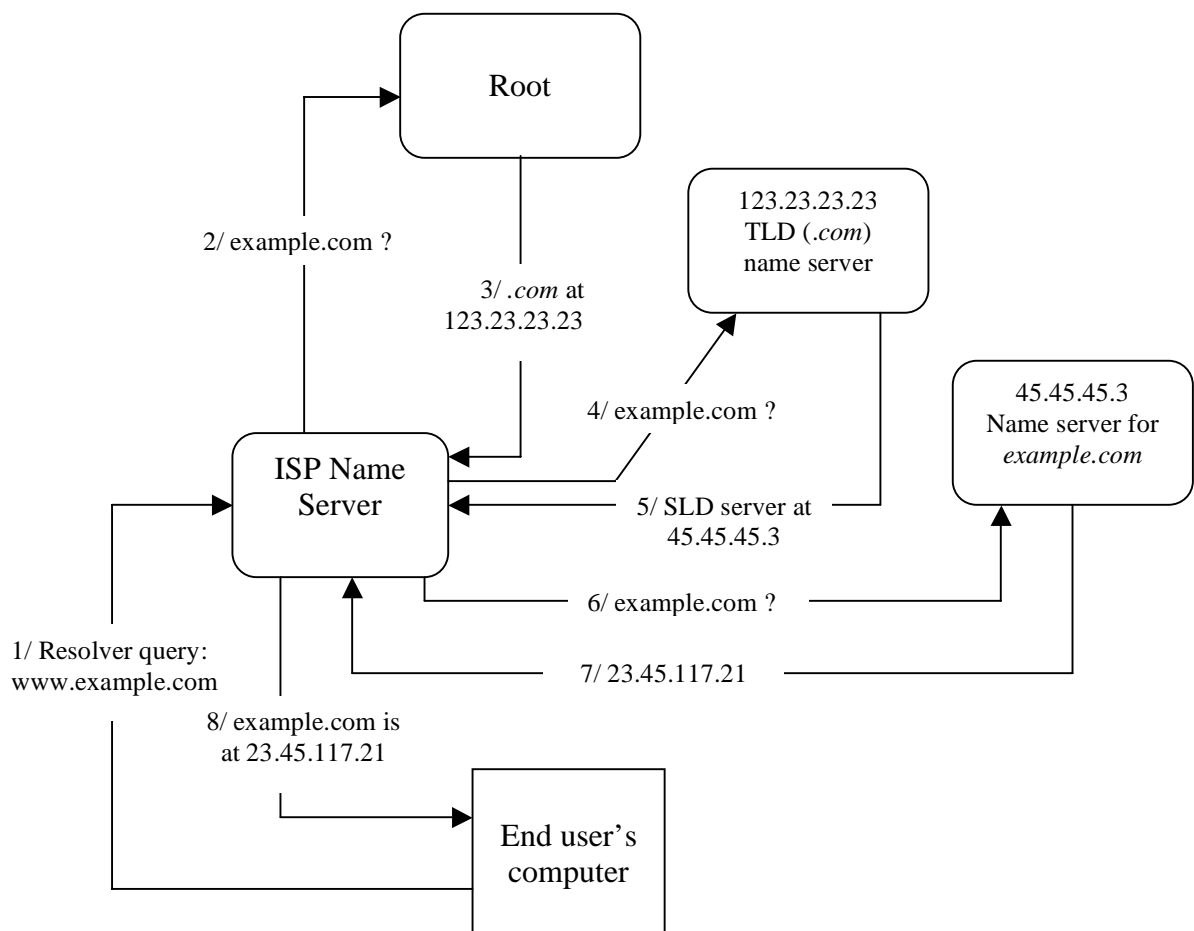


Figure 2: Domain name resolution process of example.com

Adapted from Mueller, 2002a, 46.

³ Another good illustration is provided by Albitz and Liu, 1998. See particularly: http://www.oreilly.com/catalog/dns3/chapter/dns3_0212.gif (last accessed March 17, 2005)

In spite of the reference to “the root”, it is not a single entity. In fact, the root consists in thirteen root servers, labelled from “A” to “M”, placed in various locations around the world: ten are located in the United States (from A to L), one is in the UK (root server K), another one is in Sweden (root server I), and the last one is in Japan (root server M). The “A” root server is considered to be the authoritative reference. It contains the root file, which “is the list of top-level domain name assignments, with pointers to primary and secondary name servers for each top-level domain name” (Mueller, 2002a, 47). To simplify, the root file is a rough equivalent to the old *hosts.txt* file for the DNS architecture. It lists the assignments of all the TLDs. The other root servers (from B to M) download the root zone file from the A root server. They allow the network to function more rapidly and smoothly and they also provide redundancy to protect the network in case some root servers get disconnected, attacked or crash.

Having set out the technical terms, we examine why control of the root is crucial for sovereign states.

Why the Root Matters

Internet Governance: Controlling the Root

One of the tasks of the WGIG was to define Internet governance. In their report⁴ published in July 2005, Internet governance is defined as “the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet” (WGIG, 2005, 4). The concept of governance is vague and often a catch-phrase to translate different realities. It concerns formal and informal rule-making process and coordination between the different stakeholders - private companies, governments, technical experts and civil-society. For Rosenau and Czempiel, “governance is order plus intentionality” (1992, 5). Building on this definition, Mayer, Rittberger and Zürn assert that

Governance is to be distinguished from anarchy: states and other actors recognize the existence of obligations and feel compelled [...] to honour them by their behaviour. [...] Governance without government is distinguished from government in that the compulsion exerted by the rules is not backed up by the threat or use of physical force (the state wielding the monopoly of violence); instead it is the legitimacy of rules and their underlying norms that make international actors comply [...] (1993, 393)

⁴ http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1660|1661|1662|1663|1664 (last accessed July 16, 2005)

As Paré emphasizes “the scope of the concept of ‘governance’ includes politically charged questions pertaining to who, or what, in the cyber-realm has the right to make authoritative decisions, and on what such authority is based” (2003, 44). The importance of controlling the root, in particular, was stressed in the WGIG Report⁵. Consistent with this, area experts and stakeholders have identified Internet governance as being primarily – if not only – focused on the issue of controlling the root (e.g. Mueller, Paré and Cukier) Given this consensus, this paper will focus its discussion on Internet governance on the control of the root, and more specifically, the DNS. One has to acknowledge that this is a restrictive choice. Nonetheless, the administration of the root is the most complete dimension of the governance of the cyberspace, with the creation of a new international organization (ICANN) charged with the assignment of names and numbers, the involvement of governments and the United Nations into the politics of the Internet and the development of a multi-disciplinary literature on its governance.

What does Controlling the Root Mean?

Controlling the root is controlling the names, numbers and root servers. Controlling the root servers, and in particular the A router is controlling the backbone of the Internet. The root zone file (i.e. the names and the corresponding IP addresses inside the root server) of the A router is a reference for the whole network, whose servers simply copy it. A change to that file will have an effect everywhere, on any machine connected to the Internet. Thus, the entity or government controlling the A router is granted significant control over the root. For

⁵ WGIG Report, 2005, 5

instance, it could in theory delete a country on the Internet by suppressing its ccTLD. This has already happened when the Libyan ccTLD .ly has been disabled for a few days in 2004⁶.

More generally, the entity governing the root controls “the right to define the contents of the root zone file” (Mueller, 2002a, 52). This control over the architecture of the Internet is the most important for Lawrence Lessig. For him, “code is law” (1999, 59-60) and “code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed” (1999, 60).

Controlling the root is also controlling the names and how they are used for domain names. According to Cukier, “the delegation permits it to influence the policies that the registry must follow concerning the appropriate use of words for domain names, which directly impacts freedom of speech and democratic dissent. It also determines the degree to which trademark holders are protected” (2004a, 5). The control over domain names is also control of the name market. It enables the responsible entity to regulate the companies that sell domain names, to ensure free competition among them and the price paid by end users.

Controlling the root finally encompasses controlling the numbers which principally means controlling the allocation of IP addresses and the number of devices that will be able to connect to the Internet. Control over this allocation allows the responsible entity to choose which business to apply for selling the blocs of IP addresses. The control over the allocation of IP addresses also ensures control the openness of the network. Determining the number of devices being able to connect to the Internet will significantly impact innovation and uses. Some activities could be declared “illegal” by the leading entity, hence devices enabling them

⁶ http://www.libyanspider.com/why_libyanet_fell.htm (last accessed June 23, 2005)

would not receive an IP address, thus preventing them to connect to the Internet. Controlling the root is not only controlling who can express oneself on the Internet but it is controlling who does what and how. As Cukier put it “The ability to preserve network openness affects democratic values of free expression; control of IP addresses could otherwise provide power over who may participate online” (2004a, 5).

The control of the root and of its architecture will determine who can express oneself on the Internet: As demonstrated by Lybian case, dozens of websites have been rendered inaccessible because a simple decision of ICANN, a private entity, to suspend the .ly. The same could happen to other countries with enormous impact on their economy and security.

The Need to Coordinate: The Risk of Alternative Roots

Some, of the Internet community, have tried to set up an alternative root because they were unsatisfied with the uses and architecture of the ‘official’ one. A number of stakeholders have for instance expressed their frustration that so few gTLDs exist.⁷ There are currently 10 gTLDs officially recognized by ICANN.⁸ Some members of the Internet community have soon expressed their desire to extend the number of TLDs. Some alternative roots such as Pacific Root, OpenNIC or New.net still exist and operate their own domain names, sometimes in direct competition with the root operated by ICANN, creating a possibility of redundancy of domain names. For instance, Pacific Root and ICANN both manage the TLD .biz. As a result, there are .biz domain names that exist in different roots and point to different IP

⁷ According to some observers, the main reason for this artificial scarcity lies in the fact that ICANN is more concerned with the interests of IPRs holders.

⁸ For a full list of the gTLDs recognize by ICANN: <http://icann.org/registrars/accredited-list.html> (last accessed July 31, 2005).

addresses. This could create major conflicts. A Tasmanian man had, for example, registered “Microsoft.biz” in 2001 under Pacific Root⁹ whereas this domain name points to “Microsoft.com” under ICANN supervision. This can lead to confusion as certain users could point to the “wrong” website if their Internet Service Provider (ISP)¹⁰ refers to the “dissident root”. Likewise, certain emails sent to email addresses ending by ‘@microsoft.biz’ may not reach the right person. This risk is very small since most of the servers point to the ‘official’ root but the risk posed by an alternative root still remains, questioning the reliability of the whole system. Herein lies the main criticism against an alternative root, which does not currently appear to be an effective solution.

Controlling the Root: A Component of Sovereignty

As mentioned above, controlling the root implies a control of the ccTLDs, increasingly perceived by many countries as a component of their sovereignty. Their attitude towards controlling the root was transformed from “benign neglect” to a constantly growing interest and participation. This shift has been motivated by a realization that the Internet and its evolution are not politically neutral, and that important choices have to be made in administering it (Lessig, 1999). For instance, the ccTLDs have gained a more and more political significance, becoming both practically and symbolically an important component of sovereignty, defined by the Stanford Encyclopedia of Philosophy as the “supreme authority within a territory”.¹¹ Supreme authority implies that governments should have the ultimate

⁹ <http://archive.humbug.org.au/aussie-isp/2001-05/msg00303.html> (last accessed July 18, 2005)

¹⁰ A company that enables end users to access the Internet generally in exchange of a subscription fee such as AOL or EarthLink.

¹¹ See <http://plato.stanford.edu/entries/sovereignty/> (last accessed July 18, 2005)

decision-making power regarding the administration of their ccTLD, this ccTLD defining the DNS zone that constitutes the territory in which they are sovereign. As Mueller explains:

Just as the physical world was divided up into mutually exclusive territories controlled by sovereign governments, so could the name space be. Country codes were the most direct and obvious point of entry for this kind of thinking. If national governments could gain control over the assignment of their own country code, they could translate their geographic jurisdictions into cyberspaces and gain a significant role for themselves in Internet governance. (2002a, 205)

Cukier agrees stating that “ for countries, the two-letter address suffix represents a valuable national resource that must be operated as a natural monopoly in the public interest [...] territories are starting to recognize it as a component of their sovereignty and a vital national interest. [...] it reflects the “brand” of a country” (2003, 1).

The history of the management of the ccTLDs¹² is a good illustration of the general trends of Internet governance over the last years. In the early days of the ccTLDs, governments were holding back and manifesting little interest in the management of these top-level domains. Gradually though, as the Internet grew becoming global and more and more commercial, they realized that the political dimension these new technologies were bringing could not be ignored. They understood that it was not suitable for the private sector and the technical community alone to run and manage the Internet. State security could potentially be threatened if Internet’s functioning was disrupted. The Internet quickly became a system “whose incapacity or destruction would have a debilitating impact on the defence or economic

¹² For a detailed account, refer to Van Arx and Hagen, 2002

security of a nation” (Van Arx and Hagen, 2002, 12). A mismanagement of the DNS, the resulting unreliability of the network with the risk of interception of data by illegitimate recipients due to the presence of alternative roots or the control by only a foreign country of the quasi-whole infrastructure became critical to many states, which asked for an American disengagement and for the right to have a say in the way the DNS was administered.

History of the Root and of its Governance: From an Epistemic Community to a New International Regime

International Regimes and Multiple Stakeholders: The Need to Coordinate

As it has been previously argued, coordination and rules are becoming essential for the root to function properly. The risks posed by alternative roots and non-coordination could result in instability and unreliability of the Internet as a whole. Keohane and Nye echo the need to coordinate by suggesting that “rules require authority, whether in the form of public government or private or community governance. Classic issues of politics – who governs, on what terms? Who benefits? – are as relevant to cyberspace as to traditionally physical space.” (2002, 216). If classic issues of international politics are relevant to the governance of cyberspace, classic tools of international politics can be used to describe its evolution and explain its nature. Our analysis will predominantly draw upon international regime theory reflecting the role played by the different stakeholders to attain an efficient level of coordination in the management of the root. An international regime is classically defined as “implicit or explicit principles, norms, rules and decision-making procedures around which actors’ expectations converge in a given area of international relations” (Krasner, 1983, 2).

The following part of this paper will apply tools from international relations theories to explain the historical evolution of Internet governance. This analysis will show how a new international regime has been created with its embodiment in ICANN, an international organization of a new kind where governments are not the decision makers. It will also show how the control of the root has shifted from an epistemic community of technical experts funded by the American government to a heterogeneous civil society. After the terrorist

attacks of September 11, 2001, the American policy has moved to a more proactive approach towards the management of the root, claiming its ultimate control of the A root server.

The Epistemic Community of the “Founding Fathers”

The Internet originates from a 1969 project of the American Department of Defence (DoD) called ARPANET.¹³ The Defence Advanced Research Projects Agency (DARPA), a part of the DoD, developed the programme as an experiment to send information divided into data packets between different locations inside a network. It was an immediate success. Internet and TCP/IP were born.¹⁴ Perhaps equally importantly, “the project [ARPANET] did [...] bring together the people who played a continuous role in the Internet’s technical development and its governance for the next 30 years. ARPANET created the nucleus of an Internet technical community” (Mueller, 2002a, 74). This technical community was similar to what Peter Haas has defined as an epistemic community:

Networks of knowledge-based communities with an authoritative claim to policy-relevant knowledge within their domain of experts. Their members share knowledge about the causation of social or physical phenomena in an area for which they have a reputation of competence, and common set of normative beliefs about what actions will benefit human welfare in such a domain (1995, 179).

The conditions for formulation of such an epistemic community were ripe in the US. As Peter Haas once put it “epistemic communities are likely to be found in substantive issues where

¹³ For a full story see <http://www.isoc.org/internet/history/brief.shtml> (last accessed July 28, 2005)

¹⁴ See the website of the National Museum of American history: <http://smithsonian.yahoo.com/arpamet2.html> (last accessed July 11, 2005)

scientific disciplines have been applied to policy-oriented work and in countries with well-established institutional capacities for administration of sciences and technology” (Haas, 1995, 187). It applies perfectly to the ARPANET project, a scientific project designed to create strategic infrastructure capable of resisting a nuclear attack and to the United States, one of the very first countries with “capacities for administration of sciences and technology.”

Secondly, the Internet community formed around the ARPANET possessed a common background and understanding of their objectives. This is an essential characteristic of an epistemic community: “Members of such a[n] [epistemic] community share a common understanding of particular problems in their field of research as well as an awareness of, and a preference for, a set of technical solutions to these problems” (Hasenclever and al., 1996, 209). The technical community formed around the ARPANET pioneers was undeniably an epistemic one. They were technicians and wanted to remain as such. Their objective was to avoid the politicization of the Internet in favour of a free and open network.

In essence, the technical community formed around the creators of the Internet had all the characteristics of an epistemic community¹⁵: “principled beliefs”¹⁶ in a free, open and non-politicized Internet¹⁷; “causal beliefs” on the effects of certain actions on the network such as the undesirability of alternative competing roots; and a “shared notion of validity” i.e. “criteria for weighing and validating knowledge” through open discussion, online experiment and peer reviews.¹⁸ Finally a “common policy enterprise” was embodied by the IETF

¹⁵ See Haas, 1992, 3 for the set of characteristics defining epistemic communities.

¹⁶ *ibid.*

¹⁷ The shared set of normative beliefs is embodied for instance in Barlow’s *Declaration of Independence of the Cyberspace*: <http://homes.eff.org/~barlow/Declaration-Final.html> (last accessed February 12, 2004). It reflects for most part what the members of the epistemic community believe in.

¹⁸ The technical community is used to gathering several times a year under a forum called the Internet Engineering Task Force (IETF) where every one discusses technical solutions for improving the functioning of the Internet or solving problems. One of the main features of this forum is its openness and the “rough” consensus way of deciding which technical solutions will become standards.

meetings where problems are put on the table in front of everyone willing to participate and debated freely among participants until “rough consensus”¹⁹ is reached.

This epistemic community has administered the Internet and governed the root until 1995. It has laid the grounds for the emergence of a new international regime, thereby changing the terms of relations between the epistemic community and the state system. As Haufler points out the “relationship between states and non-state actors may be reversed. Private sector actors may construct independent international regimes or play a relatively equal role with states within a regime of mixed ‘parentage’” (1993, 95). In fact, the technical community was not alone in governance of the root. There is little doubt that the United States acted along the epistemic community for the establishment of the international regime for the governance of the root. It was a regime of clearly a “mixed parentage”.

Epistemic Community in the Foreground, the United States in the Background: A New International Regime in Between

As mentioned earlier, to cope with the problems resulting from the exponential growth of the Internet, the *hosts.txt* file was replaced by the DNS hierarchical system, still used today. This transition followed all the rules of the epistemic community. A community-wide agreement appeared quickly on the shape of the future system, and in particular its hierarchical nature, to solve the shortages of *hosts.txt*.²⁰ These causal beliefs led to the formulation of different projects from eminent members of the community. Since the IETF was not born yet, the distribution of the different proposals to replace *hosts.txt* was decentralized and open to everyone interested. Mills (1981), Postel (1979), Su (1982) and Postel and Su (1982)

¹⁹ The motto of the epistemic community is perfectly summed-up by Zittrain and Clark (1997): “We reject: kings, presidents and voting. We believe in rough consensus and running code.”

²⁰ Paré, 2003, 14 and Mockapetris, 1987, RFC 1034

proposed different version of the current DNS. After peer reviews and a rough consensus from the community around RFC 819, certain members like Mockapetris (1983a, 1983b) began to write more detailed specification and implementation software (Mueller, 2002a, 76), continuing the work and ideas of Su, Postel and others with the same values of transparency, discussion and peer review.

In October 1984, RFC 920 was released specifying the norms regarding the assignment of responsibility for the administration of TLDs. The document gave a list of the six first gTLDs created²¹ and acknowledged the use of the list ISO 3166-1 for the definition of ccTLDs. RFC 920 also stressed the concept of hierarchical delegation of responsibility among organizations. Hence, the organization managing a TLD had to delegate the administration of second-level domain names for its TLD to another organization. In terms of responsibility, DARPA was the initial administrator of .arpa, .gov, .edu, .com and .org. The Defence Data Network (DDN) was administrating the .mil reserved for the American government's military use only.

This approach by the United States government would remain a constant in its relation towards the control of the root: no direct intervention but use of contractual relations with the epistemic community first and with private companies later for daily maintenance of the root. The American government wanted to reduce its visibility in managing the root to appeal to the epistemic community and to other nations in order to rally everyone around its policies. The American government, at the origin of the Internet, has been and still remains the unchallenged hegemon. Ten out of the thirteen root servers are located in the United States, six of them are administered by the American government through contract or by military agencies. In July 2005, Assistant Commerce Secretary Michael Gallagher stated clearly that

²¹ .arpa, .gov, .edu, .com and .org

the US government was the legitimate administrator of the root²² and that ICANN was only a “technical manager” of the DNS²³. This declaration surprised many observers because the United States used to be very detached from the Internet governance issues and have always stressed their will to let the non-governmental stakeholders take care of the control of the root. This “soft” hegemony has allowed the United States to keep control of the root from its creation to the present time, limiting its exposure to criticism by other stakeholders, be it individuals, companies or states. As Kenneth Waltz put it “ both friends and foes will react as countries always have to threatened or real predominance of one among them: they will work to right the balance.” (2000, 55-56).

For a long time, the American government, like many others, has not grasped the strategic and political importance of the control of the root. The epistemic technical community was developing and improving the Internet at a fast pace, private companies were increasingly involved, and self-regulation seemed the best strategy for the US government. This benign neglect by the American government has allowed substantial freedom to the epistemic community and the private sector to build a new international regime. American behaviour was not unique in terms of formation of a new regime. As Haas points out:

Under conditions of uncertainty, when the international power is concentrated in one state, and when epistemic communities have successfully consolidated influence in the dominant state, then follow-the-leader may be modified in light of the policy beliefs of the epistemic community. The regime would still be created through the intercession

²² See Michael Gallagher’s principles of July, 1,2005 at http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm (last accessed July 18, 2005)

²³ See Michael Gallagher’s presentation of June, 30, 2005 at http://www.ntia.doc.gov/ntiahome/speeches/2005/WCA_06302005_files/frame.htm (last accessed July 18, 2005)

of the hegemon, but its substance would reflect epistemic community consensus.
(1995, 187)

This describes exactly what happened. The epistemic community shaped the governance of the Internet according to its “principled beliefs”. At the same time, the private sector was advancing its own agenda, asking for more formal procedures to defend its interests, such as intellectual property provisions embodied in trademarks and other patented names. These different approaches left the time for the American government to ‘learn’ what was at stake and how to deal with this new set of problems. US strategy of temporary non-interference can be explained using a cognitive approach of international relations (Ruggie, 1982). This approach emphasizes the role of learning in shaping actor’s preferences and policies. Joseph Nye in particular stresses the point that changes in beliefs can induce changes in behaviour: this process is referred as learning (Nye, 1987, 378-382). Internet’s complex and technical environment made it difficult for states to know what their interests are and how to define adequate policies. They are under conditions of uncertainty (Adler and Haas, 1992, 369). Following this idea, Haas argues that epistemic communities can ‘teach’ governments and alter their behaviour (Haas, 1992, 27). Indeed, the US government ‘learned’ from the epistemic community that self-regulation and bottom-up decision making processes emerging from rough consensus among all the stakeholders was preferable to a top-down active hegemonic approach. Until the dramatic events of September 2001 that was the way the new international regime for the ruling of the root was designed. This equilibrium was punctuated by what certain observers such as Geist or Paré have called the “domain name wars” (Geist, 2001; Paré 2003)

The Domain Name Wars

As mentioned earlier, DARPA and DDN were the initial administrators of the first six gTLDs. On January 1985, the DNS was formally launched to replace the obsolete *hosts.txt* file. The United States Defense Communications Agency, replacing DARPA as administrator of the root, gave responsibility for the management of the root to the Information Sciences Institute (ISI) at the University of Southern California where Jon Postel was working. As a result, he became the “numbers czar” (Paré, 2003, 16), administering himself the root and assigning IP numbers at ISI. “His actions regarding the assignment of network numbers, and the moral authority he commanded within the networking community, enabled him to exert a level of control over Internet addressing that was virtually unchallenged prior to the mid-1990s” (ibid). In November 1987, the assignment of IP addresses was transferred from ISI to SRI-NIC. Until his death in 1998, Postel kept the two functions of assigning the numbers used in network protocols²⁴ and diffusing the assigned numbers to other users of the network. In December 1988, Postel created the Internet Assigned Numbers Authority (IANA). This grandiloquent name of “Authority” was a joke made by Postel to describe his work and separate it from the functions of SRI-NIC. IANA has no official status and has never been legally constituted. It is the name of function, rather than an institution.

In 1991, the United States Defense Information System Agency sought to replace SRI-NIC for its management function. The contract was awarded to Government System Inc., a private company which had previously collaborated with the American government. This shift is the first entry of the private sector into the administration of the root and the progressive removal of entities from the education/research sectors such as SRI-NIC. The contract of Government

²⁴ See the official list of ports assignment: <http://www.iana.org/assignments/port-numbers> (last accessed July 21, 2005)

System was nonetheless shortly interrupted and in the spring of 1992, the National Science Foundation (NSF) called for other candidates to administer its huge internetworking backbone, spine of the civilian Internet. The contract was awarded to three companies that were asked to collaborate: Network Solutions Incorporated (NSI) was responsible for the name and number registration services for non-military Internet networks.

The involvement of American federal agencies, notably through NSF, and the entry of private companies into the game “blurred the locus of authority over the root” (Mueller, 2002a, 102). He thus describes:

Building the Internet was now an informal collaboration among three separate but interdependent authority centers: an Internet technical community centred in North America but international in scope; a diverse group of civilian federal government agencies interested in stimulating the construction of a national information infrastructure; and the US Defense Department, which had created the protocols and still held residual authority over name and address administration (2002a, 102-103)

1991 was the year that marked the openness of the Internet to commerce. “Domain names registrations since then have increased at an unprecedented pace from 300 per month in 1992 to [...] over 30 000 per month in late 1995” (ibid, 110). The cost of handling all these registrations was becoming problematic for NSF. The foundation held discussions, set up a panel and came to the conclusion that NSI should “begin charging for .COM domain name registrations, and later charge for name registration in all domains” (InterNIC, 1994). A new market for domain name registration was appearing not only in the US but also in other countries where firms were starting to sell ccTLDs registrations. NSI began charging initial

fees in September 1995. Companies' websites aiming at selling products or advertising the brand quickly became of a strategic importance. Second-level domain names became global identifiers for private firms. Intellectual property rights (IPRs) issues were quickly brought up by businesses and other organization contesting the first come first serve basis on which registration by NSI was operating. The small amount charged for registration was allowing "typo-squatters" to operate easily. These individuals were registering commercial brands or very close names in order to resell them to the firm for a substantive amount of money. "The result was a profusion of litigation pitting the rights of trademark holders against those of domain name holders who had registered names first" (Paré, 2003, 21). Consequently, NSI issued a Domain Dispute Resolution Policy Statement maintaining the first come first serve basis of registration but also protecting IPRs on domain names. Since then, trademark holders became prominent actors in Internet governance and in the assignment of names and numbers.

The profits NSI was making by charging fees for registration of domain names²⁵ and its monopoly were becoming more and more difficult to accept for the technical community and other companies seeking to enter a lucrative market. Postel immediately asked for 150 new TLDs to be created and new registries to administer them. Trademark holders opposed this position, arguing that new TLDs would mean new need to register and secure domain names, litigation and new threats to their IPRs. The debate on the creation of new domain names split the once-unified epistemic community, leading for instance some members to create their alternative root to sell new gTLDs. From then on, the technical community was encompassing more and more members with more and more diverging opinions and the epistemic community of the Internet "founding fathers" passed away.

²⁵ From a net revenue of 5 million USD in 1995 to 94 three years later (NSI, 1998)

In November 1996 an eleven-member panel – the Internet International Ad Hoc Committee (IAHC) – was set up. It comprised representatives from the ITU, the WIPO, the International Trademark Association; five engineers appointed by the technical community; a representative from NSF and an intellectual property lawyer. The IAHC was in a way a surprising alliance between trademark defenders and a large part of the technical community behind Postel. In February 1997, after extensive consultations, the IAHC released its Final Report (IAHC, 1997). Seven new domain names were proposed to be introduced and eight new registrars²⁶ were to be equally spread within seven geographical regions. The report also included a framework for governance called the Memorandum of Understanding of the Generic Top Level Domain Name Space of the Internet Domain Name System (gTLD-MoU). Public and private parties were invited to sign it and ITU was supposed to be the repository (Paré, 2003, 29). The gTLD-MoU was signed in an official ceremony in Geneva organized by the ITU in March 1997. A month later, more than 220 private and public organizations signed the document. While some claimed this number was equivalent to a consensus among the stakeholders, the detractors of the plan were arguing that such a small number was not representative. Except Albania, no government representatives have signed the gTLD-MoU. Many feared that a part of the technical community allied with trademark holders and the ITU were trying to carve a sovereign role for themselves: a world government for the Internet.

The Late Involvement of the American Hegemon: Benign Neglect or Machiavellian Strategy?

In July 1997, despite starting the implementation of the gTLD-MoU, the United States crashed the initiative down. The contract between NSI and NSF was to expire on September 30, 1998 and on July 2, 1997 the NTIA, an agency of the Department of Commerce, was

²⁶ Registrars are companies dealing with the registration of second-level domain names under the new TLDs.

soliciting public comments for the future of the administration and registration of gTLDs. Under the supervision of Ira Magaziner, senior analyst for Internet issues for President Clinton, the DoC reviewed the comments submitted during the summer 1997 and congressional hearings were held in September and October. The result was the release of the Green Paper (without a single mention of the gTLD-MoU!) on January 1998, submitted for public comments. The Green Paper was an assertion by the American government of “its authority over the name and address root but also [an] indicat[ion] [of] its intention to relinquish that authority in a way that involved Internet stakeholders internationally” (Mueller, 2002a, 160). The Green Paper was no more than a privatization plan with the ultimate control in the hands of the US government responsible for handling the transition.

The Clinton administration issued the final plan, the White Paper, on June 3, 1998. It came as a surprise since it was a “Statement of Policy” and did not mention any direct action of the American government. Four main principles were described in the White Paper as guidelines for the management of the DNS: stability as the first priority of any DNS management system: competition, private sector, bottom-up coordination and representation (NTIA, 1998b). These are the principles that will guide the new international regime, the very rules Krasner describes when referring to the main components of a regime (Krasner, 1983, 2).

In the report of the WGIG for the WSIS, the working group states that Internet governance is under “unilateral control by the United States Government”²⁷. While unequal, this control seems nevertheless essential in maintaining the network’s smooth operation. As for Charles Kindleberger and his hegemonic stability theory, a hegemon with an outstanding political and

²⁷ WGIG Report, 2005, 5, paragraph 15.

economic power, with the capacity and willingness to lead, can supply and support the infrastructure that permits international coordination to take place (Kindleberger, 1973).

That is what happened. Built by the American hegemon on grounds laid by the epistemic community of the time, the new international regime was of a “mixed parentage” (Haufler, 1993, 95). The last step in the emergence of the regime was the creation of ICANN, the new organization called for by the White Paper. According to the White Paper, no new TLDs were to be added and no new registries were allowed to challenge NSI’s monopoly. All these decisions were to be made by a new non-profit corporation created to supervise domain name administration and fulfil other technical functions. Private stakeholders were responsible for the spontaneous formation of this organization, located in the United States and incorporated under American law.

At the end of the transition, the American government asserted that it would relinquish all power over the root and put it in the hands of this new institution at the end of 2000. This point has triggered some controversy among the scholars who debated whether the American government was unwilling to assume its hegemony over the root. Some, like Froomkin suggest that this was only rhetoric and that in fact the American government was not willing to give up its powers on the root at all: “whatever authority ICANN holds [...] emanates from, and remains subject to, DoC’s ultimate authority” (2000, 26). Harold Feld described the decision of privatization as a “fiction” (2003, 386). For these authors, privatization was a strategy to gain the confidence of foreign countries and the Internet community. Others scholars such as Cukier or Mueller believe that Ira Magaziner really wanted to give the power to the private sector and that the terrorist attacks of September 2001 have forced the United States to reconsider its position in light of Internet’s importance as a critical infrastructure.

The debate between the two schools still goes on.

ICANN, Flesh of the New Regime

ICANN has generated volumes of literature on its legitimacy, basis of power, and its relations with governments. While it is not our purpose here to discuss ICANN, a few key points will be highlighted regarding the controversies the organizations had to face.

First, its difficulty to attain legitimacy since its establishment has endangered the creation of the institution. To satisfy the American desire of a “privatization” of the DNS, ICANN bylaws²⁸ forbid any government representative to sit on the Board of the organization, instead they are represented by the GAC which only has an advisory role. Private sector and civil society are the effective decision-makers. This is the antithesis of a traditional structure of international organization where states decide and non-state actors advise. This structure is perplexing since the institution’s role is anything but apolitical. While ICANN’s supporters and the American government made it clear that ICANN was only assigned technical tasks of coordination, the new institution was asked to set up a procedure to solve trademark disputes, a very political and sensitive issue. In the same vein, ICANN was to deal with the market of the registration of domain names and assure fair competition, another political issue. Another controversy of ICANN lies in its architecture. It functions by consensus and bottom-up decision process. No formal mechanism or procedure is specified to reach consensus. “This allow[s] the ICANN Board, or ICANN staff, to simply announce consensus and impose it on the community” (Feld, 2003, 388). All these elements have made ICANN very controversial, contentious especially in the eyes of governments and its legitimacy is still questioned.

²⁸ Refer to <http://www.icann.org/general/bylaws.htm> (last accessed August 2, 2005), in particular Article VI, Section 4, Paragraph 1

Another controversy appeared in 2000 around the creation of new gTLDs. The introduction of new TLDs into the root has always been a central point of discussion among the Internet community. During the meeting in Berlin in 1999, ICANN set up two working groups on the introduction of new gTLDs. The conclusion of their debates invited the Board to “establish a policy for the introduction of new gTLDs in a measured and responsible manner.”²⁹ Instead of following these recommendations, ICANN Board members selected the new gTLDs and the organizations to manage them in a single session on November 16, 2000. The record of their conversations clearly shows that the selection was “uncoordinated, subjective and arbitrary” (Paré, 2003, 150).³⁰ This compounded ICANN’s legitimacy crisis and increased the number of its opponents. This happened when ICANN was already criticized for its unilateral decision to prolong the mandate of the non-elected members of the Board and reduce the number of members elected by the membership (Froomkin, 2000).

As mentioned above, the attempt for ccTLD managers to sign contracts with ICANN in 2001 failed. As a result, the new US administration was displeased and required major reforms, which paved way to ICANN’s reorganization of 2002. Following these reforms, the powers of the GAC were substantially increased with the right to propose new policies and send recommendations to any committee of ICANN without prior consultation with other stakeholders. As Feld put it “the veneer of private decision-making is wearing increasingly thin. The new structure provides the GAC with an independent route to developing policy within ICANN [...]” (2003, 399).

Finally, in 2003, the government frustration with the functioning of ICANN (notably among

²⁹ Refer to DNSO Names Council Statement on new gTLDs (April 19, 2000) <http://www.dnsso.org/dnsso/notes/20000419.NCgtds-statement.html> (last accessed August 2, 2005)

³⁰ Available at <http://cyber.law.harvard.edu/icann/la2000/archive/> (last accessed June 25, 2005)

developing countries) led to the WSIS backlash, symbolizing the will of nation-states to place Internet Governance in the hands of the United Nations. At this juncture, it is too soon to predict what ICANN will become and what the WSIS initiative will lead to. It is nonetheless interesting to look at ICANN as a new experiment (Nye, 2002, 167-168), a new kind of international organization where nation-states are not all mighty. If it succeeds in overcoming its legitimacy crisis and bringing governments back into to the negotiating table, it could serve as a model for an innovative way of tackling emerging issues in international relations.

Conclusion

The Internet cross-cuts many of the tier-one issues in international relations: it can be a tool of economic development, it can be used as a basis for expression and democracy, it is certainly linked to security concerns, and finally it is a global network where millions of people can share ideas real-time. Despite the importance of the issues at stake, Internet Governance faces a looming crisis and needs a more precise structure as well as input from a broader set of stakeholders and states, particularly because all countries have an interest in how the Net evolves. As we have seen, the control of the root of the Internet is crucial because it conditions who can express themselves on the Net (for individuals through the control of the gTLDs as well as countries via the control of the ccTLDs), as well as what can be said and where (through the control and the smooth functioning of the resolving process). It also shapes the architecture of the medium, its “law” as Lessig suggested. It defines who will control it (through the imposition of certain proprietary or open norms) and what the standards will be.

Given the importance of controlling the Internet, this paper has investigated how some from international relations tools and theories could be applied to the analysis and understanding of Internet governance defined as the control of the root. It has shown how a new international regime was born. First an epistemic community at the origin of the Internet has laid the grounds for the new regime to emerge. The community has defined rules, principles and practices that endured till this day. The prominence of non-state actors in the decision-making processes, the withdrawal of politicians and games of power in favour of pragmatic solutions, the reliance on men rather than law and bureaucratic red-tape, wide consultation and rough consensus, are still main components of Internet governance. Under the American discretion,

the regime was solidified with the creation of ICANN in 1997. Though the Americans have promised to surrender their prerogatives over the root to ICANN, they have dragged their feet (voluntarily or not, the debate is open) and have finally changed their position since 9/11 attacks, realizing their interest in maintaining the smooth functioning of this critical infrastructure.

So far, three main scenarios can be advanced on how Internet Governance and the newborn international regime may evolve. The first one is a return to the old politics of international treaties where sovereign states define norms and conventions through an international agreement anchored in the United Nations. In this scenario, civil society and private sector are conferred an advisory role only. There is little doubt that the United States would be able to take the lead in the WTO-like negotiation of the treaties and fully exert their hegemonic power. With control of the root servers and the most up-to-date expertise on the issue, the United States is virtually unchallenged. Though the DoC would lose most of its prerogatives over the control of the DNS, it would be able to reintegrate his powers into international treaties which are international law, thus acquiring more legitimate power over the root. Only an alliance of the European Commission and major developing countries like China or Brazil could counterweight the American influence in these debates. Developing countries would certainly lack resources and expertise to play a significant role and likely would end up being imposed treaties. In this scenario, ICANN has no more reason to exist and would be dissolved or delegated minor and technical tasks. The death of ICANN would also mean a radical change of the international regime which would become “traditional” and based on a set of international treaties.

The second scenario, on the contrary, would give more power to ICANN. Governments could acquire a real decision-making power to address issues of concern, but private business and civil society would also be entitled to the same powers. The three poles of this iron triangle

would be given equal weight. An alliance of developed countries with the private sector would be necessary for them to defend their interests. In such a scenario the United States would certainly lose its current extent of power over the root. The functions previously under DoC's responsibility would indeed be transferred completely to ICANN. Moreover, a coalition of the European Commission with major companies and NGOs could easily prove more powerful than the U.S. alone. Developing countries could seek the help of NGOs to defend their interests, with some chance of success if they coalesce. The international regime would push the experimentation further and could, in case of success, serve as an example on how to address new issues.

The last scenario consists of a pure exercise of the American hegemony over the root. The Bush Administration argues that the attacks of September 11, 2001 have changed the landscape of Internet governance. He further claims that the Internet is a critical infrastructure and its management should not be under the influence of non-democratic states via participation in a multilateral forum. Besides, since the Internet needs stability, the control by the US government is seen as the best way to achieve it. In this scenario, ICANN would remain a subcontractor of the DoC and give non-binding recommendations. Other countries, both developed and developing, may feel frustrated of this hegemony and respond by threatening or effectively implementing alternative roots, assuming the risks mentioned above. This scenario could lead to a split of the Internet into disconnected networks with little compatibility. As Cukier describes:

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 (2004b, 3).

Here, the international regime formed around the issue of Internet governance would simply disappear to the benefit of American hegemony.

These future scenarios highlight that Internet governance is still in experimentation and nobody can really foretell towards which scenario the situation will evolve. New actors are given power and sovereign states are fighting to stay afloat in these fast-moving debates. International relation scholars should carefully observe these recent and future developments. As some observers have noted, a new law of the sea is being written with the Internet in role of the oceans. It has taken four hundred years to write the law of the sea. The "law" of Internet Governance would probably emerge more rapidly, in an unprecedented form and with unprecedented outcomes. Everything is still to come.

Glossary

(Adapted from the WGIG Report)

ccTLD	Country code top-level domain, such as .uk (United Kingdom), .de (Germany) or .jp (Japan)
DNS	Domain name system: translates domain names into IP addresses
GAC	Governmental Advisory Committee (to ICANN)
gTLD	Generic top-level domain, such as .com, .int, .net, .org, .info
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communication technology
IETF	Internet Engineering Task Force
IGOs	Intergovernmental organizations
IP	Internet Protocol
IP Address	Internet Protocol address: a unique identifier corresponding to each computer or device on an IP network. Currently there are two types of IP addresses in active use. IP version 4 (IPv4) and IP version 6 (IPv6). IPv4 (which uses 32 bit numbers) has been used since 1983 and is still the most commonly used version. Deployment of the IPv6 protocol began in 1999. IPv6 addresses are 128-bit numbers.
IPRs	Intellectual property rights
ITU	International Telecommunication Union
Registrar	A body approved ("accredited") by a registry to sell/register domain names on its behalf.
Registry	A registry is a company or organization that maintains a centralized registry database for the TLDs or for IP address blocks (e.g. the RIRs — see below). Some registries operate without registrars at all and some operate with registrars but also allow direct registrations via the registry.
RIRs	Regional Internet registries. These not-for-profit organizations are responsible for distributing IP addresses on a regional level to Internet service providers and local registries.
Root servers	Servers that contain pointers to the authoritative name servers for all TLDs. In addition to the “original” 13 root servers carrying the IANA managed root zone file, there are now large number of Anycast servers that provide identical information and which have been deployed worldwide by some of the original 12 operators.

Root zone file	Master file containing pointers to name servers for all TLDs
RFC	Request for Comment. The Requests for Comments document series is a set of technical and organizational notes about the Internet open for comments to everyone.
TLD	Top-level domain (see also ccTLD and gTLD)
WIPO	World Intellectual Property Organization
WGIG	Working Group on Internet Governance
WHOIS	WHOIS is a transaction oriented query/response protocol that is widely used to provide information services to Internet users. While originally used by most (but not all) TLD Registry operators to provide “white pages” services and information about registered domain names, current deployments cover a much broader range of information services, including RIR WHOIS look-ups for IP address allocation information.
WSIS	World Summit on Information Society
WTO	World Trade Organization

Bibliography

Adler E. and P.M. Haas 'Conclusion: epistemic communities, world order, and the creation of a reflective research program', International Organization 46(1992): 367-390.

Albitz P. and C. Liu. DNS and BIND. O'reilly & Associates Inc. September 1998.

Alhert C. Research fellow at the Oxford Internet Institute. Personal interview in London (July 24, 2005).

Benhamou, B. Senior advisor to the French Prime Minister for Internet governance issues. Personal interviews in San Francisco (March 23, 2003), Paris (January 20, 2004; April 3, 2004 and September 16, 2004) and London (April 3, 2005 and July 23, 2005).

Brown, I. Professor at the Computer Science Department, University of College London. Personal interviews in London (July 21 and 24, 2005).

Cristal L.E. and N.S. Greenfield Trademark Law and the Internet, New York: International Trademark Association, 2002.

Cukier, K.N. Research fellow at the National Center for Digital Government at Harvard University's Kennedy School of Government. Personal interview in London (July, 28, 2003).

Cukier, K.N. 'Eminent Domain: Initial Policy Perspectives on Nationalizing Country-Code Internet Addresses'. Cardozo School of Law, Yeshiva University, New York, March 2003. Last accessed July 24, 2005 <http://www.cukier.com/inet02.html>

Cukier, K.N. 'Internet Governance, National Interest and International Relations.' Background paper for the United Nations ICT Task Force Meeting in NY, 24-26 March 2004a. Last accessed July 2, 2005 <http://www.cukier.com/writings/cukier-UNnetgov-mar04.html>.

Cukier K.N. 'Multilateral Control of Internet Infrastructure and its Impact on US Sovereignty'. Paper (draft) for the Telecommunications Policy and Research Conference, Washington, DC. October 2004b. Last accessed July 5, 2005 <http://www.cukier.com/writings/cukier-netgov-TPRC04.pdf>.

Cukier K.N. 'Internet Governance: What? How? Who?' Remarks presented at the ITU Workshop on Internet Governance. Geneva. 26 February 2004c. Last accessed June 23, 2005 <http://www.cukier.com/writings/ITU-Feb04.html>

Cukier K.N. 'And the Answer to Internet Governance is...' Remarks at the Oxford Internet Institute; Oxford. 5 May 2005. Last accessed August 2, 2005 <http://www.cukier.com/writings/oii-remarks-may05.html>

Cukier K.N. and A. Selian. 'The World vs. The Web: The UN's Politicization of the Information Society.' Conference report of the UN World Summit on the Information Society. Geneva. December 2003. Last accessed June 3, 2005 <http://www.cukier.com/writings/wsis-itid-july04.html>

Doyle M.W. and G.J. Ikenberry. New Thinking in International Relations Theory. Boulder, Colorado: Westview Press, 1997.

Edelman, B. 'DNS as a Search Engine: A Quantitative Evaluation', July 2002. Last accessed July 25, 2005 <http://cyber.law.harvard.edu/people/edelman/DNS-as-search/>.

Feld H. 'Structured to fail: ICANN and the "Privatization" Experiment' in Thierer A. and C. W. Crews Jr. Who rules the Net? Internet Governance and Jurisdiction Washington, D.C: Cato Institute, 2003: 369-414.

Froomkin M. 'Is ICANN's New Generation of Internet Domain Name Selection Process Thwarting Competition?' Speech before the U.S. House of Representatives, Committee on Energy & Commerce, February 8, 2001. Last accessed August 25, 2005 <http://osaka.law.miami.edu/~froomkin/articles/commerce8Jan2001.htm>.

Froomkin M. 'Beware the ICANN Board Squatters'. October 27, 2000a. Last accessed July 18, 2005 <http://personal.law.miami.edu/~froomkin/boardsquat.htm>

Froomkin M. 'Of Governments and Governance.' Berkeley Law & Technology Journal 617 (1999). Last accessed May 23, 2005 www.law.miami.edu/~froomkin/articles/governance.htm

Froomkin M. 'Wrong turn in cyberspace: Using ICANN to route around the APA and the constitution.'" Duke Law Journal 50 (2000b): 17-184. Last accessed June 3, 2005 <http://osaka.law.miami.edu/~froomkin/articles/icann.pdf>

Geist M. 'Fair.com? An examination of the allegations of systemic unfairness in the ICANN UDRP'. University of Ottawa, Faculty of Law. 2001. Last accessed June 12, 2005 <http://aix1.uottawa.ca/~geist/geistudrp.pdf>.

Goldsmith J.L. 'Against Cyberanarchy' in Thierer A. and C. W. Crews Jr. Who rules the net? Washington, D.C: Cato Institute, 2003: 15-82.

Goldsmith J.L. 'The Internet, Conflicts of Regulation, and International Harmonization' in Engel C. and K.H. Keller (ed.) Governance in the Light of Differing Local Values (Law and Economics of International Telecommunications) Baden-Baden: Nomos. 2000.

Grewlich K.W. Governance in "Cyberspace": Access and Public Interest in Global Communication. The Hague: Kluwer Press, 1999.

Haufler V. 'Crossing the Boundaries Between Public and Private: International Regimes and Non-State Actors.' in Rittberger V. (ed.) Regime Theory and International Relations. Oxford: Clarendon Press, 1995: 94-111.

Haas P. M. 'Do Regimes Matter? Epistemic Communities and Mediterranean Pollution Control.' International Organization, 43 (1989): 376-403.

Haas P.M. 'Introduction: epistemic communities and international policy coordination'. International Organization. 46 (1992): 1-35.

Haas P. M. 'Epistemic Communities and the Dynamics of International Environmental Cooperation.' in Rittberger, V. (ed.) Regime Theory and International Relations. Oxford: Clarendon Press, 1995:168-202.

Hasenclever A., Mayer P. and V. Rittberger, 'Interests, Power, Knowledge: The Study of International Regimes.' International Studies Review, 40 (1996): 177-228.

Hurrell A. 'International Society and The Study of Regimes: A Reflective Approach.' in Rittberger V. (ed.) Regime Theory and International Relations. Oxford: Clarendon Press, 1995:49-72.

International Chamber of Commerce, 'Issues Paper on Internet governance', January 2004. Last Accessed June 25, 2005

http://www.iccwbo.org/home/e_business/policy/ICC%20issues%20paper%20on%20Internet%20Governance.pdf.

Internet Ad-Hoc Committee. 'Final Report of the International Ad Hoc Committee: Recommendations for Administration and Management of gTLDs'. 1997. Last accessed June 3, 2005 <http://www.iahc.org/draft-iahc-recommend-00.html>

Internet Governance Project, 'Internet Governance: Quo Vadis? A Reponse to the WGIG Report.' July 2005. Last accessed July 15, 2005

<http://www.state.gov/documents/organization/50550.pdf>.

InterNIC. 'Midterm Evaluation and Recommendations: A Panel Report to the National Science Foundation'. December 1994. Last accessed April 18, 2003

http://www.networksolutions.com/en_US/legal/internic/midterm/index.html

Kamarck E.C. and J. S. Nye. Democracy.com? Governance in a Networked World. Hollis: Hollis Publishing Company, 1999.

Keohane R.O. After Hegemony: Cooperation And Discord In The World Political Economy. Princeton: Princeton University Press. 2005.

Keohane R.O. and J.S. Nye. Power and Interdependence. New York, London: Longman, 2001.

Kleinwächter W. 'WSIS: A New Diplomacy? Multistakeholder Approach and Bottom Up Policy in Global ICT Governance'. 2003. Last accessed July 23, 2005

<http://cyber.law.harvard.edu/wsis/Kleinwachter.html>.

Kleinwächter W. 'ICANN as the "United Nations" of the Global Information Society?' Gazette, 62 (2000): 451-475.

Kobrin S. 'Territoriality and the Governance of Cyberspace.' Journal of International Business Studies, Vol. 32, Issue 4, December 2001: 687-704.

Krasner S. 'Structural Causes and Regime Consequences: Regimes as Intervening Variables.' in Krasner S. (ed.) International Regimes, Ithaca: Cornell University Press, 1983: 1-21.

Kratochwil F. and E. D. Mansfield, eds. International Organization: a Reader. New York: HarperCollins College Publishers, 1994.

Kindleberger C. The World in Depression, 1929-1939. Berkeley: University of California Press, 1973.

Lessig L. 'Reading the constitution in cyberspace.' Emoy Law Journal. 45(1996a). Last accessed on May 3, 2005 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=41681

Lessig L. 'The zones of cyberspace.' Stanford Law Review 48(1996b): 1403-1411.

Lessig L. 'A bad turn for Net governance.' The Industry Standard September 18, 1998. Last accessed July 3, 2005 <http://www.lessig.org/content/is/0,1902,1718,00-2.html>

Lessig L. Code and Other Laws of Cyberspace. New York: Basic Books, 1999.

Loshin P. Tcp/Ip Clearly Explained. 2nd ed. Amsterdam ; Boston: Morgan Kaufmann, 1997.

Mathiason J. R. and C.C. Khulman. 'International Public Regulation of the Internet: Who Will Give You Your Domain Name?' Panel on 'Cyberhype or the Deterritorialization of Politics in the Internet in a Post-Westphalian Order', 1998. Last Accessed July 2, 2005 <http://www.intlmgt.com/domain.html>

Mathiason J., Mueller M., Klein H., Holitscher M. and L. McKnight . 'Internet Governance: The State of Play'. Report commissioned by the UN ICT Task Force, September 2004. Last accessed June 30, 2005 <http://dcc.syr.edu/miscarticles/MainReport-final.pdf>

Mayer P., Rittberger V. and M. Zürn. 'Regime Theory: State of Art and Perspectives.' in Rittberger, V. (ed.) Regime Theory and International Relations. Oxford: Clarendon Press, 1995: 391-430.

Mansell R. Inside the Communication Revolution: Evolving Patterns of Social and Technical Interaction. Oxford: Oxford University Press, 2002.

Marsden C. Regulating the Global Information Society. London: Routledge, 2003.

Mattelart A. The Information Society: an Introduction. London: Sage, 2003.

Mills D.L. 'Internet name domains', RFC 799. 1981. Last accessed July 23, 2005 <http://www.faqs.org/rfcs/rfc799.html>

Mockapetris P. 'Domain names – Concepts and Facilities', RFC 882. 1983a. Last accessed July 23, 2005 <http://www.faqs.org/rfcs/rfc882.html>

Mockapetris P. 'Domain names: implementation and specification', RFC 883. 1983b. Last accessed July 23, 2005 <http://www.faqs.org/rfcs/rfc883.html>

Mockapetris P. 'Domain names – Concepts and Facilities', RFC 1034. 1987. Last accessed July 23, 2005 <http://www.faqs.org/rfcs/rfc1034.html>

Mockapetris P. 'ICANN and Internet Governance: Sorting through the Debris of "Self-Regulation"'. Info. 1(1999): 477-500.

Morgenthau H. J. (revised by K. W. Thompson). Politics Among Nations: the Struggle for Power and Peace. New York: McGraw-Hill, 1993.

Mugabe R. '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.

Mueller M. Ruling the Root: Internet Governance and the Taming of Cyberspace. London: MIT Press, 2002a.

Mueller M. 'Dancing the Quango: ICANN as International Regulatory Regime', presented at the Johns Hopkins SAIS/George Mason University on Technology and Global Governance, February 11-12, 2002b. Last accessed June 24, 2005
<http://istweb.syr.edu/~mueller/quango.pdf>

Mueller M. 'Success by Default: A New Profile of Domain Name Trademark Disputes Under ICANN's UDRP.' Internet Governance Project, Syracuse University, The Convergence Center, 2002c.

Mueller M. 'Toward an Economics of the Domain Name System', Syracuse University School of Information Studies, 2004. Last accessed June 25, 2005
<http://dcc.syr.edu/miscarticles/dns-econ.pdf>

Mueller M. and L. W. McKnight. 'The Post-.COM Internet: Toward Regular and Objective Procedures for Internet Governance' Paper prepared for presentation at: TPRC 2003, the 31st Research Conference on Communication, Information, and Internet Policy Arlington, VA, Sept. 19-21, 2003. Last accessed June 1, 2005 <http://dcc.syr.edu/miscarticles/NewTLDs2-MM-LM.pdf>

Mueller M., Mathiason J.R. and L.W. McKnight. 'Making Sense of Internet Governance: Defining Principles and Norms in a Policy Context.' Internet Governance Project, Syracuse University, The Convergence Center 2004.

National Telecommunications and Information Agency. U.S. Department of Commerce. Improvement of Technical Management of Internet Names and Addresses. Green paper. Federal Register. 62(1998a): 8825. Last accessed July 23, 2005
<http://www.ntia.doc.gov/ntiahome/domainname/dnsdrft.htm>

National Telecommunications and Information Agency. U.S. Department of Commerce. Management of Internet Names and Addresses. White paper. Federal Register. 62(1998a): 31741. Last accessed July 23, 2005
http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm

Nye, J.S. 'Nuclear Learning and U.S. – Soviet Security Regimes.' International Organization. 41 (1987): 371-402.

Nye J.S. The Paradox of American power: Why the World's Only Superpower Can't Go It Alone. New York: Oxford University Press, 2002.

Paré, D.J. Internet Governance in Transition: Who Is the Master of This Domain? Oxford: Rowman & Littlefield, 2003.

Post D. 'Against "Against Cyberanarchy"' in Thierer A. and C. W. Crews Jr. Who rules the net? Washington, DC: Cato Institute, 2003: 83-112.

Postel J. 'IEN 116: Internet name server', IEN 116. 1979. Last accessed July 23, 2005 <http://rfc.slim.summitmedia.co.uk/ien116.html>

Prodromos T., Hosein I. and E.A. Whitley. 'The Footprint of Regulation: How information systems are affecting the sources of control in a global economy'. In Poulymenakou A. and al. (ed) IS Perspectives and Challenges in the Context of Globalization. The Hague: Kluwer Press. 2003: 355-370.

Rony E. and P. Rony. The Domain Name Handbook: High Stakes & Strategies in Cyberspace. Gilroy: RD Book, 1998.

Rosenau, J.N. and E.O. Czempiel, eds. Governance Without Government: Order and Change in World Politics. Cambridge: Cambridge University Press, 1992.

Roy J. 'E-governance and International Relations: a consideration of newly emerging capacities in a multi-level world.' Journal of Electronic Commerce Research 6(2005): 44-55. Last accessed June 3, 2005 <http://www.csulb.edu/web/journals/jecr/issues/20051/paper3.pdf>

Ruggie J.G. 'International Regimes, transactions, and change: embedded liberalism in the postwar economic order'. International Organization 36 (1982): 379-415.

Schlesinger Wass, E. Addressing the World: National Identity and Internet Country Code Domains. Lanham, MD: Rowman & Littlefield, 2003.

Shaw M. Global Society and International Relations: Sociological Concepts and Political Perspectives. Cambridge, UK: Polity Press, 1994.

Spinello R.A. Cyberethics: Morality and Law in Cyberspace. Boston: Jones and Bartlett, 2000.

Su, Z. 'A distributed system for Internet name service', RFC 830. 1982. Last accessed July 23, 2005 <http://www.faqs.org/rfcs/rfc830.html>

Su Z. and J. Postel. 'The Domain Naming Convention for Internet User Applications', RFC 819. 1982. Last accessed July 23, 2005 <http://www.faqs.org/rfcs/rfc819.html>

Swiss T. Unspun: Key Concepts for Understanding the World Wide Web. New York: New York University Press, 2001.

Thierer A.D., Crews C.W. et al. Who rules the Net? Internet Governance and Jurisdiction. Washington: Cato Institute, 2003.

U.S. National Research Council, Committee on the Internet in the Evolving Information Infrastructure. The Internet's Coming of Age. Washington: National Academy Press, 2001.

Von Arx K. and G.R. Hagen. 'Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control.' Richmond Journal of Law and Technology. 4 (2002). Last accessed June 14, 2005 <http://law.richmond.edu/jolt/v9i1/article4.html>

Working Group on Internet Governance, Report of the Working Group on Internet Last accessed June 14, 2005 <http://www.wgig.org/docs/WGIGREPORT.pdf>

Young, O.R. and G. Osherenko 'Testing Theories of Regime formation: Findings from a Large Collaborative Research Project' in Rittberger V. (ed.) Regime Theory and International Relations. Oxford: Clarendon Press, 1995: 223-252.