DNS Economics

Stakeholders, Business Models, Power Structure

Mathias Ehlert and Mathias Nitzsche

Humboldt-Universität zu Berlin, Wirtschaftswissenschaftliche Fakultät, Institut für Wirtschaftsinformatik

Abstract. The domain name service is a critical part of the Internet, used to translate human readable domain names to required IP-addresses. A variety of scientific papers were devoted to its technical details, whereas little attention has been drawn to economical aspects. Therefore, this paper focuses on identifying stakeholders along the hierarchy of the DNS, their functions and their business models. Special emphasis is put on the ICANN, in charge of managing and further developing the DNS. Eventually, the introduction of new top Level domains in 2010, as one of today's major changes in the system, supervised by ICANN, is evaluated.

Table of Contents

1 Introduction

The Domain Name System is one of the most important services for today's use of the Internet. It translates human readable addresses into the required numerical addresses and thus can be seen as a backbone of Internet communication. Its origins go back to the early 1980's and it has evolved constantly since. The technical aspects of the DNS in all their details have been the focus of many scientific contributions published over the years. With the expansion of the World Wide Web, the economic value of domain names grew accordingly. Under this premise, the analysis of the DNS, as the backbone of the WWW, from an economical point of view did not receive enough attention in literature. The following work will try to fill this gap, by giving an overview of DNS Economics. The reader shall get an understanding of where in the DNS economical considerations can be made.
Chapter two will introduce the reader to the technical basics of the DNS which are necessary for further reading. Therefore, a short historical introduction is given, and the 3 parts composing the DNS are described: The namespace, the servers and the resolvers.
In the third chapter, the hierarchical structure is used to identify stakeholders of the DNS on all levels from top to bottom. Starting with the root zone, the ICANN as the controlling organization is examined. A quick introduction to its history is given first, followed by more information about ICANNs current composition. Afterwards, the financial setting of the ICANN is analysed by describing planned revenues and expenses for the fiscal year 2010. In the next steps, stakeholders on lower hierarchy levels are covered. Registries' and registrars' economical situations are outlined and the position of Internet Service Providers is described. Furthermore, governments' possible involvements on the DNS are shown and finally end users' roles are identified.
The next chapter will focus on one of the main sources of conflicts in the DNS space since more than a decade, the introduction of new top level domains (TLD). The reasons for the shortage within the namespace and the ongoing expansion will be examined in regards to their economical value. Embedded in a brief case study of the .berlin TLD application the current activities in this field are outlined.
At the end the of this paper gained insights will be concluded and an outlook to further research on economical aspects of the DNS is presented.

2 Technical aspects of DNS

2.1 Historical background

The genesis of the DNS reaches back to the very early days of the Internet, or its predecessor the ARPANET. The first proposal for the mapping of names to numbers to identify a host has been discussed in 1971 [RFC226], because even the technically very sophisticated users of that time preferred human readable host names instead of technical numbers. This mapping was done using a file

called hosts.txt, which had to resist on every host connected to the network. With less than 100 participants until 1984 [5] the Stanford Research Institute maintained one central instance of this file, which could be downloaded via FTP by all other network hosts.[22]
With the growth of the network this system was heading towards problems: [RFC1034]

- First of all, the file got too big and changed too frequently - resulting in a high bandwidth consumption to transfer the file.
- The central maintenance of the file, was against the trend of a distributed network.
- The network changed from the original NCP based ARPANET (connecting large timesharing systems) to TCP-IP based connection of workstations. So the number of hosts increased rapidly (before roughly the number of organizations) to the number of connected host (roughly users).

Since existing name systems did not meet exactly the needs of flexibility required for the Internet [1], a new distributed management of domain resources was needed. From 1983 to 1985 Paul Mockapetris et al. developed the DNS, which offered the functionality of hosts.txt, allowed maintenance in a distributed manner, was compatible with most existing environments, had no limits in size and offered a good performance. According to RFC1034 in the next 3 chapters the 3 major components (or layers) of the DNS are explained: [RFC1034]

- domain name space and resource records
- domain name server
- resolvers

2.2 Domain Name Space and Resource Records

The namespace of the DNS is structured hierarchically, to enable distributed maintenance and almost unlimited extensibility. Each node in this variable depth tree has an associated label (with a length from 1-63 bytes) and is identified with a domain name composed of all labels from the node up to the root connected by a dot - see figure 1. By convention domain name are printed or read left to right, from the most specific (lowest, farthest from the root) to the least specific (the root). [RFC819] [RFC805] Each domain name is regarded as its own DNS zone, with a local administrator, who is independently maintaining the names-to-host mapping in his zone. How this is organized from a non technical point of view, will be the topic of Chapter 3.
Controversially discussed was which domains will be created directly under the root (called Top Level Domains, TLD) and so structure the whole namespace. In this debate the "classic" understanding of domains evolved and is still influencing today's Internet structure and development.[22] The goal was to predefine as less implicit semantics in the tree as possible and leave it to the administrator of a zone how to organize his domain. Slightly different from the initial definition [RFC920] the Internet Assigned Numbers Authority (IANA) only distinguishes the following 3 groups of TLDs:

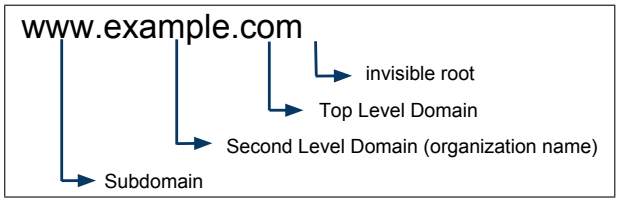

Fig. 1. Structure of Domain Names

- Infrastructure TLDs (iTLD)
- Generic TLDs (gTLD)
- Country-code TLDs (ccTLD)

Infrastructure TLDs The only 2 infrastructure TLDs are the never used .root and .arpa, used exclusively for infrastructure purposes, like reverse domain name resolution (to identify a domain name of a given IP-address). The reserved TLDs .test .example .invalid .localhost [RFC2606] are not really existing but can also be classified here.

Generic TLDs The generic TLDs should separate the namespace into very general categories, free of undesirable semantics. The initial set of gTLDs defined in October 1984 was:[RFC920]

- .edu: Education
- .com: Commercial
- .org: Organization
- .gov: Government (redefined as US Only in 1994 [RFC1591])
- .mil: Military (redefined as US Only in 1994 [RFC1591])
- .net: Internet Service Providers (not mentioned, but then created with the others)
- .int: International organizations (was mentioned under "Multiorganizations" and then created in 1988)

Despite their originally specified goals, with the upcoming of the World Wide Web in 1994 the com, net and org TLDs were opened for use for any purpose. The others still require proof of eligibility. Eventually the mass of registered domain shifted rapidly from the US government and education domains (.mil, .gov, .edu) to these freely available domains (.com, .net, .org) as shown in Figure 2. The total number of registered domains still increases continuously as shown in Figure 3.

The initial assumption was that every organization able to run a computer connected to the Internet will fit into one of these gTLD categories. Meanwhile lots of other gTLDs have been created (like .info and .biz shown in Figure 2), to meet the rising demand for more specific TLDs. The topic of new TLDs is discussed in more detail in chapter 4.

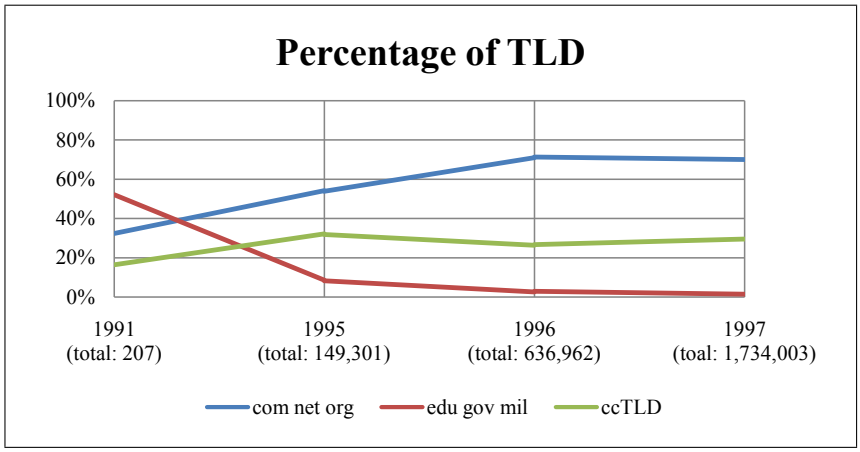

Fig. 2. Absolute number and percentage of SLD by TLD type, 1991-1997 [3]

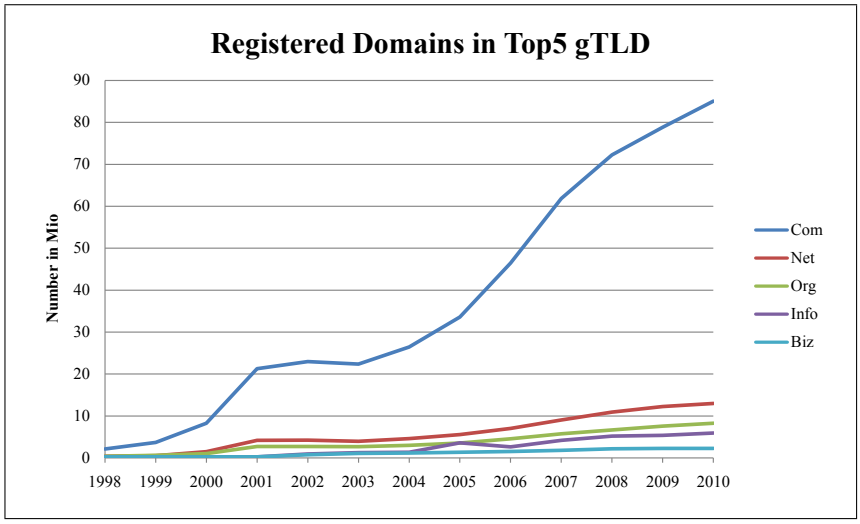

Fig. 3. Top 5 gTLD in terms of registered domains [9] [34]

Country-Code TLDs According to J. Postel - long time director of the IANA - the country specific TLDs were an afterthought to the gTLDs, to offer special domains to people from different countries.[3] Based on the country code list, defined in ISO 3166 and maintained by an agency of the United Nations, countries and regions can obtain their own top level domain. This list was chosen, because *"The IANA is not in the business of deciding what is and what is not a country"* [47].
Figure 4 displays the ccTLDs with the most registered domains, dated to July 2008, when China replaced Germany on the top position.

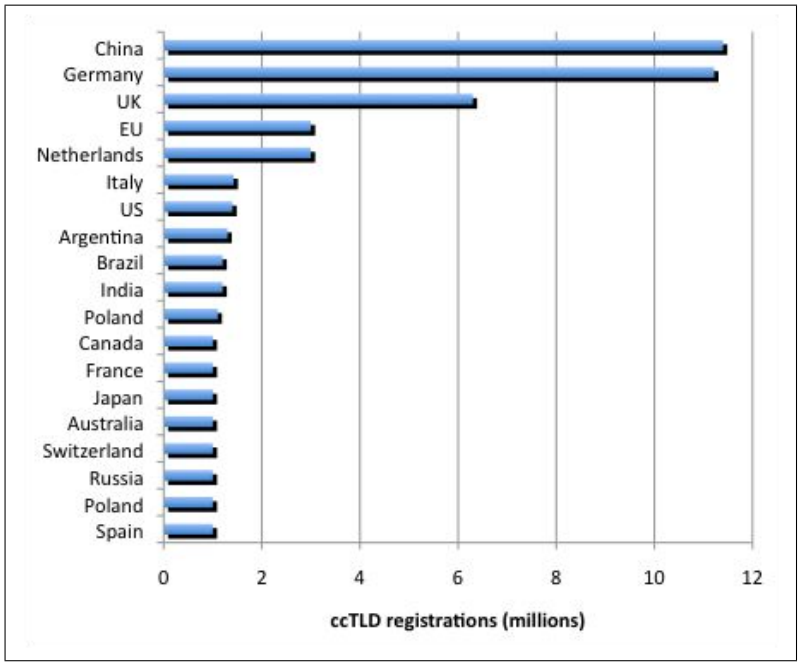

Fig. 4. ccTLD Registration in Millions

Second Level Domain Under the each TLD the administrator can define his own scheme how to structure his zone and redistribute zones. Under some TLDs it is possible to obtain a SLD directly, like in Germany (.de), France (.fr) or under .com, whereas under other TLDs another level with certain naming conventions exists. For example in Australia (.au) or Great Britain (.uk) it is only possible to get a third level domain, eg: .ac.uk (academic), .co.uk (commercial) and .gov.uk (governmental)

Resource Records The so called resource records (RR) are data elements used to hold information associated with a domain name (a tree node). Each record has among different other fields a "type"-field, defining the kind of information to be held and an "rdata"-field, containing the actual information. [RFC1034]

Resource Record *(Name TTL CLASS TYPE RDATA)*	**Explanation** *(General structure)*
www.example.com. 3600 IN **A** 172.27.171.106	**IPv4-Adress for** a hostname
example.com. 3600 IN **MX** mail.example.com.	**Mail Exchange Server** for a dns zone
example.com. 1800 IN **NS** ns.example.com.	**Name Server** which is the authority for a dns zone
example.com. 3600 IN **CNAME** example.net.	**Alias** for existing hostnames

Table 1. Examples of resource records

2.3 Name Servers

The structure of the DNS tree and the RRs are stored within a database highly dispersed over millions of servers worldwide.[26] These name servers have complete information on a subset of the tree - a DNS zone - for which they are the authority. Furthermore they temporarily provide data formally requested from other name servers (Cache Data) or delegate to another name server, which is the authority for a particular zone.[RFC1034] The root zone will now be described in more detail, whereas most facts also count for servers on lower levels of the hierarchy.

Root Servers The zone on the top of this hierarchy, is the root zone, which is basically served by 13 different root servers, named with letters from A - M. This eliminated a single point of failure, distributes load and increases the reliability of the DNS. By intention these servers are operated by 12 different organizations:[24]

- US based private companies: VeriSign (A, J), Cogent Communications (C)
- US universities: University of Southern California (B), University of Maryland College Park (D)
- US government: NASA (E), U.S. Army (H), U.S. Department of defense (G)
- US non-profit organizations: ISC (F), ICANN (L)
- International non-profit organizations: Autonomica (I, Sweden), WIDE Project (M, Japan), RIPE NCC (K, Netherlands)

The A root server is the *Primary Name Server* (master) of this virtual cluster, the others are called *Secondary Name Server* (slaves). The secondaries fetch their information from the primary, via a zone-transfer - or if just the changes

of the zone are updated, an incremental zone transfer [RFC1995]. However all secondaries are regarded as qualitatively identical and also deliver *authority data* - in opposite to *Cache Data* which can be outdated. On lower levels a name server can be an authority for more than one zone and so act as primary and secondary name server at the same time.
After several root server attacks [38] and considering the growth, the worldwide distribution of the Internet and the importance of the root zone, it became obvious that 13 root servers (10 located in the USA) are not sufficient anymore. Due to protocol limitations of the DNS (see next chapter: Resolver) it was not possible to deploy further root servers with new IP-addresses. For this reason all new root servers use a technique called anycast [RFC3258], which is a network addressing and routing scheme whereby many servers can share a single IP-address. The request is then routed to the nearest or best destination. Meanwhile the root zone is served by more than 200 root name servers (see Figure 5) and still new ones are added frequently. [11] Authoritative name service providers

Fig. 5. Image of root server destribution [24]

on lower levels of the namespace (eg: dnsMadeEasy, communityDNS, dynDNS) and recursive DNS services (called *caching only name servers* such as OpenDNS or Google Public DNS) also uses IP anycast environments to increase query performance and redundancy.
For TLDs it's also required to run at least 2 locally independent name servers and none of them is on an average load above 1/3 of the peek. [RFC2182] The DeNIC (Authority for the German .de ccTLD) for example is running name servers in 13 locations worldwide, answering more than seven billion queries every day - or 6000 per seconds - per location. [40]

2.4 Resolver

Beside the namespace and name servers, the last component of the DNS are resolvers. They are software components running on a client computer used to extract information from name servers. Resolvers must be able to access at least one name server and can then query this server in 2 modes: [RFC1034]

- iterative mode: The name server is either responding with its own authoritative data or with a reference to another name server, which the resolver then has to ask.
- recursive mode: In this mode the name server is asking other name servers for the answer to a resolvers query.

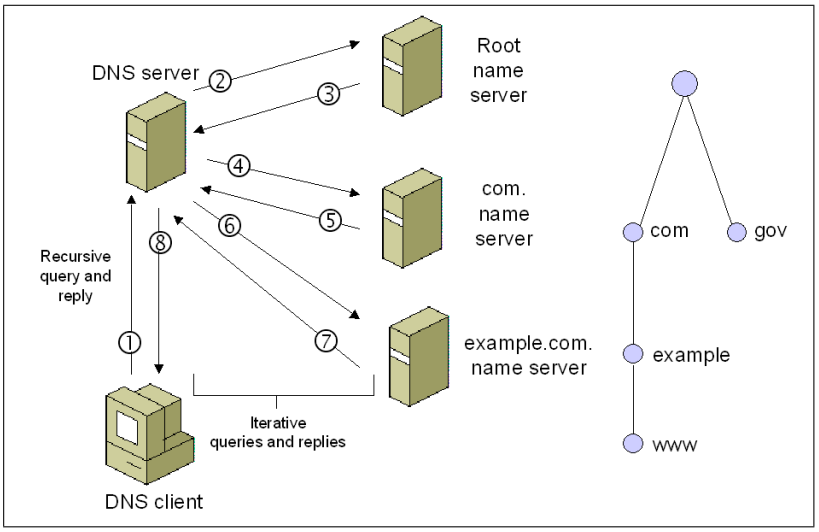

Fig. 6. Schema of dns request [8]

Using a DNS resolver every resource record can be requested. Usually DNS requests are performed over the connectionless UDP network protocol (port 53) to minimize network load and so maximize the speed. These packages have a standard length of 512 byte, causing the limit of 13 DNS Server IP-addresses per DNS zone. Queries using TCP are also possible, but significantly slower.
Well known programs to perform a dns lookup are nslookup, host and dig.

3 Stakeholders

In the previous chapter, only technical aspects and the resulting structure of the DNS namespace were described. The hierarchical layout shall now be described further, by outlining institutions from top (the root of the DNS) to bottom, which are involved in using, controlling, maintaining and refining the DNS.

3.1 The Internet Corporation for Assigned Names and Numbers

The Internet Corporation for Assigned Names and Numbers (ICANN) is a private, non-profit organization which was formed in 1998 in order to have a dedicated institution which aims at keeping the internet "secure, stable and interoperable" [54]. ICANN is one of the most important and most powerful institutions in the DNS hierarchy. Thus, the next paragraphs will summarize the historical events leading to the ICANN in its current form and with its current responsibilities.

History In the early days of the DNS, in 1985, it was the Stanford Research Institute (SRI), funded by the US Department of Defence, which handled the registration of second-level domains (SLD) for free. Later on, this task was moved to Network Solutions Inc. (NSI), which started charging $50 per domain when demand grew in the mid 1990s. Throughout the early 1990s the "A" Root Server was also administered by the NSI, even though Jon Postel himself and the IANA kept the actual authorization and control over the contents of the root. At that time few of the thirteen root server operators had any formal contracts with NSI or any US government agency.
In 1996 the Internet Ad Hoc Committee (IAHC) was formed to deal with the pressing question of whether to add new TLDs to the root or not. (see chapter 4 for more information) First official proposals reached from 7 over 150 to 300 new TLDs.[15] [22] These were objected by several Internet interest groups mostly due to organizational concerns, regarding the centralized control of J. Postel and the IANA (*"What happens if Jon Postel gets hit by a beer truck?"* [5]). It became apparent, that J. Postel's informal leadership had to be replaced by a more formal Internet governance.
As a response, the US Government issued a request for comments (RFC) January 1997, in which "desirable characteristics of Internet governance and the domain name space"[5] were to be discussed. The follow up to the RFC was, the US Government's Green Paper in 1998 which yet again proposed to form a non-profit organization to control domain names, while *"operat[ing] as a private entity for the benefit of the Internet as a whole"* [5]. The paper stressed that this organization *"must derive legitimacy from the participation of key stakeholders"* [5] and also it implied the governments role in overseeing policy making. Four months later, the subsequent White Paper was released. In contrast to the Green Paper it no longer suggested very concrete necessary steps. Important policy questions were left open to the prospective organization's board. This approach pleased

most of the community, since everybody believed, the new formed corporation "would see things their way" [5]. After a period of negotiations in 1998, a set of documents was given to the DOC by Postel, describing them as the consensus of the Internet community. Beside the articles of incorporation, they contained information about board members and an initial set of bylaws for the already established corporation: ICANN. Sadly, John Postel died shortly after. Nevertheless, after some modifications, a Memorandum of Understanding was agreed on, in which ICANN and DOC explained to work together on moving complete DNS responsibility to a non-profit organisation, a goal which today is still not completely accomplished. [5]

Functions According to its current bylaws, ICANNs mission *"is to coordinate, at the overall level, the global Internet's systems of unique identifiers"* and *"to ensure the [...] operation of the Internet's unique identifier systems"* [44]. This mainly includes the allocation and assignment of domain names, the coordination of *"operation and evolution of the DNS root"* and the development of policies related to the technical functions of the DNS. [44]
This mission is performed while following a set of core values. These values include the preservation and development of the worldwide function of the Internet, in terms of stability, security and reliability, while recognizing and respecting other responsible parties and their interests and by delegating functions to them. ICANN also tries to incorporate the *"functional, geographic and cultural diversity of the Internet"* [44] by supporting participation of a broad range of entities in decision-making and policy development. It is also stated, that a competitive environment is tried to be promoted where practicable, appropriate and beneficial. Policy development mechanisms are tried to be designed open and transparent. Decisions shall be well-informed and base on expert advice, while most affected entities are part of the policy development process. That way, decisions shall be made objectively and fair. Furthermore, ICANN recognizes, that governments' and public entities' recommendations need to be considered even though ICANN is a private organization. [44]

Structure An important characteristic of ICANN's current structure is the multi stakeholder model. Just as during the formation phase, the corporation today is trying very hard to incorporate as many people in their decision making processes as possible to ensure ICANN's legitimacy. The following image displays the composition of ICANN's board of directors in 2010.
The 21 regular positions of the board are composed of individuals coming from a variety of sources:

- The Address Supporting Organization (ASO)
- The Generic Names Supporting Organization (GNSO)
- The Country Code Names Supporting Organisation (ccNSO)
- The ICANN Nominating Committee
- Technical Liaison Group (TLG)

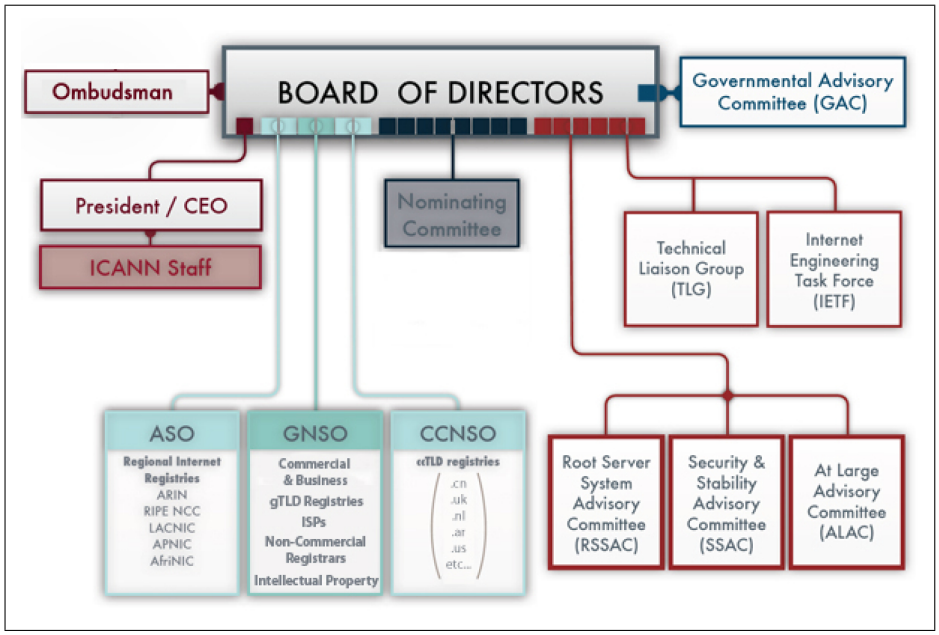

Fig. 7. Current ICANN Stucture

- Internet Engineering Task Force (IETF)
- Root Server System Advisory Committee (RSSAC)
- Security and Stability Advisory Committee (SSAC)
- At Large Advisory Committee (ALAC)

Furthermore, one position is filled by Rod Beckstrom who currently is President and CEO of ICANN and thus represents ICANN's staff. A more detailed description of each group's functions can be accessed via [46] and [44].
According to the current bylaws, ICANNs structure should be reviewed every three years by an independent institution to ensure the purpose of each organization within ICANN and to check whether effectiveness can be improved by changing the structure. [44]

Current Projects ICANNs current topics for 2010 are the introduction of DNSSEC, IDN ccTLDs and the addition of new gTLDs to the root, which the following chapter will explain shortly.

DNSSEC In general, the Domain Name System Security Extensions (DNSSEC) enables users to verify, data they receive from their ISPs DNS servers are identical to the data on the authorized zone root. A first approach to signing was made in 1999 with [RFC2535], whereas the described key management was found to be too complicated [36]. 6 years later, the completely revisited [RFC4033] was released which no longer had these issues . While several ccTLD registries

are already using DNSSEC and signed their zones, ICANN is planning to add DNSSEC to the root zone in FY2010. On January 27th 2010, the first root server started delivering signed responses (i.root-servers.net). After a period of testing whether larger DNS responses (caused by additional signing information) cause problems, it is planned to expand DNSSEC to all the other root servers in the following months [6].

Internationalizing Domain Names In early implementations of the DNS, there was no chance for users from countries using different character sets in their language than ASCII, to utilize these characters in domain names. With the ongoing expansion of the Internet in recent years it became more and more desirable to implement non-ASCII characters. With the introduction of IDNs[RFC3490] in March 2003, the use of Unicode, a much larger set of characters, was proposed. Unicode includes almost every script used in the world today [28]. IDNs are already partly implemented under several SLDs [4], for example the German "Umlautdomains" (www.müller.de). To expand internationalization to TLDs, ICANN launched the IDN ccTLD Fast Track Process on 16 November 2009. It enables countries to register their ccTLDs also in their local scripts. First applicants include Egypt, Saudi Arabia (Arabic) and the Russian Federation (Cyrillic). [50] More information about the process can be found directly at the ICANN website [63].

new gTLDs While DNSSEC is primarily interesting from a more technical point of view, and IDN ccTLD registration is already open, the analysis of the ongoing process of adding new gTLDs holds potential in terms of an economical view. Therefore, section 4 will cover this subject in a more detailed way.

Budgeting The following section shall give a basic understanding of ICANNs Budgeting by examining the financial plans for the fiscal year (FY) 2010 (June 2009 - June 2010). Sources of revenue are examined and the structure of planned expenses will be outlined.
The following numbers give a quick overview to ICANN's financial dimensions: According to ICANN's budgeting framework, revenues for FY2010 will amount to $67,642,000 while expenses are forecasted to be $54,347,000.

Revenues On a high level, revenues are categorized into five different sources as displayed in Table 2

Registrar Fees Companies can apply to ICANN to become accredited Domain Name Registrars, which enables them to perform the registration of domains under a specific set of TLDs. The $30,866,000 include application fees from new registrars, annual accreditation fees from current registrars and transaction fees of $0.20 for each performed registration.

Source	Amount in $
Registrar	30,866,000
Registry	32,153,000
RIR	823,000
ccTLDs	2,300,000
Other	1,500,000
Total	67,642,00

Table 2. ICANN Revenue Sources for FY2010

Registry Fees Opposed to a registrar, a so called Domain Name Registry administers the technical resources for the operation of a specific TLD (the most prominent example is VeriSign, controlling both, .com and .net TLDs). Here contracts signed with different registries differ. Some registries are charged a fixed amount, some pay transaction based fees and for some both is the case. Detailed information about fees can be found in [45] [17].

RIR Fees There are five RIRs (Regional Internet Registries) that manage the distribution of scarce resources of the Internet such as IP numbers, each for a specific geographical space (North America, Latin America, Africa, Europe/Middle East/Central Asia, Asia/Pacific). Each of them is contributing financially to ICANN proportionally.

ccTLD Further, ccTLD registries contribute financially to ICANN. In agreements, many ccTLDs assure different amounts which add up to $2,300,000. Detailed information on these agreements can be found in source [53].

Other In addition, $1,500,000 of revenue comes to ICANN from other sources such as sponsorships or investments made in previous periods.

Expenses There is an amount of $54,347,000 of expenses, forecast by ICANN for FY2010. The budget framework identifies several areas which need funding as described in Table 3.
A major role of FY2010's expenses is the implementation of new technologies as described on page 12. The amount of $8,698,000 contains expenses for new staff, required professional services, and upcoming technical costs.
Beside mentioned special activities, ICANN has to finance its core activities. This involves the financial equipment of IANA, which will grow partly because of technical expansions. Furthermore ICANN needs to address security and stability of the DNS, also regarding new technologies mentioned, and ICANNs legal department (contractual compliance), needs to be funded. Another set of activities resulting from ICANNs international commitments, is setting up meetings and travelling. When added up, almost 25% of ICANNs expenses ($11,458,000) are forecast to be spent on travelling in FY2010. The mentioned constituency support encloses all expenses made to expand and support the ICANN community with its registries and registrars, advisory committees and other stakeholder

Activities	**Budget in $**
New gTLD Implementation and Delegation	7,448,000
IDN Implementation	1,250,000
IANA and Technology Operations	5,079,000
Security, Stability and Resiliency (SSR)	5,483,000
Contractual Compliance	3,219,000
Core Meeting Logistics	5,289,000
Constituency Support	6,272,000
Policy Development Support	5,280,000
Global Engagement and Increasing International Participation	6,781,000
DNS Operations	1,242,000
Community Travel Support	1,467,000
Board Support	2,418,000
Nominating Committee (NomCom) Support	790,000
Ombudsman	451,000
Administrative improvement	1,878,000
Total	**54,347,000**

Table 3. ICANN Expenses for FY2010

groups. In addition, the sum of $5,280,000 is spent yearly to ensure ICANNs processes of policy making are as fair as possible and satisfy community needs. Also, these processes are steadily developed further. ICANNs global engagement includes delivering presentations, providing trainings, and translating documents to the international and multi-lingual stakeholder-base ICANN is currently based on. There is also a traveling support programme, that was established to help needy (future-) stakeholders, who otherwise would be unable to attend ICANN meetings. Therefore $1,467,000 are planned to be used on supporting especially important people for ICANNs volunteer community. Beyond that, the 21 board members are supported in a similar way. Another institution of ICANN is the so called Obudsmann, a one-man-institution accountable for solving disputes over unfair or inappropriate treatment by ICANN. An amount of $451,000 will be spent for his function. Furthermore the so called NomCom (Nominating Committee) has to be supported, which tries to find appropriate members for open positions at ICANNs key structure. Covered are travelling costs, administrative support and professional services needed. Of course, besides all these expenses, ICANN has to take care of the core function of keeping the DNS up and running and therefore spends $1,242,000 on DNS Operations, including the funding of research teams dealing with the progression of DNS. As described above, ICANNs structure is in a steady change and to support the adaption to new tasks and environments a yearly budget of $1,878,000 is determined.
The observing reader may have realized that there is a difference between ICANNs planned income and spendings. This amount of about $7,400,000 does not disappear but is rather added to ICANNs reserve fund. This sum is even below past targets of $10,000,000, mainly because of one-time spendings for gTLD and IDN

projects FY2010. More detailed Information about all revenues and expenses listed here can be found in ICANNs Budget Plan for FY2010 [45].

Problem of Legitimation Despite the fact that since the beginnings, founders have always taken into account that an organization of ICANN's relevance and power has to ensure its own legitimacy in different ways, there have always been critical voices towards ICANN's monopolistic position. [5]
The internationalization of control, especially desired by China, Russia and Brazil, already became a topic during the 2005 World Summit on the Information Society. Since no consensus could be achieved during the summit, as an alternative the Internet Governance Forum (IGF) was brought into being. It was planned to serve as a forum with international participants to discuss Internet Governance related topics. It quickly became apparent that neither China, nor Europe were satisfied by the new forum since it never helped to achieve consensus. As a result the EU proposed a new approach for internationalization by completely privatizing ICANN. The technical responsibilities should be left to ICANN, whereas political operations should be distributed to 12 regional representatives, thus ending the "US hegemony on the Internet". However this approach could be rated as unrealistic, since political and technical decisions can not be as easily separated. [23]
Besides the missing internalization, another issue faces criticism. ICANN's close relationship to the US Department of Commerce (DOC). This relationship is a result of the historical events described previously and is based on a Memorandum of Understanding (MoU) which was last renewed in 2006. At that time it was declared that the DOC's influence on ICANN was reduced and that it is the DOC's intention to make ICANN an independent and reliable organization which represents a variety of interests. As a result ICANN was able to define its goals more autonomously and reporting obligations towards the DOC were reduced. Nevertheless it was observable that US interests were still valued more than European ones. [25] [49]
On September 30th 2009, the collaboration of ICANN and the DOC changed once again, when the so called Affirmation of Commitments was signed. The new paper declares more than ever before ICANN's role as a private non-profit organization which is independent and "not controlled by any one entity". It is stated that the current model of multiple stakeholders is "robust enough to review itself" and thus a reliable platform is provided. [48]
However critics argue, that even with this new arrangement ICANN's weak accountability is still an issue, because decisions made by the Internet community can too easily be ignored. [12]

3.2 Stakeholders on Lower Levels

Of course, when moving down in the DNS tree hierarchy, more stakeholders can be identified. This includes Registries of TLDs, ISPs and of course end users. This chapter will analyze some of the stakeholders, with regard to their respective economical impacts.

Registries As explained in Section 3.1, Registries are institutions which technically administer specific TLDs, one level below the DNS root. They run required servers and change, add and delete entries in their zone. There are several registries which have been accredited by ICANN, some of which administer multiple zones (for example NeuStar Inc., in charge of .us and .biz).

German DeNIC as an Example of a large Registry To give insight on Registries in general, DeNIC located in Frankfurt am Main, Germany is chosen to serve as an example for a ccTLD registry. With about 13,4 mil. registered .de domains, DeNIC is second largest regional registry (see Figure 4). As described in its official statute, DeNIC does not have any intentions on drawing profit from its work and all earnings are used to cover costs and to ensure the organization's existence. This is in compliance to international standards, which also command, that ccTLD operators have to orientate at interests of all Internet stakeholders worldwide. Organizations which fulfill certain requirements may apply for memberships of DeNIC, which allow them to use the internal registration system and thus offer all .de domain related services autonomously. Pricing models of DeNICs end user service DeNICdirect show, that business with end users is not intended at large, but rather members are seen as the main business partners for end users (DeNICdirect charges 58€per year for each domain [42]).
In chapter 3.1, the financial relationships between ccTLDs and ICANN have been addressed shortly. It was stated that usually agreements exist, which regulate payments from registries to ICANN. In DeNICs case, a yearly contribution of $85,000 is agreed on and in addition a variable fee of $0.01 per domain is forwarded. [17]
In 2008, DeNICs total expenses added up to 13,495,000€. The biggest part were personnel expenses in the amount of 6,731,000€, followed by operating costs of 3,929,000€. The remaining spendings were caused by running expenses and depreciations. In contrast, sources of revenue in 2008 amounted to 14,330,000€, where most of the turnovers were generated by DeNIC members, and only 1,020,000€were revenues of DeNICdirect. The rest was other income declared as operating and non-operating. In the end, a surplus of around 507,000€was used for reserve funds. [17] [39] [51] [43]

Unconventional Usage of TLDs When speaking of registries, it is also worth taking a look at unconventional business models of some of them. Whereas usually the purpose of ccTLDs is, to express belonging to a geographical region, some users and registries take advantage of the fact, that two-letter TLDs can form meaningful words or sentences in combination with certain second level domains. There is a large set of "exploitable" ccTLDs which allow these so called domain hacks. For example Polynesian island Tuvalu's .tv is used by television related domain holders, Tonga's .to is used as the English word "to" in domains like go.to and the Federated States of Micronesia's .fm domain is marketed as a TLD for radio and music related websites. [35] Some registries are also aiming on taking advantage of typing errors. This could easily be used to scam users who think they reached the website they intended to. According to McAffee,

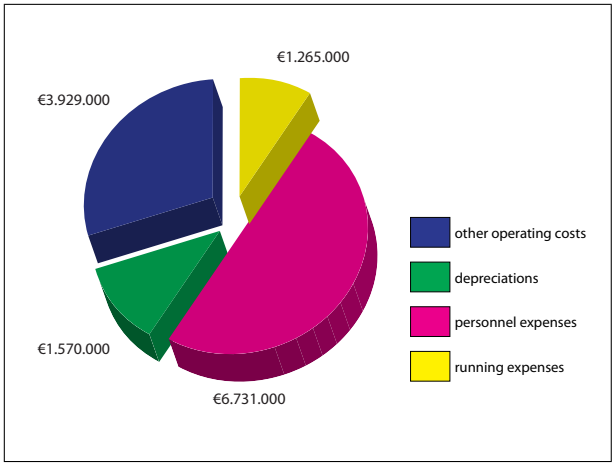

Fig. 8. DeNIC Expenses FY2009

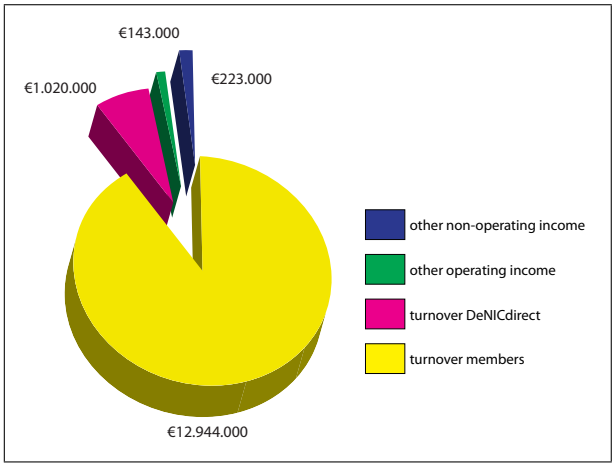

Fig. 9. DeNIC Revenue FY2009

Camerooon has the most dangerous TLD, since .cm is a common typo when entering .com. It is estimated that up to 30% of registered .cm domains are aiming at this effect and thus try to scam people. [30]

Registrars Next to registries, there are registrars which act as the gateway between end users and registries. If a user wants to register a certain domain name he usually approaches a registrar of his choice, accredited by the according registry or ICANN. [41] [55] There might also be a reseller involved in between the end user and the registrar. In many cases registrars and resellers offer multiple services in combination, for example web hosting, server housing etc. in combination with domain administration, or at least closely work together with such organizations. Registrars are free in designing prices for end users, while monthly or yearly fees are usual. So a domain can not be "bought" but is rather "rented" for a specific time. The following shall give a basic idea of pricing: at the time of this writing, renting a .de domain at a large registrar costs about 0.50€a month [66]. The fees registrars pay to registries are often not public as in the case of DeNIC, but other examples can be given. In a recent press release VeriSign announced to increase fees for .com and .net domains to $7.34 and $4.65 respectively [29]. In a recent discussion at ICANNs meeting in Seoul, an issue has been brought up concerning the separation of registries and registrars. This separation is intended by ICANN, but does not seem to work out very well in reality. Therefore, in January 2010, the GNSO council voted, to bring a policy on the way, regulating this issue more effectively. [19]

Internet Service Providers Internet Service Providers (ISPs) in the context of this work, enable their users to connect their computers and other devices to the Internet. Usually, ISPs therefore also provide their users with DNS servers. Of course the mapping information these servers hold, need to mirror information of servers on higher levels to ensure consistency all over the Internet. Aside from their standard business models, ISPs have found another way of earning profit with DNS servers. By so called typo squatting, ISPs detect whenever users try to access a non existing domain name. Instead of delivering a so called NXDOMAIN ("no such domain name exists") response, the user is redirected to a specified page where usually advertisements and search options are displayed. As it is easy to identify the domain name a user initially tried to reach, one can also easily incorporate this information into the "landing page" and thus display individual advertisement. That way the spaces "in between" registered domain names, namely non registered domain names which obviously form a much larger set, provide a very high value to businesses. [13]

Governments The DNS has also been the target of government activities recently. Keeping in mind how the DNS works, it becomes apparent that it would be an easy task to incorporate censorship measures into the technical infrastructure [20]. Governments like China, force ISPs to install so called DNS tampering

mechanisms, which detect whenever users try to access domains, which for any reason are found to be inconvenient by the government. DNS information is altered "on the way", thus assigned IP addresses, CNAMEs and authorative servers are changed and resources can no longer be reached [2].
Additionally, not only the U.S. Department of Commerce influences ICANN through their close relationship to each other. For example, also the Department of Homeland Security showed interest in the DNS when first discussions about DNSSEC were held in 2007. [18]

End Users The by far largest group of stakeholders of the DNS are of course corporate and private end users. They utilise the DNS to access services on the Internet and register domains via different registrars all over the world.
As stated in previous chapters, users are assigned DNS servers from their ISPs, but are free to change these assignments to alternative DNS servers. They are also exposed to fraudulent use of the DNS. Malicious programs can for example alter a users hosts file, which overrides mappings of DNS servers locally. That way, users could be redirected to malicious websites without their knowledge. Especially in home banking environments this can be critical.
End users, registrars, registries and the ICANN, form the four main participants of Figure 10, which shall summarize sources and destinations of fees during an end user .com domain registration (Note that actual fees may be outdated).
But once a domain is registered, the cycle is not over. Often, domains are sold

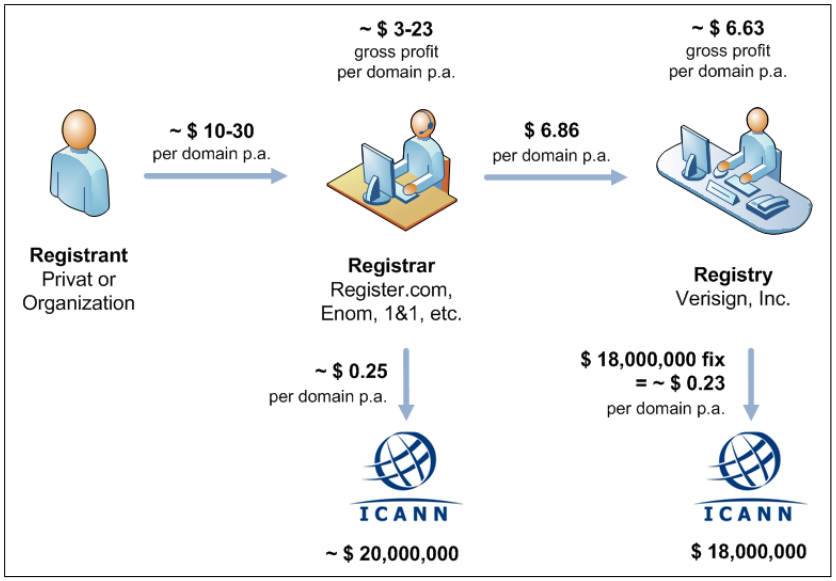

Fig. 10. .com Domain Registration: Where is Money Flowing [17]

afterwards for much higher prices. The fact that a domain name can be worth far more than the actual registration cost has always been ignored by the first-come-first-serve principle. [3] For .de second level domains estimations show, that while the primary market has a yearly revenue volume of around 14,000,000€, the secondary market for domain sales amount to around 30,000,000€[17]. This is the reason for so called "domain squatting", the purchase of second level domains, solely for the purpose of reselling them afterwards for higher prices.

4 Challenge of deploying new TLDs

As described in chapter 3.1 the process of adding new gTLDs is one of ICANNs current main activities. This chapter will describe the development so far, explain the process of obtaining a new TLD and then provide a brief case study of the .berlin TLD application.

4.1 Shortage within the namespace

After initial discussions regarding the separation of the DNS namespace, a common understanding of domains was established, as described in chapter 2. The combination of gTLDs and ccTLDs satisfied all requirements, so that J. Postel said in 1994: *"It is extremely unlikely that any other TLDs will be created"*.[RFC1591]
At the same time the World Wide Web was first perceived in public and due to its ongoing commercialization in the following years, the nature of a domain changed from a technical identifier, invented by scientist to an important economic value for businesses.[7] Even if the DNS theoretically allows more SLDs under each TLD then there a atoms in the universe, a shortage of *sensible* domains occurred. Since many people regarded the root zone as a kind of public good, they started to question the monopolistic control over the root and demanded more TLDs, to solve the shortage.[3]
They were arguing that new gTLDs would ease the problem of name conflicts in the second level by expanding supply and better categorize the namespace. The defenders of the as-is state on the other side argued, that adding new gTLDs would worsen the trademark problems by multiplying the number of domains where speculation and trademark dilution could take place. Furthermore users who are accustomed to the existing set of TLDs would get confused. In fact there is at least no empirical evidence that users benefit substantially from the limitation of numbers of categories in the top level.[3]
Technically the root zone could be expanded infinitely, like any TLD, but it is *"considered undesirable to have enormous numbers (100,000+) of top-level domains for administrative reasons"* like J. Postel wrote in 1997.[21] A newer statement from the ICANN board Member D. Wodelet emphasizes that the root is a scarce resource with a maximum of 5000 TLDs.[31]

4.2 Expanding TLDs

Early Alternatives Since expansions of the TLD namespace did not move forward, several groups emerged, which decided it would be a good choice to establish an alternative to the existing root. The technical requirements to set up such a system are rather manageable, while benefits can be significant. Once the DNS servers are in place, users only have to set their devices to use these servers instead of the ones they are usually assigned by their ISPs.
First attempts to offer alternatives to the main root servers were already made in 1997 when name-space.com calling themselves "the dot everything people" started their services to register domains under all sorts of TLDs in an alternative/additional DNS. It is even speculated, that if some larger ISPs would have additionally pointed to the alternative servers, critical mass would have been reached. As a result "two roots" would have been in place, thus offering the "standard" TLDs plus the additional name-space TLDs [3]. Other approaches include for example RealNames (founded 1997), a Microsoft Internet Explorer extension that would lead users to websites depending on keywords entered in the address bar or AlterNIC and eDNS.
Furthermore there are alternatives that do not aim on expanding or altering the namespace but rather mirror the original root. Founded in 2005, OpenDNS for example aims at providing users with alternative servers to those of ICANN. The main purpose of OpenDNS is stated to be the faster resolving of domain names, which among other fees, is financed by displaying advertisements if a user misspells a domain name. [37] Realizing the importance of the DNS, it was also no surprise that Internet giant Google announced the launch of their own "Google Public DNS" in December 2009. They also claim to increase speeds in resolving Internet addresses, while competitors such as OpenDNS argue it would be naive to believe that this service would benefit the Internet as-is. Google would rather aim on the value of controlling as much of a user's "Internet experience" as possible to further expand their revenues from advertisements. [27] [67]

Experimental phase With the foundation of the ICANN in 1998 (see chapter 3.1) the process of new TLDs was revived.
In 2000 and 2004 the ICANN conducted the first 2 small rounds of adding new TLDs, designed as a real world experiment, in order to seek compromises between all stakeholders and gain process and technical experiences for bigger rounds of TLD expansion. A formal application process with certain *Criteria for Assessing* was established. Summarized a proposal for a new TLD had to met the following requirements:[58]

- Stability
  - Provisions for orderly and reliable operation of the DNS.
  - Prospects for the continued and unimpaired operation of the TLD under all circumstances (contingency plan)
- Business concept
  - Show the market demand and supporting community for the new TLD (feasibility and utility)

  - Provide competitive business and economic models under which TLDs can be operated.
  - Define unchangeable purpose of TLD and prove that the label suggest that use for a large portion of Internet users globally.
- Legal prerequisites
  - Does the proposal provide well-thought-out plan for allocation of names during the start-up phase, an efficient mechanism for resolving domain-name disputes and protects intellectual property and trademark rights?
- Effects on DNS
  - Would the new TLD sensibly add to the existing DNS hierarchy and not create confusion. (semantically "far" enough from existing TLDs)
  - What prospects do the new TLD and registry have for effectively competing with other TLDs and registries.
  - Impact of the new TLD on the operation and performance of the DNS in general and the root-server system in particular

Furthermore an application (for even more than one TLD at once) needed to be backed by sufficient resources and will only be considered if a non-refundable fee of $50.000 is provided.
Until the deadline of the first round in the year 2000, 44 applications have been submitted [59], for a few hundred TLDs like africa, wap, home, cash, dubai, find, health, jazz, software or event.[60] In the end the following TLDs where accepted:

- Sponsored TLDs: .museum .aero .coop
- Unsponsored TLDs: .biz .info .name .pro

An unsponsored TLD is operated under policies established by the global Internet community directly through the ICANN process. Whereas for sponsored TLDs the registrar holds policy-formulation authority, to limit the use of a TLD to a defined purpose or a defined group of stakeholders, like all museums in the world.[61]
Very similar to the process of the first round, within the next phase of TLD expansion in 2004 the following sponsored TLDs have been created: .asia .cat .jobs .mobi .tel .travel .post [62]

Evaluation of the experimental phase After each of the first 2 rounds the ICANN and other researchers evaluated deeply the introduction of TLDs, regarding the process itself, the effectiveness of trademark protection, impacts on market competition and the used criteria for assessment. [56] [57] [32]

Legal Issues: Different ways of allocating domain names ("first come first serve", "round robin", "sunrise period", "intellectual property claim process", "auction of best names" or "reliance on Uniform Domain-Name Dispute-Resolution Policy") have been tested to assure the protection of right of trademark holders and individuals with legitimate interests. It was concluded that there is no general best practice, rather then it depends of the target group and community a TLD is for.

Economic Value: The impact of the new gTLDs on the competition in the market has been marginal, since for most cases a .com or .net domain was still valued higher by domain buyers. In case of .biz it was shown that 74% of registered domains (680,000+ in the study) provide no web content, only error messages or placeholders. Approximately 25% of .biz domains are registered to the same organization that owns the corresponding .com domain. With costs of around $20 the defensive registrations of .biz domains yields payments of approx. $3.4 million per year. This raises serious questions, how sensible the name space was extended. [33]
Other gTLDs have been true success stories, like .cat for the community of Catalan speaking people.[10] For cultural reasons most Catalals refused to register a .es domain and therefore went over to utilize gTLDs or other alternatives like the city of Girona which preferred .gi (ccTLD of Gibraltar). Now .cat with just over 40,000 registered domains is rather small, but is used by lots of major websites as their primary address and so considered as the home of the Catalan language and culture on the Internet. On the one hand .cat is representing a language in a certain region, what somehow contradicts the purpose of ccTLD. On the other hand this example shows clearly, how the name space could be extended in a sensible way for the benefit of the Internet community.

Role of ICANN itself: The ICANN defined its role in this process as a moderating instance, only assuring the compliance with certain criteria in order to keep the DNS stable and secure. Nevertheless one major conflict emerged when the ICANN board of directors approved the application of the adult industry for the gTLD .xxx in 2005, since their application fulfilled every requirement.[14] The ongoing complaints from Iran and Saudi-Arabia, who opposed the creation of a "virtual red light district", were ignored under reference to the freedom of speech and information and by pointing out that the ICANN is not a moral instance. The reason in the end .xxx never went live was eventually a mail from the US department of commerce, which raised a lot of questions regarding the independence the ICANN really has. Different sides saw this as another prove of illegal influence the US government has on the ICANN and the Internet Governance (described in chapter 3).[16] [64]

4.3 Current round with .berlin case study

The evaluation phase has shown, that high demand for new TLDs exists and what kind of TLDs extend the root zone in the best way for the Internet Community. Hence, since 2008 the ICANN is developing an *Applicant Guidebook*[52], which will be a full reworked catalogue of the "Criteria for Assessing" including the detailed description of the process itself. To gain a better understanding of the applicants side of the process, the development of the company .dotberlin GmbH is now retraced. [65]
When the ICANN accepted .cat and .asia in 2004 (the first regional TLDs apart from ccTLDs) the idea emerged to create a .berlin TLD. In preparation of a possible next round of root extension, the dotBerlin GmbH was founded in 2005

as the first initiative for a city TLD worldwide. The vision is to give Berliners, their locations, their companies, their organisations and local authorities a Berlin identity in the Internet. DotBerlin is aiming to strengthen the feeling of community amongst Berliners, improve communication and business and make interaction easier. Therefore the 3 .dotBerlin employees started with lobby work in Berlin companies and at different ICANN meetings to convince both, the Berlin business society and the international Internet Community about the utility and feasibility of their idea. However the biggest resistance against the plan came from the city itself, which already runs a city portal under www.berlin.de (operated by the private company BerlinOnline Stadtportal GmbH & Co. KG). The Berlin Senate had first to be convinced that the .berlin TLD, will not harm the existing website.
For the next round the ICANN increased the non refundable application fee to $185,000 and also requires higher standards regarding the contingency plan, the financial background and technical ability. These costs and all other expenses already made during the whole process, will sum up to almost 2 mil. € in case of dotBerlin, according to J. Lenz-Hawliczek (Press & Public Affairs dotBerlin). In addition the operation for a TLD will cost yearly at least 150,000€ for the operation of the servers, fees to ICANN and staff.
These costs shall be refinanced via yearly fees for registering a .berlin domain of 20-80€. Considering a fee of 50€ and 10,000 registered domains the expenses will amortize in 6-10 years.
With perspectives of "owning an endless property" in the Internet the effort seems lucrative. Furthermore the people behind dotBerlin also offer their gained experience via a consulting company (called dotZone) to others, mainly major German companies, which plan to acquire their own TLD.
During the work on this paper, for the surprise of its authors, a new company with the same goal as dotBerlin was founded, called UniteBerlin. Behind this company is Minds & Machines LLC which operate with their software over 20 TLD since more then 10 years. Its team consists of world wide known and respected domain experts. The company is financially well positioned and plans to offer a price comparable to .de registrations. Furthermore the city of Berlin of course appreciates the competition, since this overs them choice and a better negotiating position. (according to Interview with Caspar von Veltheim, founder of uniteBerlin)
So it will be very interesting to see how ICANN will decide in this case.
Regardless of the high obstacles for an application, it is expected that hundreds of applications will be submitted for:

- language TLDs: dotcym.org (Welsh), puntogal.org (Galician), dotsco.org (Scottish)
- city TLDs: dotparis.net, pointque.org, dottokyo.com, dotlondon.net
- brand TLDs: dotdisney.com, dotyahoo.com
- gTLDs: music.us, dothotel.com, dotmed.com

The actual application phase is planed to start in the end of 2010 - with first new TLDs online in 2011. So a lot of interesting developments can be expected

in this area.
. . . or as the ICANN stated: *"Launching a new gTLD is not for the faint of heart. The experiences of the TLDs that have done it already, and the wisdom the community has a whole as gained, should provide valuable assistance to those TLDs that follow."* [56]

5 Conclusion

As seen the DNS is an evolving system in the middle of many stakeholders with diverging interests, especially from an economical point of view. The DNS started as a system for a very small group of users, serving a set of less than 100 computers in 1984. Meanwhile, hundreds of millions of computers and users rely on the DNS, which proved to be extremely scalable. So from a technical perspective the DNS can be considered a success story.
However, as described in this work, with the rise of the World Wide Web the importance of the DNS grew and managerial problems emerged. Thus, the development of ICANN, involving all important stakeholders in policy making was a very reasonable action. To institutionalize ICANN as a non profit organization, independent from the US government further increased its legitimacy. So the balance of interests is ensured in large parts, whereas due to many possibilities of participation and the emphasis on fairness, processes are slow.
Further, it is remarkable, that the amount of money spent to ensure the operation of the DNS at all levels is rather small when compared to the value businesses and users obtain from its proper function. Economical analysis of the DNS identifed not only the leverage of a variety of services but also direct value generated, for example by renting domain names. This value is mainly important to end users and registrars, since registries usually are non-profit organizations as well. The delegation of authority for zones is an important tier of keeping the DNS stable.
Recent developments of expanding the TLD structure are appreciated by many stakeholders. This development is likely to continue in the next years, which offers chances for future research. The utility of new TLDs needs to be analysed regarding the impact on the DNS namespace and the sustainable value for end users. As only an overview of economical situations was given, more detailed inspections could be made for each of the stakeholders.
Overall the DNS, its structure and its stakeholder will be a subject of debate and change in coming years, which should be followed closely.

References

1. Hardie, T. (Nominum, Inc.): Development of the Domain Name System Proceeding of SIGCOMM '88 (1988)
2. Lowe, G., Winters, P., Marcus, M. L.: The Great DNS Wall of China (2007)
3. Mueller, M.: The battle over Internet Domain names Telecommunication Policy, Vol. 22, No. 2, pp. 89-107 (1998)
4. Shim, S. J.: Internationalized access to domain names: a review of methods and issues Online Information Review, Vol. 31 No. 3, pp. 290-299 (2007)
5. Weinberg, J.: ICANN and the Problem of Legitimacy, Duke Law Journal, Vol. 50, No. 1, Thirtieth Annual Administrative Law Issue (Oct., 2000), pp. 187-260 pp. 193, 198-212
6. CircleID's internal staff: ICANN Begins Public DNSSEC Test Plan for the Root Zone (2010) http://www.circleid.com/posts/20100127_icann_begins_public_dnssec_test_plan_for_the_root_zone/ Last Accessed: 09-Feb-2010
7. Committee on Internet Navigation and the Domain Name System: Technical Alternatives and Policy Implications Signposts in Cyberspace: The Domain Name System and Internet Navigation National Research Council (2005) http://www.nap.edu/catalog/11258.html Last Accessed: 09-Feb-2010
8. Davies, J.: TCP/IP Fundamentals for Windows: Chapter 8 - Domain Name System Overview (2005) http://technet.microsoft.com/en-us/library/bb727007.aspx Last Accessed: 09-Feb-2010
9. DomainTools, LLC: Domain Counts & Internet Statistics (2010) http://www.domaintools.com/internet-statistics/ Last Accessed: 09-Feb-2010
10. Gerrand, P.: History of the campaign for approval of '.cat' (2006) http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1305/1225 Last Accessed: 09-Feb-2010
11. Gibbard, S. (Packet Clearing House): Geographic Implications of DNS Infrastructure Distribution The Internet Protocol Journal - Volume 10, No. 1 http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-1/101_dns-infrastructure.html Last Accessed: 09-Feb-2010
12. Gunnarson, R. S.: ICANN's Weak Accountability Remains a Problem (2010) http://www.circleid.com/posts/icanns_weak_accountability_remains_a_problem/ Last Accessed: 09-Feb-2010
13. Huston, G.: NXDOMAIN Substitution: Good or Evil? (2009) http://www.circleid.com/posts/nxdomain_substitution_good_or_evil/ Last Accessed: 09-Feb-2010
14. ICM Registry Name Reservation: ICANN Approves .xxx Sponsored Top-Level Domain Application (2005) http://www.icmregistry.com/ICMPressRelease.html Last Accessed: 09-Feb-2010
15. International Ad Hoc Committee: Draft Specifications for Administration and Management of gTLDs (1996) http://tools.ietf.org/html/draft-iahc-gtldspec-00 Last Accessed: 09-Feb-2010
16. Kleinwächter, W.: ICANN als Zensor? - Von der virtuellen Straenprostitution zum Online-Rotlichtbezirk? (2007) http://www.heise.de/tp/r4/artikel/25/25088/1.html Last Accessed: 09-Feb-2010
17. Krischenowski, D.: dotBERLIN at ICANN Mexico 2009 - The Big Business Presentation (2009) http://www.slideshare.net/dotberlin/dotberlin-at-icann-mexico-2009-the-big-business-presentation Last Accessed: 09-Feb-2010

18. Kuri, J.: Department of Homeland Security will den Masterschlüssel fürs DNS (2007) http://www.heise.de/newsticker/meldung/Department-of-Homeland-Security-will-den-Masterschluessel-fuers-DNS-163379.html Last Accessed: 09-Feb-2010
19. Neylon, M.: Domain Name Registry and Registrar Separation Now Probably Going to Be a Policy Debate (2010) http://www.circleid.com/posts/20100202_domain_name_registry_registrar_separation/ Last Accessed: 09-Feb-2010
20. OpenNet Initiative, Global Internet Filtering Map http://map.opennet.net/filtering-pol.html Last Accessed: 09-Feb-2010
21. Postel, J.: New Registries and the Delegation of International Top Level Domains (1996) http://userpage.fu-berlin.de/~mr94/dns/stuff/draft-postel-iana-itld-admin-02.txt Last Accessed: 09-Feb-2010
22. Recke, M.: Identität zu verkaufen: Probleme und Entwicklungsoptionen des Internet Domain Name Service Page 8, Page 26 http://duplox.wzb.eu/texte/dns/domains-0.9.0beta.html Last Accessed: 09-Feb-2010
23. Rijgersberg, R.: The US as Keeper of a 'Free' Internet? (2009) http://www.circleid.com/posts/the_us_as_keeper_of_a_free_internet/ Last Accessed: 09-Feb-2010
24. root-servers.org: Distribution of Root Servers (2010) http://www.root-servers.org/ Last Accessed: 09-Feb-2010
25. Schüler, H.-P.: Drei weitere Jahre ICANN und US-Aufsicht über Adressierung im Netz (2006) http://www.heise.de/newsticker/meldung/Drei-weitere-Jahre-ICANN-und-US-Aufsicht-ueber-Adressierung-im-Netz-167292.html Last Accessed: 09-Feb-2010
26. The Measurement Factory: The Measurement Factory DNS Survey, Executive Summary (2009) http://dns.measurement-factory.com/surveys/sum1.html Last Accessed: 09-Feb-2010
27. Ulevitch, D.: Some thoughts on Google DNS http://blog.opendns.com/2009/12/03/opendns-google-dns/ Last Accessed: 09-Feb-2010
28. Unicode, Inc.: Unicode 5.2 Character Code Charts http://www.unicode.org/charts/ Last Accessed: 09-Feb-2010
29. VeriSign, Inc.: VeriSign Announces Increase in .com/.net Domain Name Fees (2009) https://press.verisign.com/easyir/customrel.do?easyirid=AFC0FF0DB5C560D3&version=live&prid=570292&releasejsp=custom_97 Last Accessed: 09-Feb-2010
30. Yunker, J.: The World's Most Dangerous Country Code Top-Level Domains (2010) http://www.circleid.com/posts/20100104_worlds_most_dangerous_country_code_top_level_domains/ Last Accessed: 09-Feb-2010
31. Ziegler, P.-M.: Grünes Licht für neue Internet-Adresszonen (2008) http://www.heise.de/newsticker/meldung/Gruenes-Licht-fuer-neue-Internet-Adresszonen-181073.html Last Accessed: 09-Feb-2010
32. Zittrain, J., Edelman, B. (Harvard Law School): The Top Level Domain Evaluation Project (2002) http://cyber.law.harvard.edu/tlds/ Last Accessed: 09-Feb-2010
33. Zittrain, J., Edelman, B. (Harvard Law School): The Top Level Domain Evaluation Project: Survey of Usage of the .BIZ TLD (2002) http://cyber.law.harvard.edu/tlds/001/ Last Accessed: 09-Feb-2010
34. ZookNIC Inc: History of gTLD domain name growth (2009) http://www.zooknic.com/Domains/counts.html Last Accessed: 09-Feb-2010

35. Wikipedia: Country-code Top-Level Domain http://en.wikipedia.org/wiki/Country-code_top-level_domain#Unconventional_usage Last Accessed: 09-Feb-2010
36. Wikipedia: Domain Name System Security Extensions http://de.wikipedia.org/wiki/Domain_Name_System_Security_Extensions Last Accessed: 09-Feb-2010
37. Wikipedia: Real Names http://en.wikipedia.org/wiki/RealNames Last Accessed: 09-Feb-2010
38. Wikipedia: Root-Nameserver, Ausfallsicherheit und Angriffe http://de.wikipedia.org/wiki/Root-Nameserver#Ausfallsicherheit_und_Angriffe Last Accessed: 09-Feb-2010
39. DENIC Domain Verwaltungs- und Betriebsgesellschaft eG: Tätigkeitsbericht 2008 (2009) http://www.denic.de/denic/aufgaben/taetigkeitsberichte-der-denic-eg.html Last Accessed: 09-Feb-2010
40. DENIC Domain Verwaltungs- und Betriebsgesellschaft eG: Name Server Service of DENIC http://www.denic.de/en/background/name-server-service-of-denic.html Last Accessed: 09-Feb-2010
41. DENIC Domain Verwaltungs- und Betriebsgesellschaft eG: Mitgliederliste http://www.denic.de/denic/mitglieder/mitgliederliste.html Last Accessed: 09-Feb-2010
42. DENIC Domain Verwaltungs- und Betriebsgesellschaft eG: DENIC-Preisliste http://www.denic.de/denic-preisliste.html Last Accessed: 09-Feb-2010
43. DENIC Domain Verwaltungs- und Betriebsgesellschaft eG: Statut der DENIC Domain Verwaltungs- und Betriebsgesellschaft eG http://www.denic.de/denic/mitglieder/statut-der-denic-eg.html Last Accessed: 09-Feb-2010
44. ICANN: Bylaws For Internet Corporation For Assigned Names And Numbers (2009) http://www.icann.org/en/general/archive-bylaws/bylaws-27aug09.htm Last Accessed: 09-Feb-2010
45. ICANN: Proposed Framework for FY10 Operating Plan and Budget (2009) http://www.icann.org/en/planning/ops-budget-framework-10-en.pdf Last Accessed: 09-Feb-2010
46. ICANN: Structure http://www.icann.org/en/structure/ Last Accessed: 09-Feb-2010
47. ICANN: Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation) (1999) http://www.icann.org/en/icp/icp-1.htm Last Accessed: 09-Feb-2010
48. ICANN: The Affirmation of Commitments What it Means (2009) http://www.icann.org/en/announcements/announcement-30sep09-en.htm Last Accessed: 09-Feb-2010
49. ICANN: ICANN's Major Agreements and Related Reports http://www.icann.org/en/general/agreements.htm Last Accessed: 09-Feb-2010
50. ICANN: IDN ccTLD Fast Track String Evaluation Completion (2010) http://www.icann.org/en/topics/idn/fast-track/string-evaluation-completion-en.htm Last Accessed: 09-Feb-2010
51. ICANN: DeNIC Agreement http://www.icann.org/en/cctlds/de/denic-icann-letters-31may06.pdf Last Accessed: 09-Feb-2010
52. ICANN: New gTLD Program: Applicant Guidebook (2010) http://www.icann.org/en/topics/new-gtlds/dag-en.htm Last Accessed: 09-Feb-2010
53. ICANN: ccTLD Agreements http://www.icann.org/en/maps/cctld-agreements.htm Last Accessed: 09-Feb-2010
54. ICANN: About http://www.icann.org/en/about/ Last Accessed: 09-Feb-2010

55. ICANN: ICANN-Accredited Registrars http://www.icann.org/en/registrars/accredited-list.html Last Accessed: 09-Feb-2010
56. ICANN: Comprehensive Evaluation of the Introduction of the .aero, .biz, .coop, .info, .museum, .name and .pro gTLDs (2004) http://www.icann.org/en/announcements/announcement-31aug04.htm Last Accessed: 09-Feb-2010
57. ICANN: Final Report - Introduction of New Generic Top-Level Domains (2007) http://gnso.icann.org/issues/new-gtlds/pdp-dec05-fr-parta-08aug07.htm Last Accessed: 09-Feb-2010
58. ICANN: Criteria for Assessing TLD Proposals (2000) http://www.icann.org/en/tlds/tld-criteria-15aug00.htm Last Accessed: 09-Feb-2010
59. ICANN: New TLD Program Application Process Archive http://www.icann.org/en/tlds/app-index.htm Last Accessed: 09-Feb-2010
60. ICANN: TLD Applications Lodged (2000) http://www.icann.org/en/tlds/tld-applications-lodged-02oct00.htm Last Accessed: 09-Feb-2010
61. ICANN: Top-Level Domains (gTLDs) http://www.icann.org/en/tlds/ Last Accessed: 09-Feb-2010
62. ICANN: Information Page for Sponsored Top-Level Domains(2004s) http://www.icann.org/en/tlds/stld-apps-19mar04/ Last Accessed: 09-Feb-2010
63. ICANN: The IDN ccTLD Fast Track Process is Open http://www.icann.org/en/topics/idn/fast-track/ Last Accessed: 09-Feb-2010
64. ICANN Forum: Public Discussion on .xxx TLD http://forum.icann.org/lists/stld-rfp-xxx/ Last Accessed: 09-Feb-2010
65. dotBERLIN GmbH: http://www.dotberlin.de Last Accessed: 09-Feb-2010
66. Strato Website http://www.strato.de/domains/index.html Last Accessed: 09-Feb-2010
67. OpenDNS Website www.opendns.com Last Accessed: 09-Feb-2010
RFC226. Karp, P. (MITRE): Request for Comments 226: Standardization of Host Mneumonics Network Working Group, (20 September 1971) http://www.ietf.org/rfc/rfc226
RFC805. Postel, J. (ISI): Request for Comments 805: Computer Mail Meeting Notes Network Working Group, (8 February 1982) http://www.ietf.org/rfc/rfc805
RFC819. Postel, J. (ISI), Zaw-Sing, S. (SRI): Request for Comments 819: The Domain Naming Convention for Internet User Applications Network Working Group, (August 1984) http://www.ietf.org/rfc/rfc819
RFC920. Reynolds, J. (ISI), Postel, J. (ISI): Request for Comments 920: Domain Requirements Network Working Group, (October 1984) http://www.ietf.org/rfc/rfc920
RFC1034. Mockapetris, P. (ISI): Request for Comments 1034: DOMAIN NAMES - CONCEPTS AND FACILITIES Network Working Group, (November 1987) http://www.ietf.org/rfc/rfc1034
RFC1591. Postel, J. (ISI): Request for Comments 1591: Domain Name System Structure and Delegation Network Working Group, (March 1994) http://www.ietf.org/rfc/rfc1591
RFC1995. Ohta, M. (Tokyo Institute of Technology): Request for Comments 1995: Incremental Zone Transfer in DNS Network Working Group, (August 1996) http://www.ietf.org/rfc/rfc1995
RFC2182. Elz, R. (University of Melbourne), Bush, R. (RGnet, Inc.), Bradner, S. (Harvard University), Patton, M.: Request for Comments 2182: Selection and Operation of Secondary DNS Servers Network Working Group (July 1997) http://www.ietf.org/rfc/rfc2182

RFC2535. Eastlake, D. (IBM): Request for Comments 2535: Domain Name System Security Extensions Network Working Group (March 1999) http://www.ietf.org/rfc/rfc2535

RFC2606. Eastlake, D., Panitz, A.: Request for Comments 2606: Reserved Top Level DNS Names Network Working Group (June 1999) http://www.ietf.org/rfc/rfc2606

RFC3258. Hardie, T.(Nominum, Inc.): Request for Comments 3258: Distributing Authoritative Name Servers via Shared Unicast Addresses Network Working Group (April 2002) http://www.ietf.org/rfc/rfc3258

RFC3490. Faltstrom, P. (Cisco), Hoffman, P. (IMC & VPNC), Costello, A. (UC Berkeley): Request for Comments 3490: Internationalizing Domain Names in Applications (IDNA) Network Working Group (March 2003) http://www.ietf.org/rfc/rfc3490

RFC4033. Arends, R. (Telematica Instituut), Austein, R. (ISC), Larson, M. (VeriSign), Massey, D. (Colorado State University), Rose, S. (NIST) Request for Comments 4033: DNS Security Introduction and Requirements Network Working Group (March 2005) http://www.ietf.org/rfc/rfc4033