Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 3 March 2010

The Internet Domain Name Registration Process:

From the Registrant to ICANN

Prepared by
Wolfgang Kleinwächter
University of Aarhus

Project funded by Romania, Estonia, Monaco, Microsoft, McAfee and the Council of Europe

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int
www.coe.int/cybercrime

Disclaimer

This technical report does not necessarily reflect official positions of the Council of Europe or of the donors funding this project or of the parties to the instruments referred to.

Contents

1 Introduction

At the end of 2009 there were nearly two billion Internet users and around 200 million registered domain names worldwide.1 Alone in 2009 there were 15 million new domain name registrations. The growth rate in 2009 was compared with 2008 about eight percent. About ninety per cent of the 4.3 billion IPv4 addresses are allocated to Regional Internet Registries (RIRs) and ISPs, but zillions of IPv6 addresses are available for future allocations. Royal Pingdom reports in 2009 there were 90 trillion e-mails (this is 247 billion every day)2. We have now 234 million websites. 47 million were added in 2009. There are 126 million Internet blogs, 4 billion photos are hosted by Flickr.com alone. You Tube serves 1 billion queries for videos online every day. And there is no end in the ongoing dynamics of the global Internet growth.

One objective of the UN sponsored World Summit on the Information Society (WSIS) was to bring half of mankind online up to 2015.3 This means that another two billion people will be linked to the Internet within the next five years. It seems not unrealistic that the target will be achieved. Recognizing new technological developments which enable more and more mobile phones to be linked to the Internet, the potential is even higher. In 2009 the number of mobile phones crossed the four billion mark.

Domain Names and IP Addresses are the two main identifiers on the Internet. While the IP address identifies the network and the computer within a network via an IPv4 or IPv6 address, the domain name – and the related e-mail address – identifies the Internet end user. The Domain Name System protocol (DNS) translates the IP number into a name and gives the chain of numbers in an IP address a "human face" which can be easier understood and remembered.

The domain name, like the IP address, is a critical Internet resource (CIR). To offer services over the Internet, users need a domain name. To communicate over the Internet, individual Internet users need an e-Mail address, linked to a domain name. The Domain Name System (DNS) is the "territory of the Internet". Some people call the global database of the domain names, the WHOIS database, also the "phone book of the Internet". Both resources – domain names and IP addresses – are de facto "unlimited resources" and are managed by a mechanism of various institutions, coordinated by the Internet Corporation for Assigned Names and Numbers (ICANN), a private non-for profit corporation, led by an international board of directors and headquartered in Maria del Rey (California).

Domain names give their holders an identity and an opportunity to do all kinds of communication services: from launching a business to establish private communication networks. Large corporations have built their whole empires on a simple domain name like www.google.com. But also individuals, like Bernhard Kroenung in Germany, have built their family platform on a domain name like www.kroenung.de.

[1] See: The Domain Name Industry Brief, VeriSign, Vol. 7, Issue 1, February 2010, in: http://www.verisign.com/domain-name-services/domain-information-center/domain-name-resources/domain-name-report-feb10.pdf

[2] See: http://royal.pingdom.com/2010/01/22/internet-2009-in-numbers/

[3] See: WSIS Geneva Plan of Action, December 2003, in: http://www.itu.int/wsis/docs/geneva/official/poa.html

2 History & Process

2.1 Historical Development of the DNS

The Domain Name System (DNS) was developed mainly by Jon Postel and Paul Mockapetris in the 1980s as part of their research for the DARPANet project, financed by the US Department of Defense. Jon Postel, who worked at the Information Science Institute (ISI) at the University of Southern California (USC) in Marina del Rey, became the manager of the DNS and developed the so-called "socket registry", which was established in 1974 after Vint Verf and Bob Kahn launched the TCP/IP protocol (which is seen by many sources as the "birthday of the Internet") into the Internet Assigned Numbers Authority (IANA).[4]

Postel did this work under a contract the ISI had first with the Defense Advanced Research Project Agency (DARPA) and later with the US Department of Commerce (DoC). Postel continued to lead IANA until his sudden death in October 1998, just days before the Internet Corporation for Assigned Names and Numbers (ICANN) was launched.

The DNS is organized as a tree with Top Level Domains (TLDs) like .com, .eu or .de at the top, Secondary Level Domains (SLDs) like www.coe.com, www.coe.eu or www.coe.de below the TLD and Third Level Domains like www.office.ceo.com, www.secretary.ceo.eu or www.member.ceo.de.

Each level has its own zone files. The TLD and SLD zone files are managed by different operators/servers, but they are interlinked in a multilayered system.

- The zone files of the TLDs are stored in the IANA database and the root servers. There are 13 root servers worldwide, linked to a global system of more than 100 so-called Anycast root servers. The main (master) server is the so-called Hidden Server (formerly the A-Root Server), operated by VeriSign Inc. under a contract with the US Department of Commerce.

- The zone files of the SLDs are stored in by the authoritative name server of the TLD registry which manages its own domain. Name servers are linked to root servers. The root server has only the TLD zone file which comes from the TLD registry in its database, while the name server has the zone files of the SDLs, which come from the registrars or registrants, in its database.

- Changes in TLD root zone files like adding a new name server of a TLD registry or introducing a new configuration of an existing name server are managed by IANA (the so-called IANA service) on the basis of a formal contract or another formal or informal service arrangement between IANA/ICANN and the relevant gTLD or ccTLD registry. Changes in SLD zone files are managed by the TLD Registry

The DNS makes it possible to assign domain names to groups of Internet users in a meaningful way, independent of each user's physical location. Because of this, World Wide Web (WWW) hyperlinks and Internet contact information can remain consistent and constant even if the current Internet routing arrangements change or the participant uses a mobile device. The DNS distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain.

[4] See: Wolfgang Kleinwächter, The History of Internet Governance, in Christian Moeller & Arnoud Amouroux, Governing the Internet, OSCE Vienna, 2007, in: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf

Authoritative name servers are assigned to be responsible for their particular domains, and in turn can assign other authoritative name servers for their sub-domains. This mechanism has made the DNS distributed, fault tolerant, and helped avoid the need for a single central register to be continually consulted and updated.

2.2 Structure of the Domain Name System

There are two main categories of TLDs:

- generic Top Level Domains (gTLDs) as .com, .info or .mobi and
- country code Top Level Domains (ccTLDs) as .de, fr. or .me.

At the end of 2009 there were 243 ccTLDs5 and 18 gTLDs6. From a technical point of view there are no differences between a gTLD and a ccTLD. Both enable the same type of Internet communication service to the same type of Internet users.

There are no technical limitations for the introduction of new top level domains, neither on the gTLD nor on the ccTLD level. While the number of ccTLDs has a natural limit, there are no such limits with regard to the number of gTLDs. There are also no technical barriers to introduce new TLD categories as it is discussed within ICANN with regard to TLDs for cities and regions, so-called geographical TLDs (GEO-TLDs). However, there is an ongoing discussion how the addition of thousands of new TLDs in parallel to the authorization of Non-ASCII (internationalized) domain names on the top level (iDNs), the introduction of the new security protocol DNSSec and the transition from the IPv4 to the IPv6 address protocol could have serious implications for the stability, security and resilience of the Internet as a whole.

The number of ccTLDs comes from the ISO 3166 list, which lists the names of countries and territories and links them to a two letter country code. The list was chosen by Jon Postel in the 1980s to avoid that his "Internet Assigned Numbers Authority" (IANA) would be pushed into a situation where it has to decide whom to give a ccTLD. In RFC 15917 he explained that "IANA is not in the business of deciding what is and what is not a country." And he added that "the selection of the ISO 3166 list as a basis for country code top-level domain names was made with the knowledge that ISO has a procedure for determining which entities should be and should not." RFC 1591 was re-confirmed by ICANN in a special policy paper (ICP-1) in 19998 as well as by the Governmental Advisory Committee (GAC) in its ccTLD principles from 2000 (amended in 2005)9. As soon as a country or territory is on the ISO 3166 list, ICANN has the obligation to delegate the ccTLD to an authorized registry, following the policies and procedures laid down in RFC 1591, ICP-1 and the GAC ccTLD principles.10

[5] List of ccTLDs (December 2009): http://www.iana.org/domains/root/db/

[6] List of gTLDs (December 2009): http://www.icann.org/en/registries/agreements.htm

[7] http://tools.ietf.org/html/rfc1591

[8] http://www.icann.org/en/icp/icp-1.htm

[9] http://www.icann.org/en/committees/gac/gac-cctldprinciples-23feb00.htm

[10] An interesting problem is the termination of a ccTLD in case a country disappears from the global political map as it happened with former Yugoslavia and former Soviet Union. In the case of Yugoslavia, the succession states got a new ccTLD but the ccTLD .yu continued to exist. ICANN adopted a transition plan to take down the .yu domain but it was several time extended and will continue up to 2012. The case of the .su domain is even more complicated. Also here all former republics of the Soviet Union got their own ccTLD, however the .su domain is still active and is growing with more than active 250 000 registrations. There are negotiations between ICANN and the ccTLD operator for .su, but the .su operator argues that the ccTLD delegation was to a "community" and not to a "country." The ccTLD operator for .su has asked for a transition period of 15 years until the year 2025. The case is still open.

The introduction of new gTLDs is under discussion since the early 1990s. When Jon Postel introduced the DNS he believed that six three letter gTLD codes (three for the US as .edu., .mil and .gov and three for the world as .com, .org and .net) will be enough to accommodate all needs of potential domain name registrants as laid down in RFC 920 from October 1984. Later, in 1998, the gTLD .int was added (for intergovernmental organizations) as a result of a special request by NATO.11

The invention of the World Wide Web in the early 1990s created a new environment for the domain name space and a domain name market emerged which is today a million dollar business. The "dotcom-boom" in the 1990s produced soon a shortage of good names (easy to find, easy to understand and easy to remember), in particular in the .com domain name space.12 As a result, registered domain names got a material/financial value beyond its main identification function and became the subject of trade (and speculation) in a fast growing market.

The discussion, how to enhance the gTLD name space to create more opportunities for domain name registration, in particular for SLD domain names, started already in 1993 when NSI got the right from the US government to charge an annual 35.00 $ fee for the registration of domain names.

The first plan of Jon Postel, to introduce 150 new gTLDs under the umbrella of ISOC (which was established in 1992)13 failed. Another effort, initiated by Jon Postel, to introduce seven new gTLDs under the regime of the Interim Ad Hoc Committee (IAHC)14 in 1997 failed as well. The IAHC included with the International Telecommunication Union (ITU) and the World Intellectual Property Organization (WIPO) also two intergovernmental organizations (IGOs) of the UN system.

When ICANN was established in 1998 it got, inter alia, the mandate "(iii) performing and overseeing functions related to the coordination of the Internet domain name system ("DNS"), including the development of policies for determining the circumstances under which new top-level domains are added to the DNS root system"15. Since 2000 ICANN has authorized the introduction of 10 new gTLDs like .info, .name, .biz, .tel or .post, some of them as so-called sponsored TLDs (sTLDs). Since 2004 ICANN is working in parallel on a more sustainable procedure for the introduction of new gTLDs, but the start of the process was numerous times delayed. It is expected that in 2010 ICANN will start to accept formal applications and that the first new gTLDs will be operable in 2011 or 2012.16

Additionally ICANN worked since 2000 on the introduction of domain names which do not use the ASCII code, so-called internationalized domains (iDNs). Since 2006 the registration of SDL in Non-ASCII code is possible. In 2007 ICANN started a fast track process to launch also iDNS at the top level (iDN.iDN) for twelve different Non-ASCII scripts in the ccTLD name space.17 The first appIications for iDN ccTLD registry services arrived in November 2009.

[11] There is another four letter TLD, a so-called infrastructure gTLD .arpa for use within IANA only

[12] One example is the story of the business.com domain which was originally registered in 1993 for 35.00 $ but later sold for 25.000.00 $ and re-sold first for 100.000.00 $ and in 1999 for 7.8 million $.

[13] http://www.isoc.org/

[14] http://www.gtld-mou.org/draft-iahc-recommend-00.html, The proposed seven new gTLDs were: .firm, .store, .web, .arts, .rec, .info and .nom

[15] http://www.icann.org/en/general/articles.htm

[16] See: http://www.icann.org/en/topics/new-gtld-program.htm. The recent 3rd version of the Applicants Guide Book is under discussion again during the forthcoming ICANN meeting in Nairobi, March 2010.

[17] See iDN Fast Track, in: http://www.icann.org/en/topics/idn/fast-track/

Negotiations started with the first applicants in December 2009. It is expected that they will be operable in 2010.

Whether and how an iDN gTLD process will follow remains under discussion within ICANN. A special problem here is also the question how many characters can be used for new gTLDs in Non-ASCII script. While ICANN is proposing a minimum of three characters, China, for instance, wants to have the flexibility to use only two characters in iDN gTLDs. In the meantime, the Chinese Ministry for Industrry and Information Technology (MIIT) is planning to authorize its own new gTLD program with Chinese characters based on an own root without asking for authorization by the IANA/NTIA procedure under the present ICANN regime.

2.3 Policies for Domain Name Registration

The policies and procedures for the registration of domain names has been developed also bottom up by the Internet developers, providers and users themselves. So far, domain name registration – from a user´s perspective - is simple, fast and cheap (as long as it is not a special name which is pre-registered by a domain name trader). A user goes to the website of an ISP, checks the availability of a name, register the name and if the name is free, the registrant fills in the forms which include, inter alia, his basic contact details and pays the fee. The whole domain name registration costs very often less than ten minutes and not much more than ten EUROs. The process is meanwhile to a high degree automated.

For technical reason and to avoid confusion and miscommunication there is an objective need that each domain name is unique and can be registered only once. As a general policy principle Jon Postel introduced the "first come first served principle". According to this principle a registrant is free to choose any name under a TLD and as long as the name is free the registrant can get it. There was not duty on the side of a TLD registry (or an ISP/registrar) to double check the identity and the correctness of the contact details of a domain name registrant. There was also no obligation to double check whether the registered domain name is in conflict with a registered trademark. The only criteria for the registration of domain names were the availability of the name. Today the majority of the TLD operators have introduced an automatic registration system which registers the name automatically if the name is free. However some ccTLD operators have introduced "blacklists" for names which users can not be register for political, religious, moral or other reasons.

Registration of gTLD names was free of charge until 1993. In 1993, Network Solutions Inc. (NSI), which managed .com, .net and .org under a contract with the US Department of Commerce, got the right to charge for a domain name (about 35.00 $ per year). For more than ten years, NSI had a monopoly in the registration of domain names in the gTLD name space. NSI offered both registry and registrar service. In 1998 NSI was pushed to enter into a Shared Registration System, (SRS) which allowed also other registrars than NSI to register domain names in the gTLD names space. The first five new registrars were authorized and got their accreditation by ICANN in 1999.

One reason for the launch of ICANN was to demonopolize the gTLD domain name registration process, to separate registry from registrar services and to allow and stimulate more competition in the emerging domain name market at all levels, both registrar and registry to offer more choice, better quality and lower prices to registrants.

NSI was bought by VeriSign Inc. in the year 2000. NSI/VeriSign entered into negotiations both with ICANN and the US Department of Commerce. As a result, NSI/VeriSign had to transfer the management of the .org gTLD to another registry (Public Internet Registry/PIR) and to separate its registry and registrar business in 2000. The management of the .net registry became the subject of an open call which saw five applicants, including VeriSign. However, the ICANN Board decided to re-delegate .net to VeriSign in 2005. In 2006 the .com domain was also redelegated to VeriSign.

Policies for the registration of domain names in the gTLD name space are defined by ICANN. These policies include a number of obligations for registries and registrars, in particular to store data of registrants for the WHOIS database, to avoid the registration of domain names of protected trademarks and a fee structure for the registration of domain names.

The policies are specified in a number of contractual arrangements, notably in the Registry Agreement between the gTLD Registry and ICANN, the Registrar Accreditation Agreement (RAA) between the registrar and ICANN and the Registry-Registrar Agreement (RRA) between a gTLD Registry and a registrar.

For ccTLDs there is no single or harmonized model for domain name registration. Different ccTLD registries have developed their own individual domain name registration policies, based on the general principles laid down in RFC 1591. Individual national regulations include, inter alia, the reservation or blocking of special names, building of a sub-structure with sponsored SLDs18, defining who has a right to register a domain name in the given ccTLD name space, access provisions to data for governmental institutions, a fee structure for registrants etc.

In contrast to the allocation of telephone numbers, governments – until the mid 1990s - were not involved in the development of policies and procedures neither for the registration of domain names nor the allocation of IP addresses. Even the delegation of a whole ccTLD was done without any governmental involvement, very often based on a handshake by Jon Postel with a "trusted person" who became the manager and/or the technical administrator of the ccTLD19.

As a result of these general principles and the specific historical background, described above, the domain name registration process became simple, fast and cheap. And it became also global. Citizens of any country could register a domain name in the gTLD name space. And a lot of ccTLD registries allowed also registration of domain names by anybody, regardless of his/her citizenship or residency.

Only in the late 1990s individual governments started to discuss the need to create a national regulatory framework for domain name registration in their ccTLD domain name space. The majority of countries have meanwhile created such frameworks, very often as

[18] Quite a number of ccTLD registries have introduced a special sub-domain system with reserved sub-domains for governmental, academic and commercial institutions as the United Kingdom Registry Nominet (.uk) has done with sub-TLDs like .co.uk, .ac.uk, .go.uk etc. RFC 1591 did not exclude this option. ccTLD registries are free to introduce such a substructure as long as they follow the general principles and connect their main name servers to the root servers via IANA.

[19] In the 1980 Postel delegated a number of ccTLD to trusted individuals who did not have the citizenship of the relevant country. The most famous case is the delegation of .cn for the People Republic of China which went by handshake to the German Professor Werner Zorn from the University of Karlsruhe whih worked in a joint project with the Chinese Academy of Science in Bejing. Zorn helped to build the name server for the Chinese ccTLD in 1987 but took the master copy of the .cn name server back to Karlsruhe with a copy remaining in Bejing. Only in 1993 the .cn domain was redelegated to the Chinese Information Center. Another case is the delegation of ccTLDs to a number of African countries. Postel delegated this ccTLDs to Randy Bush from the University of Minnesota who was involved in numerous projects in Africa, sponsored by the US International Development Agency (USAID).

part of the telecommunication regulation. In many countries, as in China or Russia, there are very detailed governmental guidelines under which conditions end users can register domain names, however in other countries, which established in the first place a rather regulated system, as France, the policies were liberalized later.

The UN World Summit on the Information Society (WSIS) discussed in detail the role and status of the ccTLD name space. In Paragraph 63 of the Tunis Agenda for the Information Society (2005) it is stated: "Countries should not be involved in decisions regarding another country's country-code Top-Level Domain (ccTLD). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanisms."[20]

2.4 Domain Name Conflicts

The flexibility of the domain name registration mechanism stimulated on the one hand the enormous growth of the domain name market. But it opened also the door for misuse.

Since the middle of the 1990s registration of domain names in bad faith started to become a plague. Practices like Cybersquatting emerged where individuals registered domain names similar or identical to trademarks or to other famous and well known names. The cybersquatters tried to sell the registered domain name to the trademark holder or the holder of a famous and well know name to make extra profit provoking very often long legal battles about rights on names.

The number of conflicts between trademark owners and domain name holders was exploding and led to hundreds of court cases. Court proceedings became difficult when the domain name registrant, the registrar and the registry operated under different national jurisdictions. When ICANN was established in 1998, one of its first duties was to introduce a global applicable dispute resolution mechanism for domain names registered in the gTLD name space. ICANN adopted its "Universal Dispute Resolution Policy" (UDRP) and introduced a mechanism for Domain Name Dispute Resolution already in 1999.

The UDRP defines criteria for domain name registration on bad faith.21 ICANN has authorized a number of UDRP service providers, including the arbitration center of the World Intellectual Property Organization (WIPO) in Geneva and the Czech Arbitration Court (which handles also domain name conflicts under the .eu domain which is treated as a ccTLD) in Prague. The UDRP service providers handle individual cases online only. The procedure is

[20] Tunis Agenda for the Information Society, Tunis, November 18, 2005, in: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2266|2267

[21] ICANN has defined "bad faith registration" in its Uniform Dispute Resolution Policy (TDRP) from October 24, 1999 as follows: "(i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or (ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or (iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or (iv) by using the domain name, you have intentionally attempted to attract, for commercial gain, Internet users to your web site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship, affiliation, or endorsement of your web site or location or of a product or service on your web site or location." See: http://www.icann.org/en/dndr/udrp/policy.htm

open and transparent. The whole case and the final decision are accessible on the UDRP website. Cases are decided by a panel (of one or three panelists) of authorized experts. The UDRP procedures are simple, fast and cheap. If conflicting parties do not accept a UDRP decision they are free to start an ordinary legal process under a relevant national jurisdiction before an ordinary court.

Internet domain name registrars, which enter into an accreditation agreement with ICANN, have to accept the UDRP as a basis for domain name conflict resolution. Registrars are obliged to follow the decision of the UDRP panels. Since the year 2000 more than 10 000 cases has been settled via the UDRP mechanism. The UDRP, which was mainly introduced for the gTLD domain name space, is used also by a number of ccTLDs to settle domain name disputes, on particular where the conflicting parties operate under different national jurisdictions. Some ccTLD registries have introduced their own online dispute resolution mechanism while other just let potential cases in the hands of the courts under the national jurisdiction where they operate.

To avoid new conflict ICANN has incorporated provisions in the registry agreements ICANN has with TLD registries. The registries of new gTLDs have to establish a so-called sunrise period if they start to register domain names for new gTLD. Within this sun-rise period owners of trademarks have a privileged special right to register their protected name in the new gTLD name space.

3 Players & Contracts

The main Players in the process of domain name registrations are

- The Domain Name Registrant / Domain Name Holder
- The Domain Name Registrar / the Internet Service Provider (ISP)
- The Top Level Domain Registry
- The Internet Corporation for Assigned Names and Numbers (ICANN)

The various players are linked via a chain of bilateral contracts to each other which specifies the rights and duties and the special responsibilities of the various parties operating at the various layers. The main contracts are

- The contract between the domain name holder and the registrar
- the Registry Agreement between the gTLD Registry and ICANN
- the Registrar Accreditation Agreement (RAA) between the registrar and ICANN and
- the Registry-Registrar Agreement (RRA) between a gTLD Registry and a registrar.

A key question in the contracts is the handling, storing and managing of the personal contact date of the registrant, the domain name holder. These personal data, which are available also via the WHOIS database, are needed in particular by law enforcement for criminal investigations. But the WHOIS database, as an open database, is used also by various types of third parties: from the music industry which wants to find out who violates intellectual property regimes until spammers who want to create e-mail list for sending out millions of spam mails to individual Internet users.

The WHOIS database is subject of a controversial discussion with regard to data protection and privacy issues both among governments – in particular between the US government and the governments of the European Union – as well as between various Internet constituencies and stakeholders, in particular between the content industry and civil society.

3.1 The Domain Name Registrant (domain name holder, individual/institutional end user)

And end-user cannot directly register a domain and manage their domain information with ICANN. The registrant – an individual user or an institution - has to choose a designated registrar and to enter into a contractual relationship.

In many cases the designated Internet domain name registrar is an Internet Service Provider (ISP) which offers next to domain name registration a broad variety of other Internet services to their costumers (end users) or a domain name reseller. The contract includes a number of rights and duties for both sides. The domain name registrant has, inter alia, the duty to provide personal contact details – full name, postal address, e-mail address, telephone and fax numbers - and to pay an annual fee, which is today between 7.00 $ and 40.00 $..

The personal data are kept in the database of the registrar and the registry (WHOIS database). Only the designated registrar may modify or delete information about a domain name.

The domain name holder has the right to change the Internet Service Provider and to transfer his/her name to another registrar under a certain domain name transfer policy defined by ICANN. If the registrant allows the use of the registered domain name for another third party, the registrant remains the domain name holder and cannot delegate the relevant rights and duties of a domain name holder to the third party. The contract between the registrant and the registrar includes also rules for the renewing of the registered domain name after the name expired and the registration period terminates.

3.2 The Domain Name Registrar / ISP / Reseller

The registrar/ISP/reseller is the central player in the chain of the domain name registration process. It operates under the national jurisdiction where it is located. But it is embedded via bilateral contractual arrangements in a triangular environment linking together the domain name holder, the TLD registry and ICANN.

- The registrar/ISP provides the domain name service to the end user against a fee (which is often part of a broader package of the special service offered by the ISP).
- The registrar/ISP gets the domain name from a registry of a top level domain (TLD) against a domain name fee, fixed in the contract between the domain name registrar and the TLD registry, the Registry Registrar Agreement (RRA).
- To provide domain name services in the gTLD domain name space for domain name registrants the registrar needs an authorization from ICANN. The authorization comes with a Registrar Accreditation Agreement (RAA) between ICANN and the registrar. The RAA regulates the various rights and duties, including the obligation of the registrar to pay a fee to ICANN.

ICANN has meanwhile more than 800 registrars accredited worldwide. However, the registrar/ISP operates also under the national jurisdiction where it is headquartered and has to follow the applicable law, in particular if it comes to access to data related to the service the registrar offers to a registrant/domain name holder. This has led to a number of conflicts where a registrar/ISP is sandwiched between its contractual obligations with ICANN and the duty to follow national legislation (mainly with regard to data protection laws).

The largest Registrar is Go Daddy with more than 30 million registered domain names. There are nearly 20 registrars with more than one million registered domain names. The list of the Top Twenty is below:

Table 1: Top Twenty Registrars (December 2009)

Rank	Registrar	Domain Count
1	Go Daddy Software	33,919,732
2	eNom	9,222,460
3	Tucows	7,569,192
4	Network Solutions	6,471,877
5	1&1 Internet AG	4,897,979
6	Melbourne IT	4,675,992
7	Wild West Domains	3,291,550
8	Moniker Online Services	2,534,494
9	Register.com	2,532,011
10	PublicDomainRegistry.com	2,530,378
11	Xin Net Corp	1,651,651
12	Key-Systems GmbH	1,601,964

13	OnlineNIC, Inc.	1,105,024
14	Cronon AG	1,042,606
15	Fabulous.com Pty Ltd	1,026,453
16	Dotster	1,015,158
17	FAST DOMAIN INC.	994,223
18	OVH	931,229
19	DomainDiscover	919,389
20	Intercosmos Media	889,865

Source: RegistrarsStats.com [22]

In the past there had been cases where a registrar went bankrupt or terminated its business which raised the issue of the security and stability of registered domain names for registrants/domain name holders. In particular the case of register,fly (2006) provoked a detailed discussion about the security and stability of the domain name registration.

ICANN has meanwhile established a procedure to save the names of the registrants and offers a policy and a clear procedure for a domain name transfer under such extraordinary circumstances. ICANN has also a right to withdraw the accreditation as it was the case with register.fly. Since the year 2000 ICANN withdraw the accreditation of 40 accredited registrars[23].

3.3 The TLD Registry

The TLD registry gets its right to operate and manage a top level domain domain (TLD) via a delegation procedure, established by ICANN. As described above there are two main categories of top level domains: Generic Top Level Domains (gTLD) and Country Code Top Level Domains (ccTLD).

- A registry for a gTLD has to enter into a formal contract with ICANN which specifies the rights, duties and responsibilities of both sides. Part of this contract is also the obligation of a registry to enter into a Registry Registrar Agreement (RRA). The TLD registry has to pay an annual fee to ICANN. ICANN operates as the oversight body for the gTLD registry. The contracts are subject of renewal after a certain time period, fixed in the contract.

- The legal situation for the ccTLD registry is different. For historical reasons, the delegation for the management of a ccTLD was done in the early days in an informal way, very often via handshake by Jon Postel himself. It was ICANNs plan in the beginning to formalize this type of informal relationship and to introduce a special contractual system between ICANN and ccTLDs (and asking for a fee from ccTLD registries as a contribution to ICANNs budget). However this effort failed. A lot of ccTLD registries rejected the proposal to enter into a contract with ICANN (and paying a fee) referring to the fact that the operate under a specific national legislation which could create conflict if a contract with ICANN collides with specific obligations the ccTLD registry has under their national regulatory framework, in particular with regard to the management of the WHOIS database and the relevant national data protection laws. The GAC ccTLD principles helped to clarify the

[22] http://www.registrarstats.com/Public/RegistrarMarketShareMain.aspx

[23] http://www.icann.org/en/compliance/archive/compliance-newsletter-200910-en.htm

mechanism of “bilateral contracts in a triangular environment” taking into account that both ICANN, the ccTLD Registry and national governments are involved in ccTLD issues. The UN World Summit on the Information Society (WSIS) has further clarified the status of a ccTLD registry, as described above. Over the years various forms of formal and informal arrangements between ccTLD registries and ICANN has emerged which is now called the “accountability framework” and is done as

- A formal contract
- A sponsorship agreement
- An exchange of letters
- A Memorandum of Understanding
- A continuation of the informal relationship

In January 2010 ICANN had a formalized relationship with 74 ccTLDs (out of the 243 ccTLDs listed on ISO 3166)[24]

The introduction of iDN ccTLDs and the discussion on new categories for gTLDs, both in ASCII and iDN, has raised a number of new issues which needs future clarification. One question is whether a TLD registry, which operates a ccTLD or a gTLD under ASCII, is automatically also the designed registry for the iDN version of the TLD or whether each iDN registry needs a special new delegation process.

For ccTLDs the question is whether the existing ccTLD registry is automatically also the registry for the iDN version of the ccTLD or whether a new delegation process for a new entitity/ccTLD registry is needed. This includes also the question how a contract between an iDN ccTLD registry and ICANN can be harmonized with national legislation under which the iDN ccTLD registry is operating (in line with Paragraph 63 of the Tunis Agenda of the World Summit on the Information Society). This is of particular important for the management of individual data of the registrants in the iDN name space.

For gTLD registries the problem is whether the ASCII gTLD is treated as a trademark in its own which automatically protected also in the various language scripts or whether, as an example, the Chinese or Russian version of .com or .info is a new gTLD which is not related to the existing .com or .info registry in ASCII, managed by VeriSign and Afilias.

3.4 ICANN / IANA

ICANNs mandate to operate the DNS is fixed in its

- Articles of Incorporation
- Bylaws and
- the various contracts ICANN had and has with the US government.

This framework of legal arrangements gives ICANN the authority to enter into contracts both with TLD registries and domain name registrars. The main provisions are laid down in the following legal documents

- The Articles of Incorporation (October 1998) give ICANN the duty for “(iii) performing and overseeing functions related to the coordination of the Internet domain name system ("DNS"), including the development of policies for determining the circumstances under which new top-level domains are added to the DNS root system”[25].

[24] http://www.icann.org/en/cctlds/agreements.html

[25] http://www.icann.org/en/general/articles.htm

- ICANNs general mission is fixed it Article 1 of its bylaws (September 2009) which says: "The mission of the Internet Corporation for Assigned Names and Numbers ("ICANN") is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems. In particular, ICANN 1. Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are a. Domain names (forming a system referred to as "DNS"); b. Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and c. Protocol port and parameter numbers; 2. Coordinates the operation and evolution of the DNS root name server system. 3. Coordinates policy development reasonably and appropriately related to these technical functions bylaws state".[26]

- In the newly signed "Affirmation of Commitments" (October 2009) the US Department of Commerce (DoC) affirms its commitment "to a multi-stakeholder, private sector led, bottom-up policy development model for DNS technical coordination that acts for the benefit of global Internet users." The AoC further states that to ensure that ICANNs decisions "are in the public interest, and not just the interests of a particular set of stakeholders, ICANN commits to perform and publish analyses of the positive and negative effects of its decisions on the public, including any financial impact on the public, and the positive or negative impact (if any) on the systemic security, stability and resiliency of the DNS." Furthermore the DoC "recognizes the importance of global Internet users being able to use the Internet in their local languages and character sets, and endorses the rapid introduction of internationalized country code top level domain names (ccTLDs), provided related security, stability and resiliency issues are first addressed." It also says that "nothing in this document is an expression of support by DOC of any specific plan or proposal for the implementation of new generic top level domain names (gTLDs) or is an expression by DOC of a view that the potential consumer benefits of new gTLDs outweigh the potential costs."

- In the so-called IANA contract (September 2006 which expires in September 2011), ICANN got mandate to "coordinate the assignment of technical protocol parameters. This function involves the review and assignment of unique values to various parameters (*e.g.*, operation codes, port numbers, object identifiers, protocol numbers) used in various Internet protocols. This function also includes the dissemination of the listings of assigned parameters through various means (including on-line publication) and the review of technical documents for consistency with assigned values." And it got also the mandate to "perform administrative functions associated with root management. This function addresses facilitation and coordination of the root zone of the domain name system, with 24 hour-a-day/7 days a-week coverage. It includes receiving requests for and making routine updates of the country code top level domain (ccTLD) contact (including technical and administrative contacts) and nameserver information. This function also includes receiving delegation and redelegation requests, investigating the circumstances pertinent to those requests, and making recommendations and reporting actions undertaken in connection with processing such requests."[27] ICANN has also the duty to "ensure the authentication, integrity, and reliability of the data in performing the IANA requirements, including the data relevant to DNS, root zone file, and IP address allocation."

[26] http://www.icann.org/en/general/bylaws.htm#II

[27] http://www.icann.org/en/general/iana-contract-14aug06.pdf

4 WHOIS & Security Issues

4.1 WHOIS

WHOIS is a query/response protocol that is widely used for querying databases in order to determine the registrant or assignee of Internet resources, such as a domain name, an IP address block, or an autonomous system number. WHOIS lookups were traditionally performed with a command line interface application, and network administrators predominantly still use this method, but many simplified web-based tools exist. WHOIS services are typically communicated using the Transmission Control Protocol (TCP). Servers listen to requests on the well-known port number 43.

The WHOIS database contains contact information of registrants. It is like the "telephone book of the Internet". If a registrant registers a domain name she/he has to give a number of basic contact information like personal name, postal address, telephone number and e-mail address to the ISP/Registrar where she/he registers the domain name.

The so-called WHOIS service was introduced in the early days of the Internet to enable the system administrators to offer a fast service in case of a technical failure or a miscommunication. When the Internet was emerging out of the ARPANET, there was only one organization that handled all domain registrations, which was DARPA itself. The process of registration was established in RFC 920. WHOIS was standardized in the early 1980s to look-up domains, people and other resources related to domain and number registrations. Because all registration was done by one organization in that time, one centralized server was used for WHOIS queries. This made looking-up such information very easy.

Early WHOIS servers were highly permissive and would allow wild-card searches. You could do a WHOIS lookup on a person's last name and get all the individual people who had that name. Someone could do a query on a keyword and see all registered domains containing that keyword. Someone could even query a given administrative contact and see all domains they were associated with.

On December 1, 1999, management of the top-level domains (TLDs) .com, .net, and .org was turned over to ICANN. At the time, these popular TLDs were switched to a thin WHOIS model. By 2005, there were many more generic top-level domains than there had been in the early 1980s. There are also many more country-code top-level domains. This has led to a complex network of domain name registrars and registrar associations, especially as the management of Internet infrastructure which has become more internationalized. As such, performing a WHOIS query on a domain requires knowing the correct, authoritative WHOIS server to use. Tools to do WHOIS proxy searches have become common. Also, there is a command-line whois client called jwhois which uses a configuration file to map domain names and network blocks to their appropriate registrars.

WHOIS information can be stored and looked up according to either a "thick" or a "thin" data model:

- Thick one: WHOIS server stores the complete WHOIS information from all the registrars for the particular set of data (so that one WHOIS server can respond with WHOIS information on all org domains, for example).

- Thin one: WHOIS server stores only the name of the WHOIS server of the registrar of a domain, which in turn has the full details on the data being looked up (such as the .com WHOIS servers, which refer the WHOIS query to the registrar where the domain was registered).

The thick model usually ensures consistent data and slightly faster lookups (since only one WHOIS server needs to be contacted). If a registrar goes out of business, a thick registry contains all important information (if the registrant entered correct data, and privacy features were not used to obscure the data) and registration information can be retained. But with a thin registry, the contact information might not be available (unless adequately escrowed), and it could be difficult for the rightful registrant to retain control of the domain.

If a WHOIS client did not understand how to deal with this situation, it would display the full information from the registrar. Unfortunately, the WHOIS protocol has no standard for determining how to distinguish the thin model from the thick model.

However the use of the data in the WHOIS system has evolved into a variety of uses which go far beyond the original purpose to offer a fast help service in cae of a technical failure.

Nowadays the use of the WHOIS includes, inter alia:

- Supporting the security and stability of the Internet by providing contact points for network operators and administrators, including ISPs, and certified computer incident response teams;

- Determining the registration status of domain names;

- Assisting law enforcement authorities in investigations for enforcing national and international laws, including, for example, countering terrorism-related criminal offenses and in supporting international cooperation procedures. In some countries, specialized non-governmental entities may be involved in this work;

- Assisting in the combating against abusive uses of Information communication technology, such as illegal and other acts motivated by racism, racial discrimination, xenophobia, and related intolerance, hatred, violence, all forms of child abuse, including pedophilia and child pornography, the trafficking in, and exploitation of, human beings.

- Facilitating inquiries and subsequent steps to conduct trademark clearances and to help counter intellectual property infringement, misuse and theft in accordance with applicable national laws and international treaties;

- Contributing to user confidence in the Internet as a reliable and efficient means of information and communication and as an important tool for promoting digital inclusion, e-commerce and other legitimate uses by helping users identify persons or entities responsible for content and services online; and

- Assisting businesses, other organizations and users in combating fraud, complying with relevant laws and safeguarding the interests of the public.

The contact information for Registered Name Holders are 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).

For example, ICANN requires accredited registrars to collect and provide free public access to the name of the registered domain name and its nameservers and registrar, the date the domain was created and when its registration expires, and the contact information for the Registered Name Holder, the technical contact, and the administrative contact.

The WHOIS database became the subject of critical discussion already in the 1990s, when the database was used for other reasons than the original limited technical purpose. Since its establishment, ICANN is working on an improvement of the WHOIS database service but no progress has been achieved so far.

There are two controversial positions with regard to the WHOIS service which have been unable to bridge so far:

- One the one had there is the camp of privacy and data protection communities which point to the fact that the present WHOIS database is in sharp conflict with the existing data protection legislation, in particular in Europe. They argue that the WHOIS database practice violates the principle of informational self-determination, which was – as an example – introduced in Germany as a constitutional right for individuals. According to this right, individuals can determine what is happening with their personal data. For instance, telephone users can determine whether their telephone number and postal address is listed in public telephone directories. They can decide not to be listed in open directories and quite a substantial number of telephone users have asked not to be listed in public telephone books or yellow pages. This is in accordance with European data protection legislation and protects the individual, inter alia, against unwanted and illegal telephone calls and conversations. The registrant of an Internet domain name does not have such a right. His/her data are published in the open database and everybody can access these data for the various reasons listed above. Critics are attributing in particular spam to the open WHOIS Database which they are seen as an open invitation to cybercriminals. They argue further that the open WHOIS database violates the right to by anonymous on the Internet. As a consequence the WHOIS database would provoke to give false information which would lead to incorrectness of the data stored in the WHOIS and would decrease the value of the service.

- On the other hand is the camp of law enforcement and the communities fighting for the protection of intellectual property against illegal downloading who argue that the open WHOPIS database is a needed instrument and a prerequisite to fight against cybercriminals and cyberterrorists. Only a fast access to the personal data of a registrant plus a strong take down regulation in cases of false data of registrants would allow a quick response in real time to an illegal activity.

ICANN has established numerous working groups and published various studies with more than thousand pages analyzing the various dimensions of the issue, however no consensus could be achieved so far. The two controversial positions seem to be unbridgeable so far.

The proposal for a compromise to establish a so called tiered system with two basic layers - an open and a closed one – did not yet find a consensus. According to this proposal it would be up to the registrant to decide whether his/her data should be in the open or closed database. The closed database would be accessible only to law enforcement and other authorized institutions to access the data in under a certain legal procedure. In particular the intellectual property community is arguing against such a layered system because they fear that they loose time in fighting illegal downloading of protected intellectual property if they have to wait until a judge allows access to the data of a registrant, based on clear evidence of an illegal activity.

ICANN continues to study the various dimensions and to search for an improved and enhanced WHOIS database service. The GNSO Council has now four new studies under consideration:

- on WHOIS Misuse,
- on WHOIS Registrant Identification,
- on Proxy and Privacy services and
- on the implications of non-ASCII registration data in WHOIS records.

A new "SSAC-GNSO Working Group" has been formed. It cooperates with another "Internationalized Registration Data Working Group" which will be studying the feasibility of introducing display specifications to deal with internationalized registration data and will be consulting with other ICANN Supporting Organizations and Advisory Committees when conducting this work. Meanwhile a fifth study area, requested in May 2009 by the GNSO Council, asks that a comprehensive set of requirements for WHOIS service be compiled based on current requirements and a review of previous GNSO WHOIS policy work. This resolution reflects increasing community concerns that the current WHOIS service is deficient in a number of ways, including data accuracy and reliability, as well as in other technical areas noted in recent SSAC reports, such as accessibility and readability of WHOIS contact information in an IDN environment. This work was just initiated in September 2009 and will likely take several months to complete.[28]

In the meantime, some progress could be reached by agreeing on basic definitions of key terms in the Whois discussion.

ICANN has published a number of working definitions for key terms used in the WHOIS debate as follows:

- 1) Illegal or undesirable activities: Illegal or undesirable activities are activities that violate the law somewhere or activities that somebody finds harmful or objectionable.

- 2) Misuse: Misuse is an action that causes actual harm, is the predicate to such harm, is illegal or illegitimate, or is otherwise considered contrary to intention and design of a stated legitimate purpose, if such purpose is disclosed. When applied to Whois data, such harmful actions may include the generation of spam, the abuse of personal data, intellectual property theft, loss of reputation or identity theft, loss of data, phishing and other cybercrime related exploits, harassment, stalking, or other activity with negative personal or economic consequences. The predicate to harmful action often includes automated email harvesting, domain name registration by proxy/privacy services to aid wrongful activity, and support of false or misleading registrant data. Predicate acts might include the use of Whois data to develop large email lists for commercial purposes.

- 3) Commercial Purpose: Related to a bona fide business use. In the Internet context, the bona fide use or bona fide intent to use the domain name or any content, software, materials, graphics or other information thereon, to permit Internet users to access one or more host computers through the DNS: to legally exchange goods, services, or property of any kind in the ordinary course of trade or business; or to facilitate (i) the legal exchange of goods, services, information, or property of any kind; or, (ii) the ordinary course of legal trade or business.

[28] All Whois references can be found under: https://st.icann.org/gnso-council/index.cgi?whois_references

- 4) Proxy and Privacy Services: Proxy and Privacy services provide anonymity and privacy protection for a domain name user. Though the terms are colloquially used interchangeably, there is a difference. Privacy services hide customer details from going into WHOIS. Privacy service providers, which may include registrars and resellers, may offer alternate contact information and mail forwarding services while not actually shielding the domain name registrant's identity. By shielding the user in these ways, these services are promoted as a means of protecting personal privacy, free speech and human rights and avoiding personal data misuse.

- 5) Relay Information Requests: Problems arise from time to time in connection with registered names. Allegations of actionable harm require copyright and trademark owners, law enforcement officials and others to be able to operate through a proxy or privacy service provider to contact the domain name user. Potential "harms" could include suspected fraud, intellectual property rights infringement, or the infringement of other civil or criminal laws. To support the relay of information requests, service providers must have reliable and timely means of communicating with their domain licensees. The ICANN Registrar Accreditation Agreement stipulates that the proxy registrant reveal the identity of the domain licensee upon reasonable evidence of actionable harm or risk liability for resulting harm.

- 6) Falsify Whois Data: Falsifying Whois data is an issue that balances the technical and legal requirements of Whois domain name registration records with the right to registrant privacy. The security and reliability of the Whois data base depends on data accuracy. ICANN therefore expects registries and registrars to collect accurate information and to take required action if false information is discovered or suspected.

- 7) Natural Persons: A real, living individual as opposed to a "legal person" which may be a company, business, partnership, non profit entity or trade association. It is often not clear whether registrants are registering a domain name as a "natural person" or a "legal person" at the time of registration. In the Whois context, personal data refers to any identified or identifiable natural person.

There is no clear perspective when and how the WHOIS debate will come to a final conclusion.

4.2 Security

The security, stability and resilience of the Internet is seen now as the key element and the most important factor in the management of critical Internet resources (CIR). More and more countries see the Internet infrastructure as a critical infrastructure for their national security and economy, similar to water, and electricity management. The functioning of the Internet is meanwhile a precondition for the functioning of the national economy.

Insofar it is not a surprise that the issue of Internet use and the role of the various players, including their rights, duties and responsibilities, has become a public policy issue which is debated both on the national level as well as in international for a as the UN General Assembly.

There is no international recognized definition of Internet security. However there are various dimensions how Internet security is understood on the various layers of the Internet architecture.

- Security and stability of the physical network and Infrastructure
- Security of the management of IP addresses and domain names
- Security of the various Internet applications and services
- Security of the data of Internet users.

The security risks are coming from various corners and include both attacks against the physical infrastructure as well as against the functioning of the application and services: from distributed denial of service attacks (DDOS), hacking and cracking via worms, malware, spyware, viruses to identity theft, steeling of intellectual property and content related crimes like child pornography.

- **Malware** is the most general name for any malicious software designed for example to infiltrate, spy on or damage a computer or other programmable device or system of sufficient complexity, such as a home or office computer system, network, mobile phone, PDA, automated device or robot.

- **Viruses** are programs which are able to replicate their structure or effect by integrating themselves or references to themselves, etc into existing files or structures on a penetrated computer. They usually also have a malicious or humorous payload designed to threaten or modify the actions or data of the host device or system without consent. For example by deleting, corrupting or otherwise hiding information from its owner.

- **Trojans** (Trojan Horses) are programs which may pretend to do one thing, but in reality steal information, alter it or cause other problems on a such as a computer or programmable device / system.

- **Spyware** includes programs that surreptitiously monitor keystrokes, or other activity on a computer system and report that information to others without consent.

- **Worms** are programs which are able to replicate themselves over a (possibly extensive) computer network, and also perform malicious acts that may ultimately affect a whole society / economy.

- **Bots** are programs that take over and use the resources of a computer system over a network without consent, and communicate those results to others who may control the Bots.

With regard to the registration of domain names the issue of accuracy of registered data is important for security. A registry has the right to take down a domain name registration in case of inaccurate data. However, issue like anonymity, false information, identity theft etc. are still unsettled and needs further discussion..

There is a need for enhanced international cooperation, both among governments and among the various involved stakeholders. The Council of Europe Cybercrime Convention has opened the door for a new quality of international (intergovernmental) cooperation however it is not yet a global instrument. Internet security has to be seen today as a joint challenge and a joint responsibility of all UN member states. There will be no national cybersecurity without international cybersecurity.

5 Conclusions & Recommendations

1. The Internet Domain Name Registration Process is a well organized open and transparent bottom up multilayer mechanism which distributes key functions among various players and guarantees the stability of the system. It is recommended that the process is further stabilized and secured by enhanced collaboration among all involved stakeholders, by strengthening the oversight role of ICANN taking into account the privacy rights of individual registrants.

2. A serious problem is the protection of privacy of the registrants in the domain name registration process, in particular in the WHOIS database. It is recommended to search for a consensus among all involved parties and stakeholder groups which would allow both the protection of private data of individual registrants as well as the opportunity of law enforcement to use the database to fight cybercrime and cyberterrorism.

3. A key player in the domain name registration chain is the registrar/ISP which operates under a given national jurisdiction. The registrar is embedded into a mechanism of bilateral contracts in a trilateral environment which links it both to ICANN, the TLD registry and the registrant. It is recommended to study further the future role of the rights, duties and responsibilities of registrars/ISPs with regard to the management of personal data of registrants.

4. A key issue in the domain name market that its further growth does not undermine the stability, security and resilience of the Internet. It is recommended to study further in depth the security implications with regard to the broadening of the domain name space by introducing new gTLDs and iDNs, implementing DNSSec and IPv6 as well as consequences from various criminal activities like DDOS, malware, botnet etc for the DNS registration system.

5. The role of governments in the domain name registration process is mainly to take care of the public policy implications. Its main responsibility is to create an environment which enables all parties to contribute to the further growth of the Internet and to bridge the digital divide. This includes a special responsibility for public policy issues related to the domain name registration process as protection of human rights, and here in particular freedom of expression and privacy of individual registrants, guaranteeing, in cooperation with ICANN, fair competition among the service providers both on the registrar and registry level and promoting the security and stability of the Internet. An enhanced cooperation both among the various stakeholders as well as among governments themselves is recommended.