

University of Westminster

# Efforts to Internationalise Domain Name System Control

by

M. Salim KETEVANLIOĞLU

A Dissertation Submitted to the  
University of Westminster

In Partial Fulfilment of the Requirements  
for the Award of the Degree of  
MA in Communications Policy

London, August 2007

## **Abstract**

Internet is being used more widespread in our daily life day by day. It is used by individuals, corporations and governments for vital transactions. However its governance is not internationalised as itself did. Now governments concern about not being involved in the management process of the thing that is used in most of the daily life.

Governments defend that international network should be governed by an international institute. But Internet domain names are under US control historically. And US enjoying this control does not seem to delegate any control to an international body.

The debate on domain name issues keep going on the international platforms like United Nations' International Telecommunications Union. There had been several summits and meeting about this issue but except small concessions, like advisory role, US preserves status quo.

## Table of Contents

Abstract .....	i
Table of Contents .....	ii
Table of Figures .....	iii
1 Introduction .....	1
2 Internet domains .....	3
2.1 Data Communication.....	4
2.2 Resolution of Domain Names .....	5
2.3 The Domain Name System (DNS).....	6
2.4 Structure of DNS .....	7
2.5 The DNS Root.....	9
2.6 Is DNS American? .....	10
2.6.1 Sovereignty.....	10
2.6.2 Property .....	11
2.6.3 Intellectual Property Law .....	11
2.6.4 Patent.....	12
3 Internet Corporation for Assigned Names and Numbers .....	13
3.1 How ICANN was born? .....	13
3.1.1 Jon Postel.....	14
3.1.2 Governance Shift from Research to Commercial .....	14
3.1.3 Controversies.....	17
3.1.4 First Efforts for International Regime .....	17
3.1.5 The Way to Green Paper .....	20
3.1.6 The Green Paper .....	22
3.1.7 The White Paper.....	23
3.2 Formation of ICANN .....	26
3.3 New Regime .....	27
3.4 Problems with ICANN .....	29
3.4.1 Legitimacy.....	30
3.4.2 Technical Coordination or Policy Making .....	31
3.4.3 Transparency .....	32
3.4.4 Democracy .....	33
4 National and International Efforts.....	35
4.1 ITU and Internet .....	36
4.2 World Summit on the Information Society .....	38
4.3 Turkish Government Contributions .....	44
4.4 Governmental Advisory Committee .....	46
4.5 Internationalised Domain Names (IDN) .....	47
4.6 Country Code Top Level Domain (ccTLD).....	47
4.7 National Sovereignty and Balkanizing Internet .....	48
4.8 Solution Proposals.....	51
5 Conclusions .....	53
6 References .....	55

## Table of Figures

Figure 2-1 Resolution of win.ac.uk on the Internet .....	6
--	---

## **1 Introduction**

Internet is believed as an anarchic network with no point of control. To some extent Internet has decentralised sides with respect to traditional hierarchic networks beginning with telegraph and progressing to telephone networks.

On contrary to general assumption of Internet, it has a basic hierarchical control point which is about domain names. All domain names are stored in a central database called "root". So this database is simply a directory including the name and addresses of Internet world.

Since Internet has developed and grown up in a United States of America (US) centric environment the domain name process has been under US control. After the early days of Internet, it became more international and all nations have been involved in that networking process. But the control of that network has not been internationalised as it did. Since Internet become vital all over the world the power controlling internet domain names is seen jeopardising to nations' sovereignty.

This dissertation examines that US power over internet domain names and attempts of other nations, in international platforms, to restructure internet governance.

Next section will introduce how Internet grew up and come to today's network, also looks how domain name system works and argues domain name system being American.

Third section examines institutionalisation of management of domain names. This process have been merely developed in US hands. Its structure and legitimacy besides its not being democratic have always been criticised. This section goes into these issues.

Forth section looks for other nation's reaction to this internet domains governance scheme. Also examines the ITU attempts to restructure internet governance and severe US reactions

Fifth section includes conclusions.

## 2 Internet domains

Traditional networks, beginning with telegraphy and going on with telephone, have a hierarchic nature. The wisdom is centralised and besides centralised wisdom all the content flows through that centre(s). Because of that centralised structure this topology makes it more susceptible and attractive to enemy interests. In 1957, cold war era, US Department of Defense saw the need for Advanced Research Projects Agency (ARPA) after the Soviet Union's launch of a satellite system. Several years later ARPA began to focus on computer networking and communications technology. (Gromov, 1996) This project aimed to help post-nuclear war communications, so would help military to communicate even one hub is disabled. (Leiner et al, 1999)

Though Internet is often described as a mostly US government creation, Drissel (2006:105) believes it is an oversimplification. Much of the earliest research on the Internet dates back to American universities and think tanks, with European scientists and institutes also directly involved. Massachusetts Institute of Technology (MIT) researchers are frequently credited with conceptualising the initial plans for an interconnected global computer network in 1962, though scientists at the British National Laboratory (BNL) had developed a similar theory at about the same time. The US DoD became involved in the project soon after a groundbreaking Rand Corporation paper was published in 1964. With the DoD underwriting the project through the ARPA, research was conducted jointly at Rand, MIT, University of California Los Angeles, and the British National Physical Laboratory (NPL), eventually leading to the first successful trans-Atlantic test of the system in 1969. (Drissel 2006:105-106)

## **2.1 Data Communication**

This Internetworking project started in military basis and gradually it began to be used by others. In the early 1970s if one wanted to network computers from a particular vendor (e.g., IBM, Digital Equipment Corporation), one used networking technology that was proprietary to the vendor. IBM developed its Systems Network Architecture (SNA) and Digital Equipment Corporation developed DECNET. The US DoD, having shown the utility of packet switching through its long-lived ARPAnet project, pursued the idea of using computers in command and control. To avoid being constrained to a single vendor's equipment and networking technology, DARPA set out in 1973 to develop a non-proprietary networking standard that would support computer-based command and control. (Cerf, 2004:1360; Mueller 2002:76)

So this non-proprietary and open standard became the core of the Internet and named as Internet Protocol (IP). IP communication is different from traditional communications. It is a type of data communication and handled by breaking the message into smaller units called packets. These packets involve destination and source addresses in numeric forms which is called IP addresses. In order a packet to be sent to destination the IP address of destination should be known. Every computer connected to the Internet must have a unique IP address. To supplement these numerical addresses, the computers and other resources connected to network can be given user-friendly names. (Mueller 2002:5)

These user friendly names are called domain names. Domain names such as <http://www.wmin.ac.uk> are meaningful for human environment but not much for that



communications of machines. So there is a need to convert `http://www.wmin.ac.uk` address to `161.74.14.28` IP address for computers and network devices to understand where to send packets.

## **2.2 Resolution of Domain Names**

Domain Name System (DNS) is used as a result of this need. To look simply it is a directory containing name and IP addresses. To explain that mechanism by an example: when a user tries to access University of Westminster web page, s/he types "`http://www.wmin.ac.uk`" at browser and users computer first asks a machine known as a DNS server. (Figure 2-1) It is the job of the DNS server, which is usually operated by Internet Service Provider, to find the correct numerical address for requested page. The DNS server reads, in effect, from right to left; seeing that this is a message destined for some machine in the UK domain, it needs to find out where addresses in the UK domain is stored. It does this by asking a different machine (known as the "root server") that question: "Who is responsible for the UK domain?" The root server replies with the numerical address of a different machine (known as the "UK domain server"). Then DNS server asks UK domain server who is responsible for `ac.uk` domain and gets the address of `ac.uk` domain server and asks `ac.uk` domain server who is responsible for `wmin.ac.uk` domain and gets another numerical address (`161.74.14.28`, IP address of `wmin.ac.uk` web server) and now user's DNS server has completed its task; once it receives the address for `www.wmin.ac.uk`, it places that address into user's request to open page and sends it on its way. So personal computer now knows `wmin.ac.uk` is located on the address of `161.74.14.28`. (Liu and Albiz, 1998:28; Post, 1999)

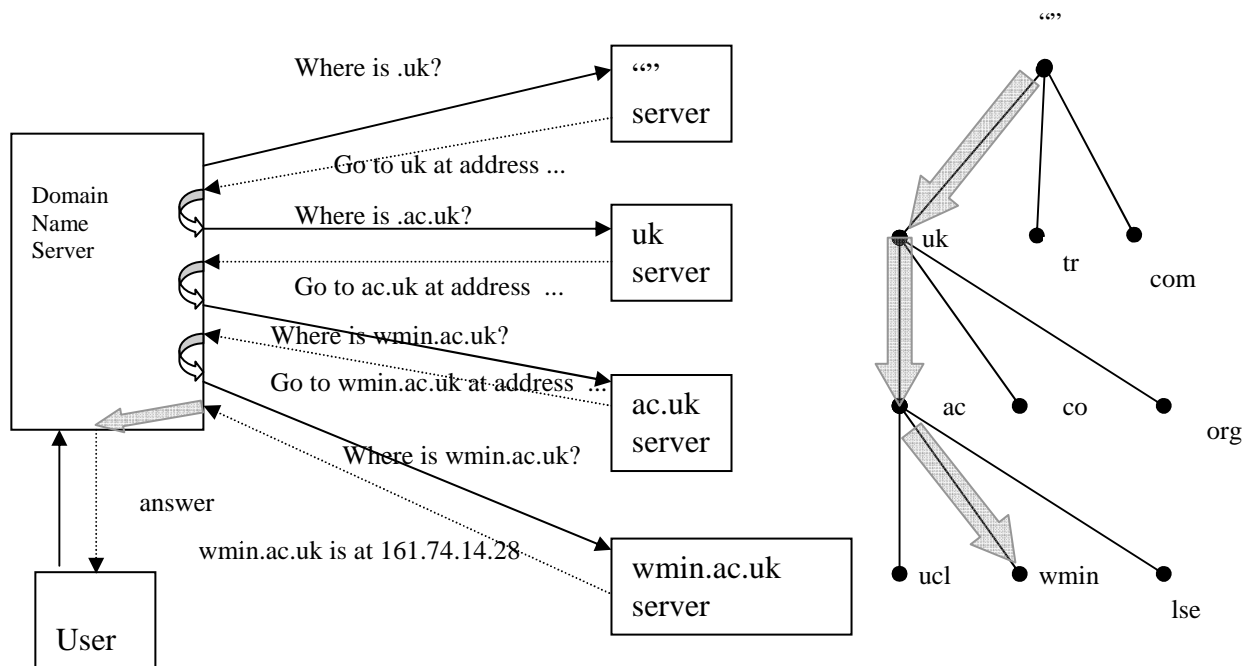


Figure 2-1 Resolution of win.ac.uk on the Internet <sup>1</sup>

### 2.3 The Domain Name System (DNS)

Through 1970s, the ARPAnet was a small friendly community of few hundred hosts. A single file, hosts.txt, was enough to map the addresses to IP numbers. Hosts.txt was maintained by Stanford Research Institute Network Information Center (SRI-NIC). This file was being updated once or twice a week. As ARPAnet grew, however, this scheme became unworkable. The size of hosts.txt grew in proportion to the growth in the number of ARPAnet hosts. Moreover the traffic generated by the update process increased even faster. (Liu and Albiz, 1998:3; Goldsmith and Wu, 2006:33; Su and Postel:1982)

<sup>1</sup> From Liu and Albiz, 1998:28

The problems were that the file, and hence the costs of its distribution, were becoming too large, and that the centralized control of updating did not fit the trend toward more distributed management of the Internet. (Mockapetris and Dunlap, 1988:112)

Various proposals for the development of a name space, and its management, were put forth in response to these problems. The common themes that emerged from these proposals were: (i) the notion of a hierarchical name space where the hierarchy roughly corresponded to organizational structure: and (ii) boundaries between differing levels of the hierarchy should be denoted by names using “.” dot. (Paré, 2003:14)

In 1984 Paul Mockapetris described Domain Name System. (RFC 882 and 883<sup>2</sup>) Domain Name System is a distributed database. This structure allows local control of the segments of the overall database.

## **2.4 Structure of DNS**

DNS has a hierarchical nature which is based on an inverted tree schemata with branches stemming from root, or “.” (dot). At nodal points, or domains, these branches divide into more branches leading to alternative nodal points, or sub domains. At Figure 2-1 right hand side depicts that reverse tree model of DNS.

---

<sup>2</sup> Mockapetris P., 1983 "Domain names Concepts and Facilities," RFC 882, USC/Information Sciences Institute, November 1983.

Mockapetris P., 1983 Implementation and Specification, "RFC 883, USC/Information Sciences Institute, November 1983.

Domains are labels assigned to the nodal points. (Paré, 2003:10) Brother nodes at same branch can not take same names. (Mockapetris and Dunlap, 1988:113) Simply on ac.uk node one other domain can not be named as “wmin” but on .com node you can name a domain as wmin which becomes wmin.com.

The domain names below root is called top level domains (TLDs). (Liu and Albiz, 1998:15, 16). There are three types of TLDs: generic top level domains (gTLDs); national or country code top level domains (ccTLDs), and top level domains restricted to use with in the United States. Some gTLDs are .com, .edu, .net, .org, .int. Some ccTLDs are .ca, .de, .tr, .uk. And .gov, .mil are reserved for exclusive use by agencies of United States federal government and military. (Hart and Rolletschek, 2003:13)

Below that top level domains there are child level domains called second level domains. (Liu and Albiz, 1998:16) .ac.uk is a second level domain within the .uk domain. This hierarchical structure gives the advantage of scalability and it is achieved through delegation. Delegating domains works a lot like delegating tasks at work. A manager may break up a large project into smaller tasks and delegate responsibility for each of these tasks to different employees. (Liu and Albiz, 1998:21)

Country registrars of domains names use that delegated power of DNS system to apply their own rules. For example in UK, .uk has elected to subdivide this top level domain into number of second level categories like .co.uk, .ac.uk, .plc.uk, .org.uk. In contrast the registry organisation for Canadian domain .ca subdivided this domain such that various aspects of Canadian political geography were incorporated into

domain names. (Paré, 2003:12) Turkish registrar subdivided .tr domain into many new sub domains like .av.tr for freelance lawyers, .bel.tr for municipalities. (NIC-tr, 2006:3)

## **2.5 The DNS Root**

All these sub domains use their rules (in line with general rules) and issue domain names under their domains. But all issued domain names are gathered into one “root”. Despite the fact that reference is often made to the “root” of the DNS in a manner that implies singularity, this root is, in fact represented by thirteen root servers. They are labelled “A” to “M”. (Paré, 2003:12) Because the system evolved informally, the root servers' administrators are diverse, including NASA, a Dutch non-profit organization, universities, the US military and private companies. Today, all told, ten root servers are operated from the United States and one each from Amsterdam, Stockholm, and Tokyo. (Cukier, 2005) The server where the root zone file is first loaded is considered authoritative; the others merely copy its contents. The additional servers make the root zone file available more rapidly to users who are spatially distributed, and provide redundancy in case some root servers lose connectivity or crash. (Mueller 2002:47) So basically domain name system is controlled or the root file is controlled by one point: “.” (dot). As stated most development of Internet and domain name system have happened in US so is DNS American? Next section looks for the answer.

## **2.6 Is DNS American?**

Markus Mueller (2004) argues legal basis of Internet ownership and control of US. The implications of the level of control the US exert over the Internet's infrastructure are far-reaching. Through its control over the root file, and over IP addresses (although to a much lesser extent), as well as any potential influence over the TCP/IP protocols, US has a power over the Internet unrivalled by any other nation. This power gives US much more influence on the policy decisions about the Internet than any other country. (Mueller Markus 2004:15) To examine the answer of question one should look it with respect to different aspects. First one is sovereignty.

### **2.6.1 Sovereignty**

A state derives from its sovereignty the title to exercise jurisdiction, which is the competence of a state to regulate conduct or the consequences of events. Territoriality is the primary basis for jurisdiction; as all persons and things within the territory of a state fall under its territorial authority, each state normally has legislative, curial and executive jurisdiction over them. (Mueller Markus 2004:15) So since the root server "A" is located in US does that gives power to regulate it?

This territorial claim can be replied depending on effects of domain name policies. These policies set by governing body of root server is directly affecting all the over the world and in the sovereign territories of other states. So the territorial claim of US sovereignty over root server creates severe problems.

## 2.6.2 Property

Ownership is the collection of rights allowing one to use and enjoy property, including the right to convey it to others; it includes the right to exclude others from use. Most conflict-of-laws questions regarding real property and tangible movables are governed by the *situs rule*, which applies the law of the place where the thing is located. However, if tangible movables are brought to another country this second country applies its law only to facts occurring after it crossed the border. Therefore the *situs rule* leads to application of the second country's property law but the second country will regularly recognize the ownership position gained in the first country. If property law rules are applied to the Internet and US owned it accordingly, then other countries would have to accept American ownership and control. But US ownership depends on to what extent the Internet can be perceived as tangible movables (or real property). (Mueller Markus 2004:18) However root file is not a tangible property only a set of data including domain names and respective IP addresses so can not be considered under property law. (Froomkin 2000:44-45)

## 2.6.3 Intellectual Property Law

US could argue a property right. Copyright protection of the root file depends on its content which includes names and addresses. Markus Mueller (2004:23-25) analysis this and finds an example of dispute *Feist Publications v. Rural Telephone Service*<sup>3</sup>. *Feist v. Rural*, was a United States Supreme Court case in which Feist had copied information from Rural's telephone listings to include in its own, after Rural had refused to license the information. Rural had sued for copyright infringement. The Court ruled that information contained in Rural's phone directory was not copyrightable, and that therefore no infringement existed. A copyrightable

---

<sup>3</sup> *Feist Publications, Inc., v. Rural Telephone Service Co.*, 499 U.S. 340 (1991)

compilation requires a creative arrangement of the facts. The arrangement of the facts within the root file is mainly alphabetical and otherwise random, i.e. non-creative. Even if there were an order similar to the use of the alphabet because of technical necessities, there would be no creativity. Thus the root file is not protected under US copyright law. (Froomkin 2000:45, Markus Mueller 2004:25)

#### **2.6.4 Patent**

The root file would have to be a process with useful, concrete and tangible results in order to qualify for patent protection but the root file is only data that is processed as input and does not represent the process itself, which is generated by the name servers. Thus the root file is not patentable and not subject to US Copyright or Patent protection. Instead of the root file one could focus on the DNS. The DNS meets today's basic requirements for patent protection because it directs users using a domain name to the corresponding IP address and therefore represents a software-based process with useful, concrete and tangible results. But it is at least uncertain whether it would have been patentable in 1983 because the patentability of computer programs was an unsettled issue then. As with TCP/IP, there is no report about a patent application and the protection would have already expired. For these reasons, the DNS is not protected by patent law. (Markus Mueller 2004:26)

So for Internet domains one can not tell about any American ownership or patent or copyright over root file. The next chapter will be about the process of how ICANN is established.



### **3 Internet Corporation for Assigned Names and Numbers**

This chapter will be about the way to ICANN and how ICANN established.

#### **3.1 How ICANN was born?**

On 1 January 1985 the domain name system was formally implemented as the addressing infrastructure for computer networks connected to the ARPAnet and/or the Defense Data Network. US Defense Communications assignment of IP numbers, on the Information Sciences Institute (ISI) at University of Southern California (USC), was awarded responsibility for managing domain name registration. (Stahl 1987) As a result the SRI-NIC acted on behalf of the ARPAnet and the Defense Data Network as both registrar of top-level domains and as administrator of the root domain servers. (Paré, 2003:17; Froomkin, 2000:53) And after that, the first domain names cmu.edu, purdue.edu, rice.edu and ucla.edu in April 1985, first .com domain think.com in May 1985, first .gov domain css.gov in June 1985, first .org domain mitre.org in July was registered. .uk was registered as the first two letter country code in July. (Paré, 2003:16-17)

In 1986, Information Systems Agency (DISA) began allowing some offshore DARPA research centres to perform some DNS registration functions, the first of which was University College, London, for a UK domain. Later, it allowed a research facility in Amsterdam to manage some IP address blocs under the European IP Networks (Réseaux IP Européens, RIPE). The government contracts for these activities remained with ISI, of which Internet Assigned Numbers Authority (IANA) was an unincorporated administrative unit. IANA's funding came from Department of Defense grants to USC. Although for a time IANA claimed to have a charter from the

Internet Society (ISOC) and the Federal Networking Council, it was at all relevant times a government contractor. (Froomkin, 2000:53-55)

### **3.1.1 Jon Postel**

Although US Defence Communications Agency had awarded responsibility for managing the DNS root and assigning of IP numbers to ISI, in a practise, this burden fell essentially on one person: Jon Postel. Postel was a researcher at the USC ISI, who had been involved with computer networking since the beginnings the ARPAnet. As a graduate student of the University of California at Los Angeles (UCLA), Postel had been present when the initial ARPAnet connection between UCLA and Stanford Research Institute was made in the autumn of 1969. Jon Postel took over the task of editing Request for Comments (RFC) and gravitated to the administration of unique number assignments for ports and protocols. (Mueller 2002:75) In 1972 he appointed himself as the numbers “czar” of numbers. (Postel, 1972) His personal influence over internetworking, and in particular the DNS, should not be underestimated. 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. (Paré, 2003:16)

### **3.1.2 Governance Shift from Research to Commercial**

In 1991, US Defense Information Agency (DISA) sought new tenders for the SRI-NIC management contract. The contract was awarded to a private entity called Government Systems Inc. This marked a shift away from the education/research-

based management of one of the Internet's core functions, toward core service provision by a commercial entity. The tenure of Government Systems Inc., as the responsible entity for managing the Network Information Center, was short lived. In 1992 US National Science Foundation (NSF) released a project solicitation seeking tenders for the provision and coordination of registration, database, and information services for the NSFnet internetworking backbone. (Paré, 2003:19)

On 31 December 1992, NSF entered into a cooperative agreement with Network Solutions, Inc. (NSI) for some of these services, including the domain name registration services. NSI managed key registration, coordination, and maintenance functions of the Internet domain name system. NSI registered domain names in the generic top level domains (gTLDs) on a first come, first served basis and also maintains a directory linking domain names with the IP numbers of domain name servers. NSI maintained the authoritative database of Internet registrations. (USDoC White Paper, 1998)

In addition to NSI two other entities, AT&T and General Atomics, were awarded collaborative partnerships to assist in the provision of a *seamless interface* for Internet users. AT&T was awarded responsibility for the provision of database services to extent and supplements the resources of the NSFnet. General Atomics, on the other hand, was awarded responsibility for the provision of information services including the development of a reference desk and a database of comprehensive networking materials. All three parties were awarded these responsibilities on the basis of a cooperative agreement, spanning a five year period from 1 January 1993 to 30 September 1998. In essence, this agreement granted NSI

a government-sanctioned monopoly over both the registration of second-level domain names in the generic top-level domain categories and the provision of registration services for the research networks funded by the NSF. (Paré, 2003:19)

The agreement gave NSI operational control of the DNS but, as in the predecessor agreement between DISA and GSI, required NSI to follow the policy directions of IANA. (Froomkin, 2000:57) Prior to 1995 Internet addressing was coordinated on informal administrative arrangements. No contractual relation existed between NSI and IANA. (Paré, 2003:20)

In 1994, Postel authored RFC 1591, *Domain Name System Structure and Delegation*, in which he described his policies and procedures for assigning domain names. Several issues which are fraught with controversy today took only a paragraph or two to explain in 1994. Thus, for example, RFC 1591 described relatively lightweight procedures for creating new top-level domains—an issue that has more recently consumed years of debate without the creation of any new gTLDs. Since establishing the basic system of gTLDs and ccTLDs, Postel and IANA had created a small number of additional ccTLDs and a few limited-use gTLDs, but no gTLDs for general use. By 1994, the demand for names in the gTLD space was still very small; the explosion in demand did not begin until at least two years later. RFC 1591 also described how one qualified to manage a ccTLD. It set up a rule of first-come, first-served so long as one had decent Internet connectivity, acted fairly, and was accepted by the user community. (Froomkin, 2000:55-57)

### **3.1.3 Controversies**

Besides number of names being registered was still relatively low in these years fees were not being levied for registering domain names, there was relatively little controversy associated with this monopoly. On 14 September 1995 National Science Foundation ignited a powder keg when it modified cooperative agreement with NSI, authorizing it to begin charging domain name registrants a fee for the free domain name registration services. (Paré, 2003:19, 23) The charge of US\$50 annual fee for all registrations worldwide among the .gov, .edu, .com, .net, and .org domains estimated 1996 to be worth \$1 billion to NSI. (Drezner, 2004:493) NSI monopolistic exploitation is seen as the initial impetus for ICANN's creation and igniting additional concern was the unveiling of a new domain dispute resolution policy in 1995 that appeared to favour corporate trademark holders over other, less powerful, domain owners. Exercising US government-approved extra-territorial regulatory powers to suspend any domain name worldwide, NSI increasingly alienated a growing number of Internet scientists, scholars, entrepreneurs, and other stakeholders. (Drissel 2006:110)

### **3.1.4 First Efforts for International Regime**

The first efforts to develop an international regime to reform the DNS came from non-state actors, particularly the Internet Society (ISOC), a network of researchers responsible for developing and managing the original ARPANET. After repeated false starts, ISOC formed the International Ad Hoc Committee (IAHC) to develop a proposal to manage domain names replacing NSI. (Drezner, 2004:494) The IAHC was an eminent persons group with representatives from ISOC, the International Trademark Association, WIPO (World Intellectual Property Organisation), IANA, IBM,

National Science Foundation and the ITU (International Telecommunication Union). (Mueller, 2002:143) The ITU secretariat was particularly eager to be involved, and viewed itself as the natural location for an international regime to manage these issues. (Drezner, 2004:494)

In 1996 and 1997, the IAHC produced a Memorandum of Understanding on Generic Top Level Domain Memorandum of Understanding<sup>4</sup> (gTLD-MoU), which was signed by eighty organizations in Geneva on 1 May 1997. ITU Secretary General Pekka Tarjanne announced with pleasure that the ITU had become the depository of the gTLD-MoU<sup>5</sup>. (Kleinwächter, 2003:1108)

The revised DNS system would be overseen by a new supranational non-profit association, headquartered in Geneva. Uniform rules would govern all registrars, though they would be allowed to compete with each other by assessing variable fees and timetables for domain name registrations. (Drissel 2006:110) However in political terms, the committee represented between the technical communities's governing hierarchy (ISOC, Internet Architecture Board (IAB) and IANA) and other political forces that contested the ISOC claim on the root in the previous round: trademark owners, the ITU, and the NSF. All were incorporated into the planning process and governance regime. The political coalition was also notable for whom it excluded. Network Solutions was not invited to be a part of group. Neither were any representatives of the alternative registries. Network Solutions Inc. (NSI) was the obvious target of gTLD-Mou. Early 1997 NSI was preparing for an initial public

---

<sup>4</sup> <http://www.iahc.org/gTLD-MoU.html>

<sup>5</sup> Press Release International Telecommunication Union, Changes to Internet Domain Names will Encourage Competition, Foster Growth and Stability, Geneva, 29 April 1997, [http://www.itu.int/newsarchive/press\\_releases/1997/itu-07.html](http://www.itu.int/newsarchive/press_releases/1997/itu-07.html)

offering of stock that would bring in hundreds of million dollars from profitable control of .com domain. The danger of losing control of .com registry to a Geneva-based corporation made NSI explicitly support the claim of the US government to authoritative control over the root. NSI was *persona non grata* within the ISOC-dominated technical community. It was also perceived with hostility by foreign governments and businesses, as a symbol of US dominance of the Internet and the cause of the domain name turmoil. In contrast, the company was well positioned in Washington D.C., backed by the lobbying and financial resources and as a longstanding government contractor; it found a US-centred institutional framework more predictable and more amenable to its interests. (Mueller 2002:143)

The body became the subject of sharp criticism, much of it centred on the identity of the decision makers. Some urged that the committee, largely composed of Internet engineers, did not adequately represent businesses interested in the Internet as a vehicle for electronic commerce; some worried that it gave too much representation to organizations, including the ITU and the International Trademark Association, that were seen as hostile to traditional Internet values; others expressed more general concerns that the committee structure was narrow, non-inclusive and secretive. (Weinberg, 2001: 315)

At those days European Union was monitoring domain name issues through its Directorate General 13, the branch in charge of telecommunications policy. Following the release of the gTLD-MoU proposal the DG-13 official Christopher Wilkinson wrote to the ISOC's Don Health, on 17 January 1997, expressing dissatisfaction with the lack of European participation and inadequate amount of time provided for

consultation. Wilkinson then convened a meeting of European Internet community members. The meeting was attended by representatives of nine top-level domain administrators of member states, Daniel Karrenberg of RIPE-NCC, and few commercial Internet service providers. The attendees reached a consensus that they should not sign the gTLD-MoU. (Mueller 2002:143)

### **3.1.5 The Way to Green Paper**

The US government withheld its support for Postel's plan to bring the A Root Server under the control of the ITU. Two months later, the Clinton Administration (1993–2000) published "The Framework for Global Electronic Commerce," which ignored the gTLD-MoU and offered an alternative proposal for the privatization of the global DNS management. (Kleinwächter, 2003:1108)

In July 1997, the responsibilities of the National Science Foundation were transferred to the Department of Commerce's National Telecommunications and Information Administration (NTIA) and, since then, the NTIA has led the transformation process. As a first step, the NTIA issued a Request for Comments (RFC) seeking input from various sources, such as experts, firms and governments. But the request also clearly laid out the position of the US Government: "The Government supports continued private sector leadership for the Internet and believes that the transition to private sector control should continue" RFC consisted of a catalogue of questions, among others the following one concerning the role of public actors: "What is the proper role of national or international governmental/non-governmental organizations, if any, in national and international domain name registration systems?" (Leib, 2002:163) In total approximately 430 comments from individuals



and organisations were submitted. (Paré, 2003:31) In its response to the RFC, the European Commission expressed deep concerns that the European private sector was inadequately represented in the self-governing mechanisms of the Internet, and that the US Government's perception of the Internet was too US-centred. The Commission emphasized the importance of the ITU and WIPO in establishing the legal basis of the new system, but it was forced to admit its lack of detailed knowledge about how the Domain Name System and the Root Server System worked. (Leib, 2002:163)

Under the direction of Ira Magaziner, a senior policy analyst on Internet issues for the President of the US, the DoC analyzed the submission throughout the autumn 1997. Congressional hearings focusing on domain naming policy also were conducted during this period. (Paré, 2003:31) As being Bill Clinton's friend and Internet policy czar Magaziner told Clinton as early as 1994 that the "commercialisation of the Internet would be a boon to the US economy that should be a top priority for US government. (Goldsmith and Wu, 2006:40)

On 10 December 1997 Magaziner met Jon Postel. Magaziner's good news was he had found funding for IANA that would last until September 1998 (the date when the new corporation envisioned in the Green Paper would be up and running). The bad news was that it would be the US government, not Postel or IANA that would decide whether and when new TLDs would be added to the root. (Mueller 2002:161)

In response to these on 28 January 1998 Postel challenged US authority that rivalled the gTLD-MoU. Postel sent e-mail to eight of the twelve operators of the Internet's

regional root servers. In the normal course of affairs, the twelve regional root servers would synchronize their information with Root Server A, the master root server owned by the US government and operated by NSI. But Postel asked the regional server to take “small step” of recognising his own server, located on the USC campus, as the authoritative root. It was a tall order with danger of US reaction but all eight operators complied because of Postel’s personal authority. NASA, US Military, the Ballistics Research continued to recognise the US government as root authority. Now the Internet was split up into two, one is controlled by US government and other simply by Postel’s server. Postel didn’t make any changes to root file only replicated the previous one so users didn’t notice any changes. But it was big a challenge to US authority. (Goldsmith and Wu, 2006:43-45)

Postel was ordered to return the root servers’ configuration to their original state, and he complied. Magaziner later publicly stated that attempt to manipulate the root without the US government’s permission would be prosecuted as a criminal offence. (Mueller 2002:161) These days were so tense that Postel suffered a heart attack and never lived to see the birth of the successor organization, ICANN. (Cukier 2005)

### **3.1.6 The Green Paper**

US DoC released its proposals in the form of a Green Paper, on how to transfer the stewardship of the DNS to a private sector based administration on 30 January 1998. The Green Paper noted that the four principles guiding the evolution of the DNS should be stability, competition, private bottom-up coordination, and representation. In spite of these principles, the scheme presented by the authors of this document was widely perceived by non-US based actors as being overly US centric. The

creation of a new private not-for-profit corporation, to be headquartered in US and incorporated under US law, was proposed. The purpose of this new corporation was to coordinate the functions that hitherto IANA had been responsible for (i.e. allocation of IP address space to regional registries, overseeing operation of authoritative root server, determining circumstances under which new top-level domains are added to the root, and coordination of technical parameters required to ensure universal Internet connectivity). Significantly, the proposal also recommended how the board of directors of this new corporation should be structured. The Green Paper also called for a separation of registry and registrar functions, and advocated experimentation by allowing each of these functions to operate on a competitive basis. To this end, the proposal called for a period of transition within which five new registries and five new top-level domains would be introduced into the DNS and monitored by the new corporation. The results of this experiment could then be used to guide future additions to the root. With regard to trademark considerations, approach set forth in this document implied moving away from the quasi-centralised governance model akin to the earlier Postel framework. The Green Paper stated that US government was opposed to the establishment of “a monolithic trademark dispute resolution process at his time”, favouring a framework wherein registries and registrars established their own minimum dispute resolution procedures. (Paré, 2003:31,32)

### **3.1.7 The White Paper**

From January 1997 release of Green Paper to June 1997 release of final policy statement (The White Paper), organised business lobbying groups spearheaded the formation of a dominant coalition. Political leadership came from Internet divisions of IBM and MCI. The key vehicle for organizing business interests was the Global

Internet Project (GIP). GIP was formed in 1996 by high level executives of 16 Internet, telecommunications, and e-commerce firms. Its objective, which had taken shape during the controversies over encryption and content regulation in the mid-1990s, was to resist “unnecessary international regulations and national laws that impede or inhibit growth”. IBM’s vice president for Internet technology, John Patricki took over leadership of the group early in 1998. Shortly thereafter, GIP began to focus on Internet governance. The business leaders behind GIP were, naturally enough, deeply involved in the Clinton administration’s attempt to develop a global framework for electronic commerce, and encouraged Magaziner’s policy of private sector leadership. MCI-Worldcom, which was an emerging as the world’s dominant Internet backbone provider, was also an active, founding member of GIP. In many respects, the coalition’s core members bore a striking resemblance to the IBM, MCI, and University of Michigan consortium that had operated the National Science Foundation’s Internet Backbone from 1987 to 1995. In the course of developing the NSFNET backbone, IBM, MCI, a few key university network administrators, and the Internet technical hierarchy all cultivated close working relationships with federal agencies to gain access to funding. During the development of the White Paper, Magaziner and GIP would play a key role in unifying the technical hierarchy, trademark holders, and larger telecommunication and information technology companies around a common agenda. (Mueller 2002:168-171)

The White Paper was not designing the executive representation of new corporation governing the root in detail which was evaluated as “step back” of US government by Weinberg (2001:316). It repeated, though, that the board should represent the direct interests of Internet users as well as membership organizations in the areas of

names, numbers and protocols. The board, it continued, should 'equitably represent' domain name registries, domain name registrars, IP number registries, the technical community, Internet service providers, and commercial, not-for-profit, and individual Internet users. Its members should be elected by means of 'mechanisms that ensure broad representation and participation in the election process'. The White Paper did not specify exactly how this new organization would come into being. It suggested, though, that if the new entity were formed by 'private sector Internet stakeholders', the US government was prepared to recognize it. (Weinberg, 2001:316)

The White Paper did not set out a specific dispute resolution policy. Rather, its recommendations regarding this matter mirrored the framework proposed earlier by the gTLD-Mou initiative. To this end, the WIPO was called upon to initiate a process, incorporating the participation of both trademark and non-trademark holders, leading to: (i) the development of recommendations for a uniform approach to trademark/domain name disputes involving cyber piracy, but not conflicts between legitimate trademarks holders with legitimate competing rights; (ii) the recommendation of process for protecting famous trademarks in the generic top-level domains; and (iii) an evaluation of the effects of adding new generic top-level domains and related dispute resolution procedures on trademark and intellectual property holders. According to the White Paper the period of transition to the establishment of private sector administration of DNS was anticipated to last approximately two years, during which time the US government would continue to participate in a policy oversight role until the new corporation was established and operationally stable. A target date for full transition to private sector administration was set for September 2000. (Paré, 2003:31,32)

### **3.2 Formation of ICANN**

In the fall of 1998, the process of forming the new corporation proceeded rapidly. In September of that year, the ICANN was legally incorporated and, two months later, it was recognized by the US Government. Many details of what happened between the publication of the White Paper and the foundation of ICANN are still unclear. Several activities, such as the International Forum on the White Paper, ran parallel to the US Government's action, but could not influence the process considerably. The reform of the Internet's governance structure had moved to high-level politics and behind closed doors. The organizational structure of ICANN reflected the relative power positions of the major players in the process. First of all, the US Government insisted on establishing the new organization in the US, and, accordingly, ICANN was incorporated as a private not-for-profit corporation under California law. Nevertheless, the Europeans (and other participants from outside the US) had to be convinced in that ICANN's units were filled using principles of geographic diversity and international representation. ICANN's structure included the Governmental Advisory Committee (GAC) as a forum for public actors of all kinds – government officials, as well as representatives of intergovernmental organizations. The existence of the GAC indicates that the voices of those actors who spoke out against the purely private sector self-regulation of Internet addresses and names, especially the European Commission, were not completely ignored. But the GAC has never had power to directly influence ICANN's decisions. Since its establishment, ICANN has formed the centre of a predominantly private global regime of Internet governance whose evolution has not yet come to a close. (Leib, 2002:168)

Besides GAC, ASO (Address Supporting Organisation) is another unit of ICANN, developed and recommends for global policies concerning allocations of IP addresses. Other unit is the Domain Name Supporting Organisation (DNSO), develops recommendations for global policies concerning the DNS. Trademark and IP groups, businesses, registries, ISPs/Telcos, and non-profit organisations were represented in DNSO. The Protocol Support Organisation (PSO) advised ICAN on Internet protocols and technical standards. The IETF, W3C, ITU and ETSI were represented in the PSO. The GAC had representatives from WIPO, ITU, European Union (EU), Organisation for Economic Cooperation and Development (OECD) and some 59 national governments. (Caral, 2004: 18,19)

### **3.3 New Regime**

According to Mueller (2002:185) the new regime defined and distributed property rights in the domain name space and imposed economic regulation on the domain name industry. The property system that ICANN created was a highly regulated and conservative one, analogous in many respects to broadcast licensing in US. Its essential features can be summarised like this. (i) NSI monopoly profits were redistributed to a broader class of claimants by regulating its wholesale rates and transforming .com, .net, and .org into shared domains. (ii) The administration of the domain name space was linked directly to intellectual property protection. Trademark protection became one of the major determinants of the contractual features of registering a domain name, of policies governing access to information about domain name registrants, and of policies governing the creation of new top-level domains. (iii) End users were stripped of most of their property rights in domain names and deliberately deprived of most opportunities for representation in ICANN's processes.

(iv) Artificial scarcity in top-level domains was maintained. Just as in broadcast licensing, artificial scarcity fostered a regime of merit assignment and weak property rights for licensees. (v) NSI succeeded in retaining a long-term property right over the .com registry. The gTLD-MoU faction's attempt to require all registries to be non profit was unsuccessful. (vi) National governments and intergovernmental organizations had a limited role. (vii) The US government retained residual authority over DNS root. Instead of giving up that authority after two years, as originally contemplated, the government has held on to it definitely. (Mueller 2002:185-186)

Mueller (2002:218-219) defends that ICANN is not only a technical coordination body or only standard setting organisation. Rather, it is an institution that ties the need for technical coordination to regulation of industry built around the resources it manages. And Mueller (2002:219) gives example of radio frequency administration at the national level. Nominally, the assignment of the radio frequencies in a given location must be coordinated to prevent electromagnetic interference among users. However national governments don't simply coordinate frequency use: they regulate wireless industries by attaching conditions and standards to assignment of frequencies. Sometimes the regulatory intent of the conditions is overt, as when broadcast licensees are required to fulfil specific public interest obligations or when broadcast content is regulated or censored as a condition of using broadcast channel. The industry can also be regulated in less direct but equally important ways, through the imposition of uniform technical standards, by controlling the number of entrants into the market or by approving or rejecting corporate mergers. The common element is that the regime has exclusive control of a critical input into an industry and uses the leverage it has over access to that resource to regulate industry. In radio spectrum



management, control is exercised through licenses issued by government regulatory agencies. In ICANN's case, Mueller (2002:218) thinks regulation of conduct and market structure is imposed on registries and registrars via contracts with root administrator. Mueller's (2002) argument on ICANN's policy setting is based on three main areas: (i) Rights to Names: ICANN defines and enforces property rights in names. This function involves the recognition and protection of various kinds of intellectual property claims on domain name assignments, and resolution of disputes based on those claims. (ii) The second policy is economic regulation of supply industry for domain names. ICANN uses its control of the root to regulate the supply of top-level domains, and to regulate the price, performance, and market structure of the domain name registration industry. (Mueller, 2002:219) And Mueller (2006:463,469) adds the vertical separation of registrar and registry aspects and price controls are imposed by ICANN. (iii) The third policy area involves the exploitations of data generated by Internet identifiers to facilitate surveillance and control of Internet users by law enforcement agencies. (Mueller, 2002:219)

### **3.4 Problems with ICANN**

The most controversial ICANN issues have been the DNSO (At-Large Membership, representation, democratic legitimacy) and the GAC (role of Governments, accountability). There has been less controversy with respect to the ASO and PSO, whose remit is largely technical in nature, and less likely to impact on commercial and political interests. The EU has extended its qualified support for ICANN, but has expressed its concern on certain issues including: the nature of, and arrangements for, balanced and equal oversight of some of ICANN's activities by public authorities; the rules to govern generic domains; the redelegation of certain ccTLDs to another

manager at the request of the Government concerned, and the transfer of the management of the root server system from the USDoC to ICANN, under appropriate international supervision by public authorities. (Caral, 2004:19) Some of the problems are examined below.

### **3.4.1 Legitimacy**

Lindsay (2001:15) argues that ICANN can not obtain legitimacy from its relationship with US government, as US government cannot claim untrammelled authority over the DNS or legacy root and, in fact, has been concerned to disown authority. The legitimacy conferred by an international treaty between nation states has been consciously eschewed. ICANN has therefore been forced to search for new forms of legitimacy. ICANN has sought to establish legitimacy through a variety of mechanisms. First, it has contended that it is engaged in technical coordination, not policy-making. The next part will be about this claim which is undefendable. Second, largely as a result of pressure from DoC, it established certain accountability mechanisms, including the election of 'at-large' directors and an independent review policy. These mechanisms have not yet proved successful and, without more, are unlikely to resolve ICANN's legitimacy deficit. Thirdly, ICANN has claimed that it is consensus-driven and that it represents the consensus of the Internet community. This is an attempt to trade off the successful Internet standards-making process and to capitalise on a tradition of thought favouring 'bottom-up self-ordering' governance for the Internet. ICANN policy decisions are not at all suited to consensus decision-making. Moreover, in practice, ICANN decisions cannot possibly be made on the basis of consensus, and there is no way of determining whether there is a consensus of the Internet community. Nevertheless, the problem of legitimacy confronting

ICANN is an example of a significant legal and political problem: the problem of the legitimacy of international actors, whether public or private, that engaged in public policy-making in the absence of a global 'civil society'. The legitimacy of such organisations depends, in large measure, upon establishing mechanisms for democratic accountability. Democratic accountability does not, however, equate simply with direct elections or plebiscites. An important means for establishing legitimacy at the national level has been the imposition of legal limitations on decision-making, in the form of constitutional limitations, procedural safeguards and independent review of decisions. Rather than ignoring these traditional accountability mechanisms, or claiming that they are too inflexible to apply to the Internet, the legitimacy of ICANN would be enhanced by learning from legal techniques used at the national level. Establishing a clear legal basis for ICANN's functions and obligations, entrenching transparent decision making, and providing for effective review of ICANN decisions would not only remove many doubts concerning ICANN's legitimacy, but would improve ICANN decision-making. (Lindsay 2001:15,16)

### **3.4.2 Technical Coordination or Policy Making**

As Mueller (2002:219) sets ICANN itself as policy maker on the other hand Fromkin (2000:93) argues the relationship between ICANN and US DoC and finds the exact nature of DoC's relationship with ICANN difficult because a studied ambiguity on a few key points serves the interests of both parties. According to Fromkin (2000:94) Both ICANN and DoC deny that ICANN is engaged in either regulation or governance. Instead they proffer the standard-setting view, in which ICANN is engaged in nothing more than routine standard setting or perhaps technical coordination. The standard-setting view seeks to take advantage of a long line of

cases accepting delegations of near-regulatory power to private technical, agricultural, mechanical, or scientific groups.

Although White Paper's (USDoC White Paper, 1998) "4. Creation of the New Corporation and Management of the DNS" title it is stated that "... the creation of a new private, not-for-profit corporation responsible for **coordinating** specific DNS functions for the benefit of the Internet as a whole." Froomkin (2000) does not agree that ICANN "has no statutory or regulatory authority of any kind.

### **3.4.3 Transparency**

At American Society of International Law 101<sup>st</sup> Annual Meeting, Esther Dyson, founding Chairman of ICANN admits making two huge mistakes. (Wu et al., 2007:3) The first was not to be open in how the ICANN was created and how the initial board was selected. But then holding the board meetings in private for the first year or two, which completely destroyed any affection ICANN might have had among the people who were supposed to be the people on behalf of whom ICANN were developing policies. That created a very unhappy relationship between ICANN itself and the Internet community. It was exacerbated by the fact that ICANN was trying to privatize Network Solutions, which owned the .com, .net and .org registries. Dyson tells NSI behaved extremely badly, which made things worse because the US wanted to pretend that ICANN was not created by the US and had given it no funding. And he adds ICANN had very little in the way of the budget so it had to "tax the Internet." For Dyson the second big thing they did wrong was to impose way too strict and precisely defined contracts. And he thinks even now, the terms on which registries and registrars can compete are extremely limited; they have to offer pretty much the

same services for the same prices, with restrictions on almost anything creative – including stronger security, privacy services and the like. (Wu et al., 2007:3,4)

The appointed initial ICANN Board extended their terms unilaterally without public input. The ICANN has also been criticised for allowing occasional Board meetings to be held in without minutes or transcripts of proceedings available to the public. (Drissel, 2006:114)

#### **3.4.4 Democracy**

Internet users elected 5 of the 19 ICANN Directors in an online election in 2000. These directors are supposed to represent At-Large Membership, i.e. the general public of Internet users. However, out of an estimated 300 million Internet users at that time, only 33,000 (or 0.01%) cast their votes. (Caral, 2004:19) An Internet user approaching the ICANN process from the outside would have little way to determine how to participate meaningfully in the decision-making process. (Palfrey 2004:1)

The Center for Democracy and Technology examines the democracy of ICANN and tells ICANN Board and governance structure that made the gTLD selection is not appropriately representative of the public voice. (Berman and Davidson 2000)

A Governmental Advisory Committee (GAC) for the 180+ governments of the world was invited to give 'advise' to the board of directors on issues of public interests. But according to the ICANN bylaws, the recommendation of the GAC had no binding power for the ICANN directors. (Kleinwächter, 2004:239)

Gross, the US coordinator for international communications and information policy, states that governments are extraordinarily uncomfortable in fact, are completely perplexed by the fact that they would give non-binding advice to some private entity, that's something that government officials don't normally do. (Wu et al., 2007:8)

Esther Dyson, founding Chairman of ICANN, rationalizes national governments playing fewer roles in ICANN governance by claiming governments being very small part of the world, even though they putatively control most of it. And Dyson states users, all around the world, being treated shabbily by their own governments, censored, ignored are now part of governance of ICANN. Dyson adds that international meetings being very useless because of attending people being cousins of important ministers living very nicely in expensive hotels in Geneva. (Wu et al., 2007:8) Dyson's these rationales reflects the point of view of ICANN founders to international governance of domain name system.

#### **4 National and International Efforts**

Communication is a precious strategic resource. Its role is fundamental in an economy dominated by the non-material. So control of the net could put whoever holds it at a decisive strategic advantage. In the 19th century control of sea routes (“ruling the waves”) were at the heart of the British Empire’s enormous power. In theory, hegemony over the net gives the US the power to limit anyone’s access to any site in any country. It can also block emails anywhere in the world. So far, it has never done this. But technically it could, and a number of countries are worried by this potential. (Ramonet, 2005)

The governments are concerned about Internet being controlled by a private entity. Brazil for example raised a very legitimate and serious issue. The question, was, the Brazilian government, rely tremendously on the Internet. They basically use it for tax purposes; for government services. When and if the Internet goes down, if some catastrophic event outbreaks, are citizens of US going to look to Brazilians? The Brazilian government, to be responsible for fixing this problem, and to whom will they go? Do they go to some international organization? Brazil stated they know how to go to the UN or any international organisation. But on the other side going to a not-for-profit company at California and asking what is going on is very weird for Brazilian government. (Wu et al., 2007:7)

DNS not being American (2.6 Is DNS American?) but governed by a private company under US California laws made governments seek ways of designing a new structure under an international body for domain name system governance. The arena for

these efforts has been World Summit on the Information Society (WSIS). WSIS is held by ITU.

#### **4.1 ITU and Internet**

ITU is the United Nations agency for information and communication technologies. ITU's role in helping the world to communicate spans 3 core sectors: radiocommunication, standardization and development. ITU also organizes TELECOM events and was the lead organizing agency of the World Summit on the Information Society. It was founded as the International Telegraph Union in Paris on 17 May 1865. Its main tasks include standardization, allocation of the radio spectrum, and organizing interconnection arrangements between different countries to allow international phone calls. ITU is based in Geneva, Switzerland, and its membership includes 191 Member States and more than 700 Sector Members and Associates.<sup>6</sup>

The early telegraph and telephone companies appreciated that the value of their networks increased with their greater interconnection. This required the adaptation of technical standards led the treaty establishing ITU. At those days PTT's were owned by states so the main actors of ITU were sovereign countries. In contrast Internet was developed in an academic and corporate technical elite environment. So the mentality of governance between these two structures has always been different. In early 1990s the ITU and the IETF clashed with competing e-mail standards of X.400 and TCP/IP. (Caral, 2004: 14,15)

---

<sup>6</sup> [www.itu.int](http://www.itu.int) last accessed 12 August 2007



ITU was conspicuously absent from Internet governance debates in the 1990s, for two reasons. One was a self-imposed restraint on the grounds of its charter that clearly limited its authority to the international telephone and radio system. The other reason was the widespread rejection of any established bureaucratic and regulatory structure by the Internet's technical elite, which would have rendered any attempt to get engaged in Internet governance by the ITU futile to begin with. Yet with the convergence of technologies and applications, and the criticism of ICANN and other US based institutions, the ITU seemed to position itself as an outright governing body, but at least as neutral facilitator. In the tradition of international treaty conferences, it convened the WSIS as a process projected to last several years including plenary conferences and working groups, reports and resolutions. (Pommerening, 2006:5)

When ITU had its Plenipotentiary Conference in Minneapolis in October/November 1998, the gTLD-MoU was treated as a non-existent paper. Even the ITU Resolution 102, *Management of Domain Names and Internet Addresses*, did not refer to the gTLD-MoU with a single word. It invited instead the secretary-general of the ITU, to take an active part in the international discussion and initiatives of the management of domain names and Internet addresses, which is being led by the private sector. The Minneapolis Deal was reached by classic diplomatic asymmetric compromise. The US government withdrew its opposition to the plans of the ITU to prepare a world conference on the information society and got in exchange the recognition of the private sector leadership in Internet governance. Later the US DoC recognized ICANN. ITU secretary-general Pekka Tarjanne accused President Clinton's Internet adviser, Ira Magziner, during the World Economic Forum in Davos, January 1999, of

hypocrisy. The US government was arguing for self-governance of the Internet by the providers and users of services without governmental involvement, but was reserving for itself a special role by placing the DoC as the final overseeing body for ICANN. Magaziner defended his position by referring to the two year transition period and the foreseeable end of the special role of the DoC. But this transition was extended. (Kleinwächter 2004:239)

## **4.2 World Summit on the Information Society**

The Cold War's end stimulated new interest in a long-standing UN institution: the World Summit. World summits are one-time conferences organized by the UN to address global issues such as environment, housing, or food. They involve thousands of policy makers working together over several years to develop consensual visions of principles and possible solutions to some of humankind's most challenging problems. While each summit embodies this form, each also departs from it in some ways. WSIS adopted two significant innovations. First, WSIS was a double summit, with the first meeting in Geneva in 2003 and the second in Tunis in 2005. This possibly offered opportunities for more prolonged policy making. Second, WSIS formalized the role of civil society to an unprecedented degree, creating an official "civil society bureau" that held formal meetings with the bureaus for governments and the private (business) sector. (Klein, 2004:3-5)

ITU has promoted the establishment of the WSIS after Minneapolis 1998 plenipotentiary conference. The main purpose of the WSIS is to address issues such as the digital divide between developing countries and Western economies. (Pommerening, 2006:5)

Ambassador David Gross (Wu et al., 2007:1), the US coordinator for international communications and information policy, depicts summits as parties and the fun and games happen before the summit, not at the summit. All of the negotiations happen ahead of time in what's called preparatory meetings, where the world gathers, or at least diplomats from the world gather. One thing that was done differently, something that was really unique, was that the private sector, NGOs, private companies were invited in some fashion to participate. This was done because the Internet, of course, was being driven forward by the private sector. But, of course governments and in particular many diplomats are uncomfortable with that, and so the first big fight was on the summits rules of the game. (Wu et al., 2007:1)

So in order to understand what happened at WSIS we have to look back to preparatory meetings. Preparations for the first WSIS phase started in June 2002. At this time, ICANN was in the middle of its reform process and the ITU prepared its next plenipotentiary conference for Marrakesh, which had, inter-alia, a re-evaluation of Resolution 102 on its agenda. Internet governance was not an issue at that meeting. But during the series of regional ministerial WSIS conferences, it got more and more attention. The African Regional WSIS Conference in Bamako, 30 May 2002, ignored the subject. None of the 14 content-related preparatory workshops for Bamako dealt with Internet governance. The nine pages of the Bamako Declaration did not include a single word or paragraph on Internet governance. The European WSIS Regional Ministerial Meeting in Bucharest, November 2002, raised one aspect of the issue, the management of domain names, but with low priority. Bucharest Declaration includes the heading 'setting up an enabling environment, including legal,

regulatory and policy frameworks'. The Asian WSIS Regional Ministerial Conference in Tokyo (January 2003) followed the Bucharest Declaration, but added to 'domain names' also the management of 'IP addresses'. One step further went the Latin American WSIS Regional Ministerial Conference in Bavaro (January 2002) in the Dominican Republic. Here, for the first time, the term 'Internet governance' appeared in a WSIS document. The final Regional WSIS Ministerial Conference for West Asia (Beirut, February 2003) took this one big step further by introducing ideas like suitable international organization, multilingualism and national sovereignty with regard to Internet governance. (Kleinwächter, 2004:240,241)

Beirut Declaration stated that:

"The responsibility for root directories and domain names should rest with a suitable international organization and should take multilingualism into consideration. Countries' top-level-domain-names and Internet Protocol (IP) address assignment should be the sovereign right of countries. The sovereignty of each nation should be protected and respected. Internet governance should be multilateral, democratic and transparent and should take into account the needs of the public and private sectors as well as those of the civil society." (Beirut Declaration, 2003:5)

Then first WSIS was in Geneva in 2003. Peake (2004:5) determines that at first WSIS many developing nations, particularly China, South Africa, Brazil and most Arab States expressed the view that Internet governance was a matter related to national sovereignty and that an intergovernmental process, preferably under the UN (with the ITU being specifically mentioned), was needed where governments could discuss policy issues of international scope. Besides most developed nations, including US, European Union, Japan, Canada and Australia, supported the current system of private sector leadership. They were referring to the narrower definition of Internet governance, particularly to ICANN's responsibilities, but also to general understanding that the Internet had developed successfully through self-regulation

and that this should be encouraged to continue. They took the view that the system works so there is no need to change it. (Peake 2004:5) Delegates agreed to postpone the decision until the 2005 meeting in Tunis, where, after much uncertainty, the status quo once again prevailed. (Pickard, 2007:127)

At Geneva (WSIS-1) the decision to try to resolve differences of opinion through a working group established under the auspices of the UN Secretary General reflected a compromise between those governments that felt the WSIS process was not open enough to enable the full and active participation of private sector and civil society, and others who wanted a process within the UN framework. So Working Group on Internet Governance (WGIG) was established. (Peake 2004:5) The main activity of the WGIG was "to investigate and make proposals for action, as appropriate, on the governance of Internet by 2005." The WGIG was asked to present the result of its work in a report "for consideration and appropriate action for the second phase of the WSIS in Tunis 2005. (OECD, 2005:31)

Preparatory Conferences for Tunis had witnessed hard arguments. At Prep-Com3 EU made a surprise proposal to create an intergovernmental body that would set principles for running the Internet. US has sharply criticized demands (like by Iran) for a UN body to govern the Internet, US Ambassador Gross stated "No intergovernmental body should control the Internet, whether it's the UN or any other." US officials argue that a system like the one proposed by the EU would lead to unwanted bureaucratization of the Internet. David Hendon, a spokesman for the EU delegation, stated US as overreacting. (Wright, 2005)

In response to EU proposal US launched an enormous lobbying campaign to retain its position. Most significant among all those lobbying efforts was a letter sent from the US secretary of state Condoleezza Rice to the UK foreign minister Jack Straw acting in the role of presidency of the EU. In the letter, Rice used strong language for a diplomatic missive, to stress how seriously the US administration was taking the issue and how determined it was to retain ICANN in overall charge of the Internet. European diplomats privately confessed that the letter had a significant impact on their position. (McCarthy, 2005) The letter is below:

7 November 2005

To: The Right Honourable Jack Straw MP, Secretary of State for Foreign and Commonwealth Affairs, London

Dear Foreign Secretary,

The governance structure and continued stability and sustainability of the Internet are of paramount importance to US. The Internet has become an essential infrastructure for global communications, including for global trade and commerce, and therefore we firmly believe that support for the present structures for Internet governance is vital. These structures have proven to be a reliable foundation for the robust growth of the Internet we have seen over the course of the last decade.

As we approach the World Summit on the Information Society (WSIS), we should underscore the vast potential of the Internet for global economic expansion, poverty alleviation, and for improving health, education and other public services, particularly in the developing world where Internet access remain unacceptably low.

The Internet will reach its full potential as a medium and facilitator for global economic expansion and development in an environment free from burdensome intergovernmental oversight and control. The success of the Internet lies in its inherently decentralized nature, with the most significant growth taking place at the outer edges of the network through innovative new applications and services. Burdensome, bureaucratic oversight is out of place in an Internet structure that has worked so well for many around the globe. We regret the recent positions on Internet governance (i.e., the "new cooperation model") offered by the European Union, the Presidency of which is currently held by the United Kingdom, seems to propose just that - a new structure of intergovernmental control over the Internet.

The four principles US issues on June 30, 2005, reinforce the continuing US commitment to the Internet's security and stability, including through the historical US role in authorizing changes or modifications to the authoritative root zone file. At that time, we also expressed our support for ICANN as the appropriate private sector technical coordinator of the Internet's domain name and addressing system. We believe that ICANN is dedicated to achieving broad representation of global Internet communities and to developing policy through consensus-based processes. We have also expressed our interest in working with the international community to address legitimate public policy and sovereignty concerns with respect to country code top-level domains (ccTLD). We wish to underscore that, in our statement of June 30, we supported ongoing dialogue on issues related to Internet governance across international forums.

US and the European Union have long worked together toward the goal of global access to the Internet. The WSIS offers us the opportunity to reaffirm our partnership to spread the benefits of the Internet globally. At the same time, the security and stability of the Internet are essential to US, the European Union, and to the world. We firmly believe that the existing Internet system balances the stability and security we need with the innovation and dynamism that private sector leadership provides.

The history of the Internet's extraordinary growth and adaptation, based on private-sector innovation and investment, offers compelling arguments against burdening the network with a new intergovernmental structure for oversight. It also suggests that a new intergovernmental structure would most likely become an obstacle to global Internet access for all our citizens. It is in this spirit that we ask the European Union to reconsider its new position on Internet governance and work together with us to bring the benefits of the Information Society to all.

Sincerely,

Carlos M. Guterrez Secretary of Commerce

Condoleezza Rice Secretary of State

(McCarthy, 2005)

At the Summit of Tunis 2005 (WSIS-2), according to Klein (2005:1), states other than US made concessions but took some advantages. ICANN's greatest weakness – its lack of legitimacy and its related lack of support from governments around the world is less after WSIS. Governments that criticize ICANN are criticizing an arrangement that they themselves reviewed and left unchanged. However the WSIS decision cannot really be called an endorsement of ICANN. The text nowhere mentions ICANN by name, and there is no real declaration of support. Still, the UN has decided not to act against the organization, and this collective inaction is the final word after years of debate. Another important WSIS outcome is the launch of the Internet Governance Forum (IGF). IGF is a multi-stakeholder forum. Although a creation of the UN, the forum membership includes more than just UN member states; participating equally are entities from the private sector and from civil society. However, the forum has no concrete power. It is an advisory body. Its member discusses and formulates collective recommendations, but those recommendations do not carry the weight of policy. (Klein, 2005:1-5)

The formation of the IGF was an important step in creating a flexible procedural structure for identifying, discussing and addressing key issues through a growing multi-stakeholder policy dialogue. (Dutton, 2006:1) The IGF is intended to be a multi-lateral, multi-stakeholder non-binding body. Thus, the remit is broad, but the power is minimal. The UN have taken the lead in formulating this body, and in February 2006 organised a consultation in Geneva to discuss its structure. (Rogers, 2007:7) The Inaugural Meeting of the IGF took place in Athens, Greece from 30 October - 2 November 2006. The meeting only went into internationalised domain name issues, security and access issues. (IGF Secretariat, 2006)

#### **4.3 Turkish Government Contributions**

Turkish Government contributed both WSIS processes. For Geneva phase Turkish government stated the intellectual property rights should be subject to the regulations of WIPO rather than IMF, WB and WTO. (Turkish Republic, 2003:2)

While commenting on WGIG report Turkish Government stated that the international governance of the Internet should be multilateral, legitimate, transparent, accountable and participatory. Turkish Government explicitly supported the general principle that no single government or a group of governments should have a pre-eminent role in relation to international Internet governance. (Turkish Republic, 2005a:1)

Turkey suggested the new organizational structure should function under the auspices of the United Nations, which can guarantee the participation of all



governments on an equal basis. And Turkey stated there should be three bodies within this new structure: (i) Policy and decision making body, (ii) operational body, and (iii) advisory body. (Turkish Republic, 2005a:2)

According to Turkish suggestion:

1. Policy and decision making body should be responsible for international Internet-related policy issues. Besides, this body should act as the final decision making mechanism of the whole structure. This body will consist of members from governments with appropriate representation, which allows equal and rotating participation from all UN regions. The representatives of private sector and civil society should follow this body's work as observer.
2. Operational body should be responsible for the development of the Internet in both technical and economic fields and day-to-day operational management of the Internet. This body should consist of administrative, technical and legal experts, and follow the rules and the procedures of other specialized UN agencies for recruitments. There should be cooperation mechanisms between this operational body and other technical entities, such as the Internet Engineering Task Force.
3. Advisory body should be responsible for providing suitable platforms for all relevant parties to discuss and facilitate coordination of Internet-related policy issues.

(Turkish Republic, 2005a:2)

At the preparatory meeting (WSIS – Prepcom 3 - Sub-Committee A) Turkey stated special attention should be paid for multilateral, fair and legitimate administration of the root zone files and root server system of the domain name system. (Turkish Republic, 2005b) For multilingual domain names, Turkey also determined that the effort of multilingualization of domain names and e-mail addresses needs international cooperation. (Turkish Republic, 2005c)

Besides these Turkey emphasized national sovereignty while commenting on WGIG report stating: 'there is a great need for international and enforceable legal regulations and measures, while respecting national sovereignty.' (Turkish Republic, 2005a:2)

#### **4.4 Governmental Advisory Committee**

Governmental Advisory Committee (GAC) is ICANN's the body for channelling governmental input into ICANN's policy development processes. ITU is a full GAC member and its Telecommunication Standardization Sector (ITU-T) is also a member of ICANN's Protocol Supporting Organization (PSO). (Kleinwacher 2004:243) At WSIS governments made it clear that they want a greater voice in ICANN decisions, and the GAC is expected to be the vehicle for that. (Klein, 2005:1-5)

GAC has been seen as US compromise to other nations in order to make ICANN internationalised. But as governing power considered other nations have never been happy with GAC's weak power on ICANN policies. For example Government of Germany, at ITU Reform Meeting, stated that:

Germany is not in a position to support concepts regarding the future GAC structure which would give the ICANN GAC a more independent legal structure and/or would result in direct or indirect financial obligations, e. g. by introducing membership or meeting fees, because this would, in the end, mean to establish a new intergovernmental body for Internet Governance issues. If no other cost-neutral solution will be available, it should be carefully considered if and under which conditions the ITU would be in a position to provide the secretariat function for the ICANN GAC. Due to the fact that the ITU has taken part in the GAC work as observer from the very beginning, the necessary expertise is already available. (Germany, 2006:3)

Germany explicitly argued the government inactive position at GAC. Instead of the artificial GAC setting including the GAC advice "detour", governments would have a chance to work together with all significant parts of the Internet community in a more direct way. In this new setting, the ITU could possibly not only provide the framework for the necessary cross-issue government coordination prior to ICANN meetings, but also take a leading role e. g. regarding the outreach and capacity building challenges. (Germany, 2006:4)

#### **4.5 Internationalised Domain Names (IDN)**

Language is one the most important tool for a nation. Internet domain names being used with English alphabet poses problems to people who can not speak English. So internationalised domain names are big issue for governments. While the Internet can deliver text in email or by web pages in most of the world's languages' scripts, email addresses and web page addresses must be typed in English language "ASCII" characters. (Peake, 2004:15) There are many different alphabets like Chinese, Arabic, Cyrillic, Greek etc. which are not represented in domain name system. And WGIG defines 'multilingual TLDs, e-mail addresses and keyword lookup, as well as insufficient multilingual local content' as unresolved issue. (WGIG, 2005: 8)

ICANN's 2007-2010 draft strategic plan (ICANN, 2007b:10) includes "The deployment of Internationalized Domain Names as TLDs" as one of the key priorities. On the other hand during WSIS, some countries gave the impression that they considered the lack of IDNs to be the result of a pro-English language conspiracy. (Peake, 2004:15)

#### **4.6 Country Code Top Level Domain (ccTLD)**

On 17 August 2007 press release, ICANN declared that it is not into the operation of ccTLD but ICANN verifies the validity of the delegation request.

The operation of a country's ccTLD is an internal matter for each country and its local Internet community. In support of this, ICANN is responsible for delegating authority for the operation of ccTLDs to a specific operator based upon requests received from the country and its local Internet community. ICANN's evaluation is focused on verifying the validity of the request, and ensuring it meets a number of technically-focused criteria. Apart from this analysis, the selection of both the operator, and the method of operation of a ccTLD is a matter for countries and local Internet communities to decide. (ICANN, 2007a)

But delegation happens by commitments on contract, it is like licensing and obvious way of regulation, rules of which is defined by ICANN. So ccTLD policies impinge on domestic policy, and they also diminish the sovereignty of nations to adopt laws independently of ICANN. (von Arx and Hagen, 2002)

#### **4.7 National Sovereignty and Balkanizing Internet**

In 1978, delegates from 78 governments attending a conference of the Intergovernmental Bureau of Informatics endorsed a report warning that transborder data flows could place national sovereignty in jeopardy. In 1979, a committee of the Canadian government suggested that transborder data flows pose possibly the most dangerous threat to Canadian sovereignty. Similarly, in 1979 a report by Commission of European Community worried that foreign control of transborder data flows and related industries threatened a reduction in Europe's independence in decision-making in all walks of public and private life. From mid-1970s to the mid-1980s, an international debate raged over the transmission of computerised information via telecommunications and across national borders for processing, storage, and use. Many governments and independent analysts worried that the use of transborder data flows, particularly by American-based transnational corporations, could have negative effects on national economic, legal and sociocultural independence. Cumulatively, these effects were said to undermine national sovereignty and justify new regulations. (Drake, 1993:259,260)

In 70s and 80s transborder data flow and its control by American-based transnational corporations was big concern for state nations. But after 90s, besides financial data

flows, Internet began to be used at many areas of daily life and governmental processes. According to Mueller et al. (2007), for territorial states founded on the principle of national sovereignty, formal acceptance of the principles of nonterritoriality and end-to-end information flow constitutes a significant surrender of power.

Besides Mueller et al., Kleinwächter (2004:248) believes in transformation, where the 'old governance system', rooted in the concept of the sovereign nation-state, is complemented by an emerging 'new governance system', which is global by nature and includes more actors than the 180+ national governments and their intergovernmental international organizations.

As these scholars define new system actors as 'more' actors, the ICANN, 'the manager of the domain name system root zone' (ICANN, 2007a), does not accept any other old actor (government) to be in its policy setting processes. GAC only plays the advisory role having no political over ICANN board.

To exemplify this situation, North Korea (Democratic People's Republic of Korea) requested the '.kp' domain to be delegated to North Korean Government. '.kp' has been assigned to North Korea at ISO 3166-1 standard<sup>7</sup>. This request hasn't been on the agenda of ICANN board for a while and at 17 August 2007 ICANN announced that the request is discussed at 14 August but no decision was made on the delegation during this meeting. (ICANN, 2007a)

---

<sup>7</sup> International Standardization Organization Standard  
<http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/index.html>  
accessed 20 August 2007

Another example is Zaire case, in 1997; Zaire changed its name to the Democratic Republic of the Congo. It has since occupied the .cd name space. (Yu, 2003:11) And '.zr' top-level domain deleted from the root zone. (IANA, 2001)

Besides North Korea and Zaire, Afghanistan's country code top level domain name was altered. In the late 1990s, the ongoing civil war situation inside Afghanistan, registration of new domain names in the .af registry was halted. And in January 2003 the .af ccTLD redelegated the current delegees to the Ministry of Communications of the Islamic Transitional Government of Afghanistan. (IANA, 2003)

All these examples explicitly puts that country code domain names are delegated, redelegated, deleted, or refused to be delegated to governments. Obviously this process is not a day-to-day or technical operation, it is political decision made by ICANN.

Nations, not being able to participate in governance processes of Internet, are very concerned about using Internet all of parts of the daily life. This situation may pave to rise of new roots which are dangerous for universality of Internet. Any country may establish its own root server and push Internet service providers to use this server to resolve addresses. Then the result will be spitted Internet.

While Mueller (2002:50) defines it as creating parallel Internets, Carney (2005) sees balkanization of Internet. Besides Kumar and Mowshowitz (2006:36) depicts the

situation as chaos, Klein (2005:4) finds it interesting to see how many groups propose technical innovations that effectively decentralize the root.

Mestdagh and Rijgersberg (2007:31) tells it is not only possibility, China already launched alternatives to .com domain names using Chinese characters that are directly accessible to 110 million Chinese Internet users and are not accessible outside China without configuration changes.

#### **4.8 Solution Proposals**

Many governments (like Turkey, Chapter 4.3 ) proposed alternative regimes for Internet domain name governance. Output of WGIG (WGIG, 2005) the group proposed four models for solution.

First one is establishing Global Internet Council (GIC) members from Governments with appropriate representation from each region and with involvement of other stakeholders. And take over governance from the Commerce Department and replacing ICANN's Governmental Advisory Committee (GAC). ICANN would be accountable to GIC. Second one is no specific oversight organization handling governance, but GAC's role possibly enhanced to "meet the concerns" of some governments on specific issues. Third one is handling of national policy issues, along with international issues that don't fall under another intergovernmental organization, by an International Internet Council (IIC). And the last one is splitting Internet governance authority between a Global Internet Policy Council (GIPC), with private sector and civil society in "observer" roles; the World Internet Corporation for Assigned Names and Numbers (WICANN), a "private sector-led," "reformed

internationalized ICANN"; and a Global Internet Governance Forum (GIGF) for coordination. (WGIG, 2005:13-16 and Washington Internet Daily, 2005)

Most of the solution proposals (like WGIG, 2005; Schönberger and Ziewitz, 2006:2-3(EU); Turkish Republic 2005a) include international and intergovernmental management of domain name system. At technical level day-to-day operations may be still handled by existing structure but policy setting affairs should be delegated to an international body.



## 5 Conclusions

Internet was born and bred in US and then began to be used all over the world. In its early days name system governance was not an issue of politics. Few technical groups were using it and it was governed by Postel. After internet taking part of lives of individuals, organisations, corporations and governments it became vital for 21<sup>st</sup> century man kind and its governance now is not only a technical thing as its early days.

Many governments concern about not being involved in the governing process of the thing affecting their nation deeply, and demand international governance with participation of all multistake holders.

ICANN's current structure has problems of legitimacy, democracy, transparency. And it not only a technical coordination institute as claimed. Its political decisions directly influence other nations where they can not participate in decision making mechanisms.

US, using its power, enjoys keeping ICANN relation to DoC and gives international community symbolic roles in ICANN's units. And other nations are not satisfied with these roles that not influential for agenda setting and policy making mechanisms of internet governance.

So they look for ways of internationalising internet governance and reduce US impact on political level. On the platform of UN's ITU these attempts embodied several years

ago. Two world summits about information society witnessed the domain name control wars. But US did not give big compromises and status quo keep continuing with small roles given to international institutions and governments.

The debate seems keep going on with US firm defence of preserving current structure and other nations and international institutions struggle internationalise internet governance. But now the danger of splitting internet emerges, some governments and some commercial companies already put in service.

So the besides internet governance debate we will witness network wars between the biggest US controlled internet and other small networks managed by other governments and commercial companies. So far, US depending on giant network have not taken into account of these newly emerged small networks which can operate parallel to internet. But while US preserving status quo on political and commercial control over domain names, alternatives will get larger and larger and in future we may not talk about a unique universal network called internet.

## 6 References

Beirut Declaration (2003) Report of the Western Asia Regional Conference for WSIS. Document WSIS/PC-2/DOC/8-E. Beirut, 4-6 February 2003. Available from: [http://www.itu.int/dms\\_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0008!!PDF-E.pdf](http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/doc/S03-WSISPC2-DOC-0008!!PDF-E.pdf)  
(Date viewed 12 July 2007)

Berman J. and Davidson A. (2000) 'ICANN: Towards Domain Name Administration in the public interest'. Center for Democracy and Technology. Available from: <http://www.atlanticroot.com/cdtresponse.html>  
(Date viewed 23 July 2007)

Caral, J.M.A. (2004) 'Lessons from ICANN: Is self-regulation of the Internet fundamentally flawed'. *International Journal of Law and Information Technology*, Vol. 12, No1, 2004, Oxford University Press.

Carney, B.M. (2005) 'Breaking Up Is Hard to Do Should the US or the U.N. control the Internet? Here's a third way'. *The Wall Street Journal*, 12 November, 2005  
Available from: <http://www.opinionjournal.com/extra/?id=110007543>  
(Date viewed 23 July 2007)

Cerf V. (2004) 'On the Evolution of Internet Technologies', *Proceedings of the IEEE*, Volume 92, Issue 9, Sep 2004 pp.1360 – 1370.

Cukier K.N. (2005) 'Who Will Control the Internet?'. *Foreign Affairs*, November/December 2005. Available from: <http://www.foreignaffairs.org/20051101facomment84602/kenneth-neil-cukier/who-will-control-the-internet.html>  
(Date viewed 2 August 2007)

Drake W.J. (1993) 'Territoriality and Intangibility: Transborder Data Flows and National Sovereignty'. In: Nordenstreng K., Schiller H.I.(eds.) *Beyond National Sovereignty: International Communications in the 1990s*. 2<sup>nd</sup> Printing 1995, Ablex Publishing. pp.259-313

Drezner D. W. (2004) 'The Global Governance of the Internet: Bringing the State Back In'. *Political Science Quarterly*, Volume: 119, No:3. pp.477-498.

Drissel D. (2006) 'Internet Governance in a Multipolar World: Challenging American Hegemony'. *Journal Cambridge Review of International Affairs*, Volume 19, Issue 1 March 2006 , pp.105 –120.

Dutton, W.H. (2006) 'Addressing the Issues of Internet Governance for Development: A Framework for Setting an Agenda for Effective Coordination'. *Paper submitted to the first Internet Governance Forum*. Available from: [http://www.intgovforum.org/Substantive\\_1st\\_IGF/Dutton-IG4D-30July06.pdf](http://www.intgovforum.org/Substantive_1st_IGF/Dutton-IG4D-30July06.pdf)  
(Date viewed 4 July 2007)

Froomkin A. M. (2000) 'Wrong Turn in Cyberspace'. *Duke Law Journal*, Volume 50:17, pp17-184

Germany (2006) 'ITU and WSIS Follow-Up - Food for Thought'. ITU Council Working Group on the World Summit on the Information Society, Government of Germany Federal Ministry of Economics and Technology, Document:3, 22 January 2006. Available from: <http://www.itu.int/reform/contributions/3.doc>  
(Date viewed 16 July 2007)

Goldsmith J and Wu T. (2006) *Who controls the Internet?*. New York: Oxford University Press.

Gromov, G.R. (1996) *The roads and crossroads of Internet's history*. Available from: <http://www.netvalley.com/intvalold.html>  
(Date viewed at 12 July 2007)

Hart T. and Rolletschek G. (2003) 'The challenges of regulating the Web'. *info* Volume 5 Number 5. pp. 6-24  
(Date viewed 13 May 2007)

IANA (2001) Deletion of .zr Top-Level Domain, *IANA Report*, 20 June 2001. Available from: <http://www.iana.org/reports/zr-report-20jun01.htm>.  
(Date viewed 13 July 2007)

IANA (2003) Request of Islamic Transitional Government of Afghanistan for Redlegation of the .af Top-Level Domain, *IANA Report*, 8 January 2003 Available from: <http://www.iana.org/reports/af-report-08jan03.htm>  
(Date viewed 13 July 2007)

ICANN (2007a) 'Clarification Regarding .KP Country Code Top-Level Domain', *Internet Corporation for Assigned Names and Numbers Announcements*, 17 August 2007. Available from: <http://www.icann.org/announcements/announcement-2-17aug07.htm>  
(Date viewed 23 August 2007)

ICANN (2007b) ICANN Strategic Plan, July 2007. Available from: [http://www.icann.org/strategic-plan/draft\\_stratplan\\_2007\\_2010\\_clean\\_final.pdf](http://www.icann.org/strategic-plan/draft_stratplan_2007_2010_clean_final.pdf)  
(Date viewed 19 August 2007)

IGF Secretariat (2006) Summing Up The Inaugural Session of the Internet Governance Forum (IGF). Athens, 30 October - 2 November 2006 Available from: <http://www.intgovforum.org/Summary.Final.07.11.2006.htm>  
(Date viewed 11 May 2007)

Klein H. (2004) 'Understanding WSIS: An Institutional Analysis of the UN World Summit on the Information Society'. *The Massachusetts Institute of Technology Information Technologies and International Development*, Volume 1, Number 3-4, Spring-Summer 2004. pp.3-13

Klein H. (2005) *An Assessment of the WSIS-2/Tunis '05 Outcomes*. 23 November, 2005. Available from:  
<http://www.IP3.gatech.edu> and [www.InternetGovernance.org](http://www.InternetGovernance.org)  
(Date viewed 11 July 2007)

Klein H. and Mueller M. (2005) *What to do about ICANN: a proposal for structural reform*. Available from: [www.Internetgovernance.org/pdf/igp-icannreform.pdf](http://www.Internetgovernance.org/pdf/igp-icannreform.pdf)  
(Date viewed 21 July 2007)

Kleinwächter, W. (2003) 'From self-governance to public-private partnership: The changing role of governments in the management of the Internet's core resources'. *Loyola of Los Angeles Law Review*, vol:36. pp.1103-1126

Kleinwächter, W. (2004) 'Beyond ICANN Vs ITU? How WSIS tries to enter the new territory of Internet governance', *Gazette: The International Journal for Communication Studies*, vol:66(3-4). Pp.233-25.

Kumar N. and Mowshowitz A. (2006) 'Who should govern the Internet?'. *Communications of the ACM*, Vol. 49, No. 2. pp.35-37.

Leib V. (2002) 'ICANN - EU can't: Internet governance and Europe's role in the formation of the Internet Corporation for Assigned Names and Numbers (ICANN)'. *Telematics and Informatics*, Volume 19, Issue 2, May 2002. pp.59-171

Leiner B.M., Cerf V. G., Clark D.D., Kahn R.E, Kleinrock L., Lynch D.C., Postel J., Roberts L. G. and Wolff S., (1999) *A Brief History of the Internet*. Available from:  
<http://arxiv.org/abs/cs/9901011> (Date viewed at 13 July 2007)

Lindsay D. (2001) 'Should We Believe in Rough Consensus? ICANN and the Problem of Legitimacy in Managing the Domain'. *Communications Research Forum*, 26 - 27 September 2001 Canberra, Australia

Liu C., Albiz P., (1998) *DNS and BIND*, O'Reilly & Associates, Inc.

McCarthy K. (2005) 'Read the letter that won the Internet governance battle Condoleezza Rice's missive to the EU', 2 December 2005 Available from:  
[http://www.theregister.co.uk/2005/12/02/rice\\_eu\\_letter](http://www.theregister.co.uk/2005/12/02/rice_eu_letter)

Mestdagh, C. N. J. De Vey and Rijgersberg, R. W. (2007) 'Rethinking Accountability in Cyberspace: A New Perspective on ICANN'. *International Review of Law, Computers & Technology*, Volume:21, No:1. pp 27-38.

Mockapetris P.V. and Dunlap K.J. (1988) 'Development of the Domain Name System'. *ACM SIGCOMM Computer Communication Review*, Volume 25 , Issue 1. pp.112-122

Mueller Milton L. (2002) *Ruling the root: Internet Governance and Taming of Cyberspace*, MIT Press

Mueller Milton L (2006) 'Toward an Economics of Domain Name System' In: Cave M.E., Majumdar S.K., Vogelsang I.(eds.), *Handbook of Telecommunications Economics*. Elsevier. pp.443-500.

Mueller Milton L., Mathiason J. and Klein H. (2007) 'The Internet and Global Governance: Principles and Norms for a New Regime'. *Global Governance* Volume: 13, Issue: 2. pp.237-254.

Mueller Markus (2004) 'Who Owns the Internet? Ownership as a Legal Basis for American Control of the Internet'. *Fordham Intellectual Property, Media & Entertainment Law Journal*, Vol. 15, Book 2.

NIC-tr (2006) ".tr" Domain Names, Policies, Rules and Procedures; Version 4.6 June, 2006. Available from: <https://www.nic.tr/forms/eng/policies.pdf>. (Date viewed 24 July 2007)

OECD (2005) *OECD input into the UN Working Group on Internet Governance* (WGIG) DSTI/ICCP(2005)4/Final, Available from: <http://www.oecd.org/dataoecd/34/9/34727842.pdf> (Date viewed 24 May 2007)

Paré, D. J. (2003) *Internet Governance in Transition: Just Who is the Master of this Domain?*. Rowman & Littlefield Publishers, Inc.

Peake A. (2004) 'Internet governance and the World Summit on the Information Society', *Report for the Association for Progressive Communications*.

Pickard, V. (2007) 'Neoliberal Visions and Revisions in Global Communications Policy From NWICO to WSIS'. *Journal of Communication Inquiry*, Volume 31 Number 2. pp.118-139.

Pommerening, C. (2006) 'National Sovereignty and Global Institutions: An Analysis of Recent Developments in Internet Governance.'. Critical Infrastructure Protection Program May 2006, George Mason University. Available from: <http://cipp.gmu.edu/archive/Pommerening-SovereigntyInstitutionsInternet.pdf> (Date viewed 24 July 2007)

Post, D. G. (1999) 'Governing cyberspace, or where is James Madison when we need him?' *Plugging in*. Available online at: [www.temple.edu/lawschool/dpost/icann/comment1.html](http://www.temple.edu/lawschool/dpost/icann/comment1.html) (Date viewed 19 July 2007)

Postel J. (1972) 'Proposed Standard Socket Numbers', *Request for Comments : 349*, 30 May 1972. Available from: <http://www.ietf.org/rfc/rfc349.txt> (Date viewed: 23 July 2007)

Ramonet I., (2005) 'The spider in the web' , *Le Monde diplomatique*, November 2005, Available from: <http://mondediplo.com/2005/11/01Internet> (Date viewed: 27 July 2007)

Rogers, K. M. (2007) 'The Early Ground Offensives in Internet Governance', *International Review of Law, Computers & Technology*, Volume:21 No:1. pp5-14.

Schoenberger V.M and Ziewitz M. (2006) 'Jefferson Rebuffed: US and the Future of Internet Governance.', *Faculty Research Working Paper Series, Harvard University*, Available from:  
[http://ksgnotes1.harvard.edu/research/wpaper.nsf/46ad8749e613af608525693c0014d6cc/8ea51cb384b27b6785257178007afd9b/\\$FILE/Jefferson%20Rebuffed.pdf](http://ksgnotes1.harvard.edu/research/wpaper.nsf/46ad8749e613af608525693c0014d6cc/8ea51cb384b27b6785257178007afd9b/$FILE/Jefferson%20Rebuffed.pdf)  
(Date viewed 14 July 2007)

Stahl M. (1987) *Domain Administrators Guide, Request for Comments : 1032*, November 1987, Available at <http://www.ietf.org/rfc/rfc1032.txt>  
(Date viewed 23 July 2007)

Su Z.S. and Postel J. (1982) *The Domain Naming Convention for Internet User Applications, Request for Comments : 819*, August 1982, Available from:  
<http://www.ietf.org/rfc/rfc819.txt> (Date viewed 23 June 2007)

Turkish Republic (2003) *The Contribution of Turkey for PrepCom-2, Document WSIS/PC-2/CONTR/68-E*, 23 January 2003. Available from:  
[www.itu.int/dms\\_pub/itu-s/md/03/wsispc2/c/S03-WSISPC2-C-0068!!PDF-E.pdf](http://www.itu.int/dms_pub/itu-s/md/03/wsispc2/c/S03-WSISPC2-C-0068!!PDF-E.pdf)  
(Date viewed 27 July 2007)

Turkish Republic, (2005a) *The Comments of the Government of Turkey On the Report of the Working Group on Internet Governance, Document WSIS-II/PC-3/CONTR/56-E*, 15 August 2005. Available from:  
<http://www.itu.int/wsis/docs2/pc3/contributions/co56.pdf>  
(Date viewed 27 July 2007)

Turkish Republic (2005b) *WSIS Executive Secretariat Compilation of Comments Received on the Report of the Working Group on Internet Governance (WGIG) Corrigendum 1 to Document WSIS-II/PC-3/DT/7(Rev.1) E*, 26 September 2005. Available from: <http://www.itu.int/wsis/docs2/pc3/working/dt7rev1corr1.doc>. (Date viewed 27 July 2007)

Turkish Republic (2005c) *Initial Comments of the Government Of Turkey on Internet Governance WSIS – Prepcom 3 - Sub-Comittee A*, 20 September, 2005 – Morning Session. Available from:  
[http://www.bilgitoplumu.gov.tr/dbtz/dbtz/Comments%20of%20Turkey\\_20092005.doc](http://www.bilgitoplumu.gov.tr/dbtz/dbtz/Comments%20of%20Turkey_20092005.doc)  
(Date viewed 27 July 2007)

USDoC White Paper (1998) *United States Department of Commerce, DNS Management of Internet Names and Addresses*. Available from:  
Available at [http://www.ntia.doc.gov/ntiahome/domainname/6\\_5\\_98dns.htm](http://www.ntia.doc.gov/ntiahome/domainname/6_5_98dns.htm) (Date viewed 12 July 2007)

von Arx K.G. and Hagen G. R. (2002) 'Sovereign Domains: A Declaration of Independence of ccTLDs from Foreign Control'. *Richmond Journal of Law & Technology*, Volume 9, issue:1.

Available from: <http://www.law.richmond.edu/jolt/v9i1/article4.html> (Date viewed 12 July 2007)

Washington Internet Daily, *Developing Countries Back New Internet Oversight Body*. June 15, 2005, Available at <http://www.warren-news.com/Internetservices.htm> in (Date viewed 14 July 2007)

Weinberg J. (2001) 'Geeks and Greeks'. *info*, vol.3, no.4. pp.313-332.

WGIG (2005) Report of the Working Group on Internet Governance. June 2005, Château de Bossey. Available at <http://www.wgig.org> (Date viewed 24 July 2007)

Wright T. (2005) 'EU Tries to Unblock Internet Impasse'. *International Herald Tribune* 30 September 2005, Available from:

<http://www.nytimes.com/iht/2005/09/30/business/IHT-30net.html>  
(Date viewed 27 July 2007)

Wu, T., Dyson E., Froomkin, A. M. and Gross, D.A. (2007) 'On the Future of Internet Governance'. *American Society of International Law, Proceedings of the Annual Meeting*. Vol. 101, 28-31 March 2007, Washington DC.

Yu P.K. (2003) The Never ending ccTLD Story In: Erica Schlesinger Wass (ed.) *Addressing The World: National Identity and Internet Country Code Domains*. Rowman & Littlefield, 2003 Available from: <http://ssrn.com/abstract=388980>  
(Date viewed 17 August 2007)