Recent Developments in the Domain Name System

M. Tariq Banday
P.G. Department of Electronics and Instrumentation Technology
University of Kashmir, India

ABSTRACT
The Domain Name System (DNS) makes it possible to access information from host computers and to send and receive messages anywhere on the Internet. It is a distributed set of databases residing in computers around the world that contain IP address mapped to corresponding domain names. Currently, Internet Corporation for Assigned Names and Numbers (ICANN) manages DNS and designs policies for its operations. Recently, DNS has witnessed phenomenal developments in terms of technical, operational, and managerial decisions which have made significant impact on Internet-related policy issues such as intellectual property, privacy, e-commerce, and cyber-security. This paper surveys remarkable developments that Domain Name System has undergone in recent times. The advancements particularly advancements in the areas of international domain names, managerial decision of expanding generic top-level domain space, deployment of DNSSEC protocol at the root servers, approval of Triple X top-level domain, domain resolution policy, present status of contractual compliance programs and privacy of domain name holders have been presented in detail.

General Terms
Domain Name System, Domain Name, DNS, IP Address, ICANN, IANA

Keywords
Domain Name Distribution; DNSSEC; New gTLD Program, ICANN; Triple X TLD; .XXX top-level domain; ccTLD; IDN; International Domain Names; WHOIS

1. INTRODUCTION
The communications protocol named Internet Protocol (IP) underlying the Internet allows large and geographically diverse networks of computers to communicate with each other instantly and economically over a variety of physical links. An Internet Protocol Address [1] is the numerical address of the form 192.0.43.10 (IP Version 4) or 2001:500:88:200:0:0:0:10 (IP Version 6) by which a location in the Internet is identified. Computers on the Internet use IP addresses to route traffic and establish connections among themselves. E.g. when a request for a Webpage is sent from a client computer system to a Webserver, the client computer includes the IP address of the Webserver. In order to make the identification of destination computer system simple and mnemonic, a Domain Name System (DNS) [2] has been developed which enables to use globally unique easy-to-remember names called domain names for Webpages and mailboxes, rather than long numbers or codes (IP addresses), e.g. www.example.com instead of 192.0.43.10 (IP Version 4) or 2001:500:88:200:0:0:0:10 (IP Version 6). Users can also request resources like Webpages, mailboxes, files, etc. that are available on the server computer by specifying a unique Uniform Resource Locator (URL) which includes a protocol like HTTP, FTP, etc. to be used for accessing that resource. Another benefit of using DNS is that it allows names to be separated from locations thus allowing services and devices to be moved to different network locations, without the need for name change and without any effect on the way users visit or use that website. The purpose of the DNS as depicted by figure 1 is quite simple: it is a service running on different computers that looks up domain names and resolves them into an IP address so that clients that only know the domain names of the servers and not their IP addresses can communicate with them.

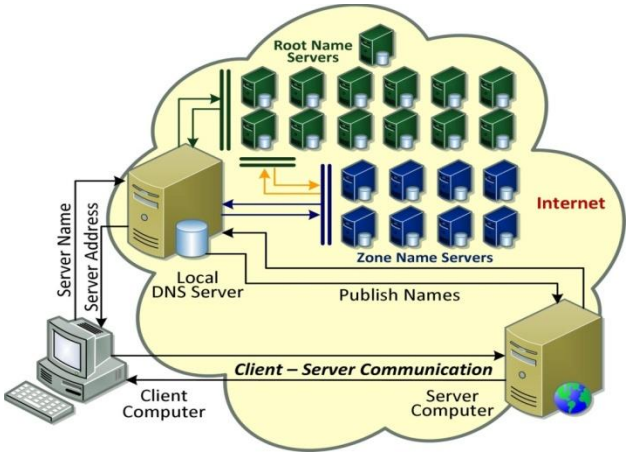

Figure 1: DNS resolving Domain Name to IP Address

2. DOMAIN NAME SYSTEM
The abbreviation DNS is used to describe two related things: the Domain Name System and the Domain Name Service. The domain name system is the distributed database responsible for the domain name-to-IP address conversion, while the domain name service, as the name implies, is the service offered by this system. The DNS infrastructure is made up of computing and communication entities that are geographically distributed throughout the world. This infrastructure comprises of several integrated components including Domain Names, IP addresses, Resource Records, Servers, Resolvers and Communication Protocols managed by structured governing bodies.

Domain Name is a symbolic representation of an object on the Internet from a set of all possible potential names in a particular context and has a meaning within this context. It is a virtual address of some resource, device or service. The domain name space is organized in the form of a hierarchy as shown in figure 2. The topmost level in the hierarchy is the root domain, which is represented as a dot (“.”). The next level in the hierarchy is called the top-level domain (TLD). TLDs are the names at the top of the DNS naming hierarchy. They appear in domain names as the string of letters following the last (rightmost) ".", such as "info" in "www.banday.info". The administrator for a TLD

controls what second-level names are recognized in that TLD. The administrators of the "root domain" or "root zone" control what TLDs are recognized by the DNS. Commonly used TLDs include .COM, .NET, .EDU, .IN, .US, .INFO, etc. There is only one root domain, but there are many TLDs. Each TLD is called a child domain of the root domain. In this context, the root domain is the parent domain because it is one level above a TLD. Each TLD, in turn, can have many child domains. The children of TLDs are called second-level or enterprise-level domains. In a domain name representation, the symbol for the root domain usually is omitted. For example, consider the domain name www.india.gov.in. The rightmost label in this domain name ("in") is a TLD. The next label to the left ("gov") is the second-level or enterprise-level domain. The leftmost label ("india") is the third-level domain. The beginning www indicates the host within india.gov.in domain. Often domain name includes a protocol like http, ftp, etc. (http://www.india.gov.in) to be used in accessing the resource from the host. Each label can be a maximum of 63 characters long and the total length of the URL cannot exceed 255 characters. It also is possible to have a fourth-level domain, fifth-level domain, and so forth. Because each of the labels in india.gov.in is called a domain (TLD, second-level domain, third-level domain, etc.), the concatenation of all these labels from the current level to the TLD is a fully qualified domain name (FQDN).

Organizations that register and obtain an enterprise-level domain name often create child domains called sub-domains to properly identify Internet resources associated with their various functional units. To facilitate this grouping, the DNS defines the concept of a zone. A zone may be either an entire domain or a domain with one or more subdomains. A zone is a configurable entity within a name server under which information on all Internet resources pertaining to a domain and a selected set of subdomains is described. Thus, zones are administrative building blocks of the DNS name space just as domains are the structural building blocks. As a result, the term zone commonly is used even to refer to a domain that is managed as a standalone administrative entity (e.g., the root zone, the .com zone).

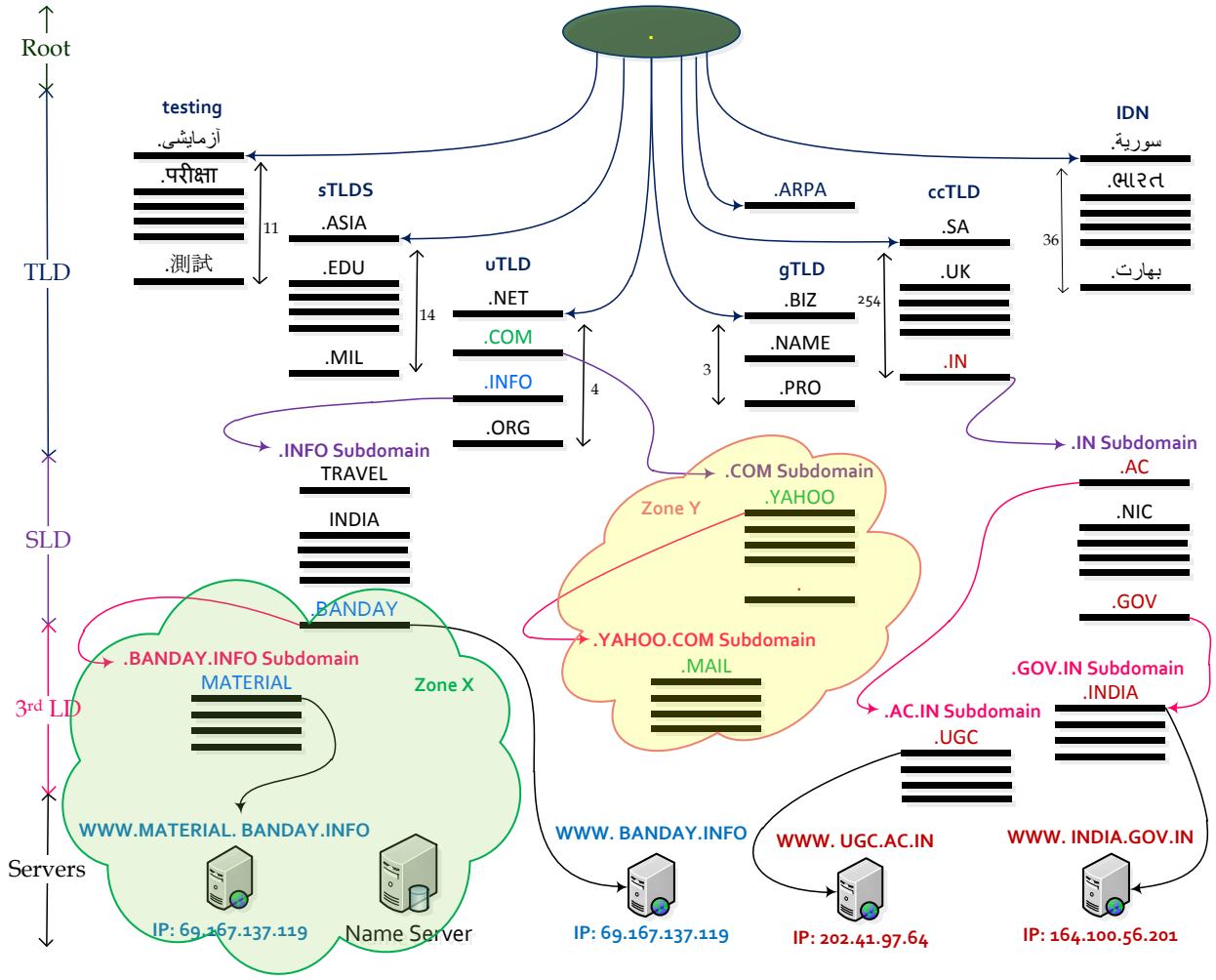

Figure 2: Domain Name Space

As shown in the figure 2, the top level domain .IN has a sub-domain (2nd level domain) .GOV besides others which further has a sub domain (3rd level domain) .INDIA which has a Webserver named WWW serving Webpages to users. The top

level domain .IN also has a sub-domain .AC which further has a sub-domain. UGC which has a Webserver named WWW serving Webpages to users. The sub-domain .BANDAY of top level domain .INFO and its subdomain .MATERIAL form a Zone named Zone X. Similarly, the subdomain .YAHOO and its sub-domain .MAIL form a Zone Y.

3. RECENT DEVELOPMENTS

3.1 Top Level Domain Name Distribution

There is only one root domain. As shown in figure 3, there were 323 TLDs as on July 2011, categorized into the following types: i) testing – reserved for testing internationalised domain names, ii) sponsored top level domain (sTLD) – specialized domains with a sponsor representing a community of interest, iii) unsponsored top level domain (uTLD) – generic domains without a sponsoring organization, iv) generic top level domain (gTLD) – generic domains, v) Country-code top level domains (ccTLDs) – domains associated with countries and territories, and vi) Internationalized top level domains (IDN) – domain names represented by local language characters besides one *arpa* domain reserved exclusively to support operationally-critical infrastructural identifier spaces as advised by the Internet Architecture Board [3]. There are billions of domain names registered as second or lower level domain names.

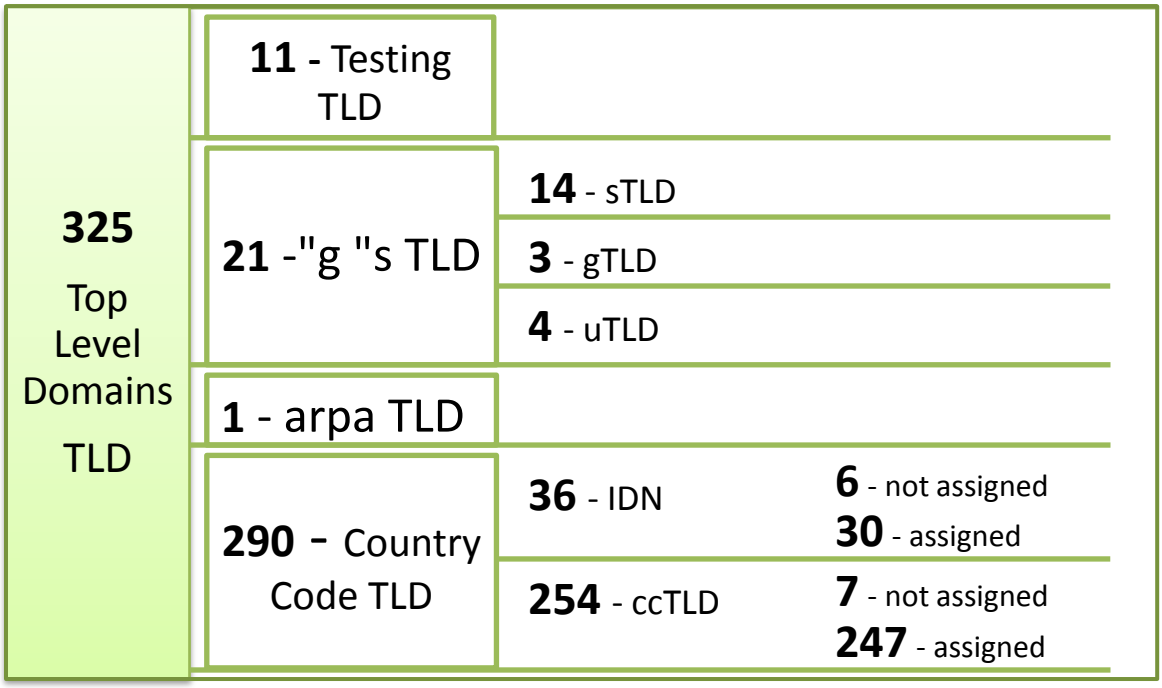

Figure 3: Distribution of Top Level Domains (TLD) as on July 2011

3.2 Internationalized Domain Names

The domain name system (DNS) was originally developed using the ASCII character set, employing only Roman characters and a limited number of symbols. With the global growth of the Internet, there have been increasing calls for *Internationalized Domain Names* (IDNs), particularly support for other character sets in the top level of the DNS. ICANN has approved providing of Internationalized Domain Name (IDN) [4] which are top level domain names that include characters used in the local representation of languages that are not written with the twenty-six letters of the basic Latin alphabet "a-z". An IDN can contain Latin letters with diacritical marks (such as accents) or may consist of characters from non-Latin scripts such as Arabic or Chinese. IDN top-level domain names offer many new opportunities and benefits for Internet users around the world by allowing them to establish and use top-level domains in their native languages and scripts. ICANN is operating an IDN ccTLD Fast Track Process that enables countries and territories that use languages based on scripts other than Latin to offer their users domain names in non-Latin characters. These IDN ccTLDs is available only to the governments and administrations of countries and territories listed in the ISO 3166-1 standard, or their designated representatives or operators. There are a number of string requirements for IDN ccTLDs to be delegated through the process, one of which is demonstration that the IDN ccTLD constitute a meaningful representation of the corresponding country or territory name.

This year ICANN approved delegation of seven internationalized county code domain names to National Internet Exchange of India (NIXI) [5]. These delegated IDN ccTLDs besides previously delegated .IN domain are:

a) The string "भारत", as represented in ASCII-compatible encoding according to the IDNA specification as "xn--h2brj9c". The individual Unicode code points that comprise this string are 092D 093E 0930 0924. The string is expressed in Devanagari script, and in Hindi language.

b) The string "بهارت", as represented in ASCII-compatible encoding according to the IDNA specification as "xn--mgbbh1a71e". The individual Unicode code points that comprise this string are U+0628 06BE 0627 0631 062A.

The string is expressed in Arabic script, and in Urdu language.

c) The string "ಭಾರತ್", as represented in ASCII-compatible encoding according to the IDNA specification as "xn--fpcrj9c3d". The individual Unicode code points that comprise this string are U+0C2D 0C3E 0C30 0C24 0C4D. The string is expressed in Telugu script, and in Telugu language.

d) The string "ભારત", as represented in ASCII-compatible encoding according to the IDNA specification as "xn--gecrj9c". The individual Unicode code points that comprise this string are U+0AAD 0ABE 0AB0 0AA4. The string is expressed in Gujarati script, and in Gujarati language.

e) The string "ਭਾਰਤ", as represented in ASCII-compatible encoding according to the IDNA specification as "xn--s9brj9c". The individual Unicode code points that comprise this string are U+0A2D 0A3E 0A30 0A24. The string is expressed in Gurmukhi script, and in Punjabi language.

f) The string "இந்தியா", as represented in ASCII-compatible encoding according to the IDNA specification as "xn--xkc2dl3a5ee0h". The individual Unicode code points that comprise this string are U+0B87 0BA8 0BCD 0BA4 0BBF 0BAF 0BBE. The string is expressed in Tamil script, and in Tamil language.

g) The string "ভারত", as represented in ASCII-compatible encoding according to the IDNA specification as "xn--45brj9c". The individual Unicode code points that comprise this string are U+09AD 09BE 09B0 09A4. The string is expressed in Bangla script, and in Bengali language.

The Tamil string is pronounced "India", with the remainder of the strings pronounced "Bharat". Each has a meaning equivalent to "India". Once the Indian-language domain names start rolling out, Internet users can register their website addresses in Indian scripts like بھارت.ووبانڈے. However, Indian language scripts are complex and have some issues with spellings as they can be written in different ways which needs to be solved to make efficient use of delegated IDNs. Multilingualism is a very complex issue as there are formidable technical, administrative and security challenges like operating system and browser compatibility, hardware compatibility, spelling standardization, etc. involved in it [6].

3.3 ICANN New gTLD Program

Promoting competition in the domain name marketplace ICANN, has decided to give expansion to the generic top-level domain (gTLD) space by allowing any established entity located anywhere in the world to apply to form and operate a new gTLD Registry [7]. The application period will be open from 12 January to 12 April 2012. Currently organizations and individuals around the world can register second-level and, in some cases, third-level domain names. The application for a new gTLD is a much more complex process. An applicant for a new gTLD is, in fact, will be applying to create and operate a registry business supporting the Internet's domain name system. This will involve a number of significant responsibilities, as the operator of a new gTLD is running a piece of visible Internet infrastructure. The delegation of new gTLDs will potentially change the way people find information on the Internet and how businesses plan and structure their online presence.

In the process of creation of new gTLDs, ICANN has adopted the following mechanism to protect the rights of trademark holders:

a) An objection-based process – It will enable rights holders to demonstrate that a proposed gTLD would infringe their legal rights. In the event that the legal rights objection is successful the application will not proceed.

b) Rights Protection Mechanism - Applicants for new gTLDs will be required to describe in their applications the rights protection mechanism, which must meet certain minimum standards, they propose for second-level registrations.

c) UDRP - All new gTLDs must ensure that second-level registrations are subject to ICANN's Uniform Domain Name Dispute Resolution Policy (UDRP) (http://www.icann.org/en/udrp/), a process that has worked well to protect rights for many years.

Besides these, ICANN is working with the trademark community to find additional solutions to potential issues for trademark holders in implementing new gTLDs which include a trademark clearinghouse, the uniform rapid suspension system (URS), and a trademark post delegation dispute resolution procedure (PDDRP).

The Applicant Guidebook and other material have been uploaded by ICANN at http://www.icann.org/en/topics/new-gtlds/dag-en.htm that demonstrates step-by-step procedure for new gTLD applicants. It specifies what documents and information are required to apply; the financial and legal commitments; and what to expect during the application and evaluation periods.

ICANN has initiated a global campaign about the change in Internet names and to raise awareness of the opportunities afforded by new gTLDs. ICANN is launching a communication campaign from September 2011 to raise global awareness about gTDL program and has also asked community members to recommend events for its wider promotion and for possible participation by ICANN's in these events. Meanwhile ICANN is preparing multilingual material that can be used during this campaign [8].

Recent months have witnessed a growing demand from some major corporations for withdraw of new gTLD program initiated by ICANN [9]. According to the Interactive Advertising Bureau (IAB) and Association of National Advertiser's, major corporations will be forced to buy domain names that cover their brands like .verizon or .facebook in order to prevent cyber squatters from grabbing them first. Given that applications include a heavy fee, which could be an expensive undertaking, IAB has asked ICANN to abandon the plan.

3.4 Deployment of DNSSEC at the Internet's Root

DNS is a critical infrastructure service that supports the Internet and corporate networks to locate other computers by name resolution. Web, e-mail, and instant messaging, applications and technologies like Active Directory Domain Services

(AD DS) rely on DNS to perform their operations. DNS is the primary protocol used in the Domain Name System but it does not offer any form of security and is thus vulnerable to spoofing, man-in-the-middle and cache poisoning attacks. These attacks can compromise all future communications between the host and the client. Domain Name System Security Extensions (DNSSEC) [10] is a suite of extensions that add security to the DNS protocol. DNSSEC applies digital signatures to DNS data to authenticate the data's origin and verify its integrity as it moves across the Internet. DNSSEC ensures that the IP addresses generated by the DNS have not been intercepted or spoofed. Using public-key cryptography to digitally sign each IP address sent out by the DNS at each stage of the hierarchical name-to-number resolution process, DNSSEC allows Internet-connected systems to verify that the responses are authoritative and have not been altered. The core DNSSEC extensions are specified in IETF RFCs 4033, 4034, and 4035, with additional RFCs providing supporting information. Specifically, DNSSEC provides origin authority, data integrity, and authenticated denial of existence. In addition to several new concepts and operations for both the DNS server and the DNS client, DNSSEC introduces four new resource record types namely Resource Record Signature (RRSIG), DNS Public Key (DNSKEY), Delegation Signer (DS), and Next Secure (NSEC). It also adds two new DNS header flags: Checking Disabled (CD) and Authenticated Data (AD). In order to support the larger DNS message sizes that result from adding the DNSSEC RRs, DNSSEC also requires EDNS0 support (RFC 2671). It also requires support for the DNSSEC OK (DO) EDNS header bit (RFC 3225) so that a security-aware resolver can indicate in its queries that it wishes to receive DNSSEC RRs in response messages. By checking the signature, a DNS resolver is able to check if the information is identical (correct and complete) to the information on the authoritative DNS server.

A significant advancement in the security of the Internet in the form of deployment of a critical security technology namely DNSSEC was enabled recently (on 15th of July 2011) at the root Internet zone. This zone lies at the core of the Internet's global addressing system. It has took years of intensive design, testing, and implementation work, to deploy new security upgrade to the Internet's domain name system which allows Internet service providers and end users to protect against an important online vulnerability: the clandestine redirecting of online communications to unwanted destinations. The release of the root zone trust anchor, distribution of a signed root, and subsequent deployment of DNSSEC across the global Internet together comprise the strongest defence against vulnerabilities like DNS cache poisoning. The Internet Corporation for Assigned Names and Numbers (ICANN) [11] published the "root zone trust anchor" for DNSSEC and VeriSign [12] distributed a DNSSEC- signed root zone file. The trust anchor provides a pre-configured public key that allows the thirteen root name servers to verify each other's digital signatures and exchange valid certificates, enabling them to identify each other securely. The signed root zone file creates an authentication and verification capability right from the top of the DNS hierarchy. Throughout the increasingly rigorous testing process, these organizations reported no detrimental impact on DNS performance, which led the Department of Commerce to authorize of the signing of the root zone. There is still a lot more to do to achieve global implementation of DNSSEC and to secure the Internet's core infrastructures and practices against other known vulnerabilities.

In a significant and recent development, prominent Internet Organizations Packet Clearing House (PCH) [13] and the Internet Corporation for Assigned Names and Numbers (ICANN) joined by the Infocomm Development Authority of Singapore (IDA) [14] and the National University of Singapore (NUS) [15] in June 2011 created three new facilities, located in Singapore; Zurich, Switzerland (still under construction) and San Jose, California that will provide secure digital signatures for the country-code top level domains of dozens of countries. They will provide cryptographic security using the recently deployed Domain Name System Security (DNSSEC) protocol assuring Internet users in each country that adopts the new service of the authenticity of the websites they visit and the email addresses they use [16].

3.5 Approval of .XXX TLD

To protect children from obscene or indecent material on the Internet, legislation was enacted to create a "kids-friendly top level domain name" that would contain only age appropriate content. The .KIDS Implementation and Efficiency Act of 2002 was signed into law on December 4, 2002 (P.L. 107-317), and authorized NTIA to require the .us registry operator (currently NeuStar) to establish, operate, and maintain a second level domain within the .us TLD that is restricted to material suitable for minors.

On the contrary establishment of an adult content top level domain name (such as .XXX) [17] that could be filtered by parents was also considered which did not advance beyond introduction. Since 2000, ICANN has repeatedly considered whether to allow the establishment of a gTLD for adult content. The announcement of ICANN on 1st June 2005 pertaining to its commercial and technical negotiations with a registry company (ICM Registry) to operate a new ".xxx" domain proved highly controversial. After several deliberations and meetings ICANN Board on March 30, 2007 voted 9-5 to deny the creation of gTLD .xxx domain. ICM Registry subsequently challenged ICANN's decision before an Independent Review Panel (IRP), claiming that ICANN's rejection of ICM's application for .xxx gTLD was not consistent with ICANN's Articles of Incorporation and Bylaws. Finally, after several meetings and debates among ICANN's Governmental Advisory Committee (GAC), Independent Review Panel (from the International Centre for Dispute Resolution) and ICANN Board, the Board on March 18, 2011, at the ICANN meeting in San Francisco approved a resolution giving the CEO or General Counsel of ICANN the authority to execute the registry agreement with ICM to establish a .XXX TLD. The vote was nine in favour, three opposed, and four abstentions. The .XXX TLD is expected to launch in December 2011.

Lawyers for the most storied brands in the United States are scrambling to prevent an x-rated rip-off of an invaluable asset: corporate Web addresses. The domain operator administering the .XXX domain is accepting early applications from brand owners who want control over their names. ICM Registry says it has received over 900,000 "expressions of interest" from companies that want to pre-register their trademarks or block others from snapping them up to create, e.g. a BARBIE.XXX or COKE. XXX. [18]. Companies are ready to pay preregistration

fees to protect trademarks. However, not all registrants have to pay fee. Under ICANN's rules, certain non-profit organizations including the Red Cross and the International Olympic Committee receive special protection in new domains because of their international status. Further, it is expected that the sale of .XXX domain names could cost several times more than the cost of a standard domain name. Further, each new TLD domain brings a new round of cyber-squatters, who register well-known trademarks to increase Web traffic or later sell them at an inflated price. The author is of considerate opinion that the decision of approval of establishing .XXX domain will created serious concerns in several sections of the societies as well and when such domain names will come up on the Internet.

3.6 Domain Name Dispute Resolution

Domain Names has raised concerns pertaining to intellectual property, trademark and piracy of online content [19]. Several legal battles have been fought between contending parties throughout the Globe for domain names. At ICANN's August 1999 meeting in Santiago, the board of directors adopted a dispute resolution policy to be applied uniformly by all ICANN-accredited registrars. Meanwhile, the 106th Congress passed the Anti-cybersquatting Consumer Protection Act (incorporated into P.L. 106-113, the FY2000 Consolidated Appropriations Act) [20] which gives courts the authority to order the forfeiture, cancellation, and/or transfer of domain names registered in "bad faith" that are identical or similar to trademarks, and provides for some statutory civil damages per domain name identifier. The Combating Online Infringement and Counterfeits Act (COICA) [21] enacted in the 111th Congress, S. 3804, gives the Department of Justice authority to seek a court order to compel domestic registries and registrars to suspend the operation of domain names used by Internet sites dedicated to infringing activities. In the case of domains for which the registry or registrar is not located domestically, the act would give the Department of Justice authority to seek a court order to compel domestic Internet service providers to impair the functionality of the domain name used by infringing Internet sites.

3.7 Privacy and the WHOIS Database

WHOIS services provide public access to data on registered domain names stored in a public online database (the "WHOIS" database), which currently includes contact information (phone number, address, email) for Registered Name Holders. The extent of registration data collected at the time of registration of a domain name, and the ways such data can be accessed, are specified in agreements established by ICANN for domain names registered in generic top-level domains (gTLDs). The scope and accessibility of WHOIS database information has been an issue of contention between privacy advocates and many businesses, intellectual property interests, law enforcement agencies, and the U.S. government [22]. While the former argue that access to such information should be limited, the later argue that complete and accurate WHOIS information should continue to be publicly accessible.

Generic Names Supporting Organization (GNSO) of ICANN developing policy recommendations about WHOIS database after several deliberations approved an official "working definition" for the purpose of the public display of WHOIS information. A narrow technical definition has been supported by privacy advocates, registries, registrars, and non-commercial user constituencies which is being opposed by intellectual property interests, business constituencies, Internet service providers, law enforcement agencies, and ICANN's Governmental Advisory Committee. The GNSO voted to defer a decision on WHOIS database privacy and recommended more studies in October, 2007. It also rejected a proposal to allow Internet users the option of listing third party contact information rather than their own private data. Several Working groups have been formed since 2007 by GNSO to study and explore different aspects of WHOIS. GNSO Council Approved WHOIS Misuse Study in September 2010 and Carnegie Mellon University will analyse the extent, nature, and impact of harmful actions taken using WHOIS contact information for about a year. The WHOIS Proxy and Privacy "Abuse" Study was approved by the GNSO Council in April, 2011. An extensive study is conducted to compare a broad sample of privacy and proxy-registered domains associated with alleged harmful acts. WHOIS Proxy and Privacy "Relay and Reveal" Pre-Study Survey was approved by the GNSO Council on 28 April 2011, and will take about four months to conduct once a contract is finalized. The WHOIS Registrant Identification Study, gathering information about how business/commercial domain registrants are identified and correlate such identification with use of proxy/privacy services is still being considered by the GNSO Council.

Currently, the GNSO is exploring several extensive studies of WHOIS [23]. WHOIS study recommendations were provided to the Study Group by gTLD Registries Stakeholder Group in March, 2011 regarding the study of: i) WHOIS Registrant Identification, ii) WHOIS Privacy and Proxy "Abuse", iii) WHOIS Privacy and Proxy "Relay and Reveal", and iv) WHOIS Registrant Identification Study. In May 2011, a small group of volunteers has proposed a revision "Revised Terms of Reference for Whois Registrant Identification Studies" to an earlier WHOIS Registration Identification study that was previously developed for Council consideration.

3.8 Contractual Compliance Programs

Consistent with ICANN's mission to preserve the operational stability and security of the DNS and promoting competition, consumer trust and consumer choice, ICANN's contractual compliance programs aim to ensure all ICANN-accredited registrars and registries comply with the terms of the agreements they have with ICANN. ICANN is accepting complaints from anyone who believes that an accredited registrar or gTLD registry operator or sponsor or a ccTLD registry is violating its agreement with ICANN. After the reception of the complaint, it is reviewed by the ICANN staff which may be dismissed with a notification to the complainant if it does not falls under the purview of the ICANN or has already been resolved. In case, the initial review decides to investigate the complaint, compliance staff is appointed by the ICANN which gathers factual material for the initial investigation, and sends the complaint to the entity complained about for its response. Depending upon the response from the entity complained about, the complaint may be closed or appropriate action may be taken or more material may be asked from complainant or the entity complained about. In the year 2011, ICANN has so far send notice of breach to as many as 11 registrars. Complete listing of these complaints and their current status can be checked from http://www.icann.org/en/compliance/. ICANN also offers various general guidelines relating to domain name registration

for individuals and organizations to help them avoid any possible future disputes and problems.

ICANN also has ccTLD Compliance Program, gTLD Compliance Program and ICANN Accredited Registrar Compliance Program. ICANN does not have contract authority to take compliance action against ccTLD operators but has a limited number of sponsorship agreements and MoUs with ccTLDs which includes the commitment to adhere to relevant technical standards. ICANN works cooperatively with ccTLD operators to resolve technical issues in furtherance of their common interests to ensure the security, stability and operability of the internet for the benefit of the local and global Internet users. The gTLD Compliance program includes several areas that include: functional specifications, performance specifications, equivalent access to registry services, reserved names, zone files, WHOIS, data escrow, registration restrictions, use of registrar data, and payments to ICANN. Under the ICANN Accredited Registrar Compliance Program [24], every accredited registrar signs an identical Registrar Accreditation Agreement (RAA) so that compliance efforts can be carried out in a consistent manner across all registrars. Under RAA, provisions are divided into seven general Compliance Areas which are monitored by ICANN. RAA has undergone several revisions; latest being in May 2009 which has made a set of 17 amendments to it and follows an extensive consultation that engaged all interested elements of the Internet community including governments, individual Internet users, and gTLD registrars. The changes include: enhanced enforcement tools to assure full compliance with the ICANN contract and policies, expanded requirements for reseller agreements, additional audit and data escrow requirements, more explicit requirements for providing contact information, and new notice requirements and termination provisions. In addition to approving these amendments, the GNSO constituent groups have committed to an on-going review process where additional amendments will be considered and a registrant rights charter will be drafted.

3.9 Other Developments

The IPv6 policy had been in development in the Regional Internet Registries namely AfriNIC, APNIC, ARIN, LACNIC and RIPE for several years which has resulted in 'The Global Policy for Allocation of IPv6 Address Space' [25]. The IPv6 address management function has been delegated to IANA and the registration procedure has been confirmed in March 2010.

Several requests for new registry services have been submitted to ICANN in recent years which have either been approved or are undergoing through a registry services evaluation process [26].

In July 2011, Generic Names Supporting Organization (GNSO) of ICANN has approved the recommendations on the "Post-Expiration Domain Name Recovery Policy Development Process (PDP)" which is currently pending for ICANN Board action. It proposes solutions to several vital issues regarding post-expiration of domain names [27].

ICANN through its fellowship program seeks to create a broader base of knowledgeable constituents and build capacity within the ICANN community of volunteers by reaching out to the less developed regions of the world. The recipients of the fellowship are expected to actively contribute to ICANN processes and be a part of the next generation of ICANN leadership. The 14th round of this fellowship program is being held in Dakar, Senegal in October, 2011 to be followed by similar fellowships in 2012 [28].

4. CONCLUSION

Both domain name system and domain name service have undergone improvements in the recent years. The count of top-level domains has risen to 323 which include 290 country-code domains out of which 36 are international domains. International top level domain names in non-Latin characters have been approved by ICANN and several such TLDs have been delegated to various governments and administrations of countries and territories listed in the ISO 3166-1 standard, or to their designated representatives or operators. Generic top-level domain (gTLD) space is soon expected to expand as ICANN has allowed any established entity worldwide to apply to form and operate a new gTLD registry. Although, ICANN insists that it has adopted appropriate mechanism to protect the rights of trademark holders but recently, there is a growing demand from some major corporations for its withdraw as they argue that it would be an expensive undertaking as that they will be forced to buy domain names that cover their brands and to protect their trademarks to prevent cyber squatters from grabbing them. Root zone of the DNS has been secured against several vulnerabilities by the deployment of DNSSEC which applies digital signatures to DNS data to authenticate the data's origin and verify its integrity. After several years of deliberations ICANN has agreed to establish .XXX TLD. Under domain name dispute resolution policy several acts have been created to protect intellectual property, trademark and piracy of online content. Policy recommendations for WHOIS database privacy are being studied by Generic Names Supporting Organization of ICANN. ICANN is monitoring registrars, and other operators through several contractual compliance programs which are being reviewed and amended to incorporate new developments. Various other aspects of the DNS like allocation of IP version 6 address spaces, post-expiration domain name recovery policy development process, fellowships for building capacity within the ICANN community, etc. have also undergone some developments.

5. REFERENCES

[1] Charles M. Kozierok, "The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference", No Starch Press, 1st Ed., ISBN-13: 978-1593270476, Oct. 2005.

[2] Committee on Internet Navigation and the Domain Name System: Technical Alternatives and Policy Implications and National Research Council, "Signposts in Cyberspace: The Domain Name System and Internet Navigation", National Academies Press, ISBN-13: 978-0309096409, Jul 2005.

[3] IAB, Internet Architecture Board, http://www.iab.org.

[4] J. Klensin, "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", Internet Engineering Task Force (IETF), RFC 5890, August, 2010, https://www3.tools.ietf.org/html/rfc5890.

[5] NIXI, National Internet Exchange of India, http://nixi.in/.

[6] Ivkovic, Dejan and Lotherington, Heather, "Multilingualism in Cyberspace: Conceptualising the Virtual Linguistic Landscape", International Journal of

Multilingualism, 6(1), pp. 17-36, Feb 2009, http://www.tandfonline.com/doi/abs/10.1080/14790710802582436.

[7] ICANN New gTDL Programme, http://www.icann.org/en/topics /new-gtlds/program-en.htm.

[8] ICANN, "How Should We Raise Global Awareness of New gTLDs? Engage the ICANN Community" http://www.icann.org/en/announcements/announcement-17aug11-en.htm. August, 2011.

[9] Esther Dyson, "Esther Dyson On New Top-Level Domains: There Are Huge Trademark Issues", interview of Esther Dyson founding chairwoman of ICANN on Techcruch.com, 21st July, 2011, http://techcrunch.com/2011/07/21/esther-dyson-top-level-domains/.

[10] Amy Friedlander, Allison Mankin, W. Douglas Maughan. "DNSSEC: a protocol toward securing the internet infrastructure", Communications of the ACM - Smart business networks, 50 (6), pp. 44 – 50, June 2007.

[11] ICANN, Internet Corporation for Assigned Names and Numbers, http://www.icann.org.

[12] VeriSign, http://www.verisign.com/.

[13] PCH, Packet Clearing House, http://www.pch.net/.

[14] IDA, Infocomm Development Authority of Singapore, http://www.ida.gov.sg.

[15] NUS, National University of Singapore, http://www.nus.edu.sg/.

[16] PCH, ICANN, IDA, NUS, "Internet Groups Inaugurate Cyber Security Facility in Singapore", http://www.icann.org/en/news/releases/release-22jun11-en.pdf.

[17] ICANN, "Delegation of the .XXX top-level domain", http://www.iana.org/reports/2011/xxx-report-20110407.pdf

[18] FOX News, "Barbie.xxx? RedCross.xxx? Brands Scramble to Prevent X-Rated Rip-Offs", Technology, 16th August, 2011, http://www.foxnews.com/scitech/2011/08/16/barbiexxx-redcrossxxx-brands-scramble-to-prevent-x-rated-rip-offs/

[19] Daniel W. McDonald et al, "Intellectual Property and the Internet", COMPUTER, Dec. 1996.

[20] Committee on the Judiciary, "The Anticybersquatting Consumer Protection", AUGUST 5, 1999, http://www.citmedialaw.org/sites/citmedialaw.org/files/ACPA%20leg% 20history.pdf.

[21] S. 3804--111th Congress: Combating Online Infringement and Counterfeits Act. (2010). In*GovTrack.us (database of federal legislation)*. Retrieved August 24, 2011, from http://www.govtrack.us/congress/bill.xpd?bill=s111-3804.

[22] Lennard G. Kruger, "Internet Domain Names: Background and Policy Issues", CRS Report for Congress, Congressional Research Service, March, 2011, http://www.fas.org/sgp/crs/misc/97-868.pdf.

[23] Generic Names Supporting Organization (GSO), http://gnso.icann.org/issues/whois/.

[24] ICANN Accredited Registrar Compliance Program, http://www.icann.org/en/compliance/registrar-compliance.htm.

[25] Proposed Global Policy for Allocation of IPv6 Address Space, http://www.icann.org/en/policies/proposed-ipv6-policy-14jul06.htm.

[26] Registry Services Evaluation Process, http://www.icann.org/en/registries/rsep/.

[27] Post-Expiration Domain Name Recovery Recommendations for ICANN Board Consideration,, http://www.icann.org/en/announcements/announcement-15aug11-en.htm.

[28] ICANN, "Fellowship Programs", http://www.icann.org/en/fellowships/.