Dr Paul Twomey
President and Chief Executive Officer
ICANN

Keynote Speech
ITU/MII Seminar on Internet Development and Online Environment
Zhengzhou, China
October 11, 2006

Good morning

I'm delighted to have been invited to give the keynote address at this important seminar. The Internet is evolving at such a breath-taking pace; we all must continue to stay aware of how far it has come and where it is going.

Before I start, I'd like to say how pleased I am to be in Zhengzhou.

So, I thank you for the opportunity to tell you about some key developments in the realm of the Internet, especially as it relates to ICANN's areas of responsibility: the Internet's system of unique identifiers. I would particularly like to make some observations on the four themes of this seminar from the perspective of the Internet address and naming system.

May I remind you of ICANN's mission, and its four closely linked goals?

ICANN — the Internet Corporation for Assigned Names and Numbers — is the international multi-stakeholder organisation responsible for the technical management and oversight of the coordination of the Internet's domain name system and its unique identifiers.

It is an internationally organised public benefit, non-profit entity responsible for coordinating the Internet's —

- Internet Protocol (IP) address space allocation;
- protocol identifier assignment;
- generic (gTLD) and country code (ccTLD) top-level domain name system management; and

- Root server system management functions.

In fulfilling its mission, ICANN is guided by four founding principles —

To preserve the operational stability and security of the Internet, particularly the Domain Name System;

To promote competition and choice for registrants, especially in the generic top level domain arena;

To achieve broad representation of global Internet communities;

And, to develop policy appropriate to its mission through bottom-up, consensus-based processes.

So the perspectives I share with you today will be within that framework.

I think we all agree that the Internet is unique from all other media we use to communicate, or to conduct business, or to store and transmit data.

It is unique in the way it operates; that is, it is a single, globally interoperable medium that has led to innovations in commerce and communication, and in our social lives.

It is also unique in the way it has operated since its inception. From the pioneering days of the ARPANET in 1969, the technologists, funders and, later, business people who built the Internet have operated according to a set of common values. Some of these values include a commitment to:

- Ensuring a single, end-to-end interoperable Internet;
- Bottom-up technical policy making and decision making;
- Cooperation, coordination, and consultation among participants and groups pushing forward initiatives;
- Global efficiency in the allocation of resources such as IP addresses;
- Encouraging innovation, particularly at the edge of the network;
- And building on the many layers of protocols to ensure the stability of the whole construct.

These values were key to the successful rapid development of the Internet. In the late 1990’s, a new network was choosing to link to the Internet every seven hours. Today's Internet is a vast collaboration of many components built on many layers by many combinations of business and technical skills.

Today, over 200,000 private networks make up the global Internet. The coordination, collaboration, and cooperation of many entities are vital to the Internet's successful operation, and have been integral to its design since the earliest research network.

ICANN itself is a unique model of governance. Its approach, which involves cooperation among multiple technical, business, civil society and government stakeholders, has supported explosive growth in the use of the naming and addressing system.

Today, there are more than 1 billion users of the Internet.

The root system that ICANN helps coordinate supports about 30 billion resolutions per day, nearly 10 times the number of phone calls in all of North America each day.

This rapid growth in use also supports a continued increase in e-commerce, Internet businesses, and new markets. Today the users of the Internet conduct some 2 trillion US dollars worth of e-commerce every year.

While I realise each of panellists and speakers will discuss these topics later, I would now like to address from an ICANN perspective the four themes of the seminar:

- Development and application of Internet technologies
- Effective measures to combat spam
- Protection of Internet Domain Names and Intellectual Property Rights
- Protection of Children from unhealthy Internet contents

1. The development and application of Internet technologies.

Two new developments are worth noting under this theme:

- The availability of Internet Protocol version 4 and deployment of the new Internet Protocol version 6, and;
- The introduction of Internationalized Domain Names.

IPv4 and IPv6

Globally, regional distribution of IP addresses is the responsibility of the five Regional Internet number Registries. However, IP addressing and address policy are subjects that remain clouded by common misunderstandings.

The most prevalent of these involve IP addressing in the Asia Pacific region, or in specific parts of the region such as China. According to much of the world media, IPv4 address space will soon run out, although when "soon" will occur is a matter of conjecture. Still, this 'scare' makes a great headline.

In contrast, expert analyses has responded to recent volatility in consumption rates of IPv4 by projecting that the unallocated pool of IPv4 addresses could last as long as 4 to 7 or even 15 years. Even with increased consumption rates, there is no immediate scarcity crisis – but network operators do need to plan now for an environment where there may be a scarcity premium on IPv4 addresses. These projections are certainly not predictions, as the future of the Internet is unknown. Still, from tracking several years of IPv4 address consumption, they are important results.

At first, IPv4 address space was allocated according to a class-based system, with address blocks available in three sizes with most allocations far exceeding the immediate needs of the networks. At the time, address conservation was not a priority and during the 1980s and early 1990s many large organisations, most of them in the United States, received the largest size of address blocks. These organisations included large universities such as MIT and Stanford, as well as corporations like Apple Computer and Boeing. But with the rapid growth of a globally pervasive, commercial Internet, the addressing community came to realise that this early policy would not support future growth. They changed policy to a needs based allocation system that has been very successful in supporting the rapid growth of the last 15 years or more.

In the intervening years the belief has become widely held that Chinese organisations hold a combined total of less address space than one of these early "legacy" holders. This has not been true since the beginning of this century. The only factor inhibiting allocation of address space was the comparatively slower early growth of China's Internet activity. Today, China holds the equivalent of more than four of these largest IPv4 address blocks, and this number is constantly increasing. Indeed, the massive growth of the Internet in China is sure to continue for many years to come.

Another myth says there is an IP address shortage in China. However, to claim a shortage implies that addresses are somehow not available, which is not true.

Address space is allocated throughout the Asia Pacific region in response to allocation requests, and very few requests are turned down. When they are, it is normally because the requestor is an end site that does not meet the basic criteria for an allocation. In recent years, China has been receiving addresses at a faster rate than any other economy in the world, followed by Japan, then the USA.

The allocation of address space to Regional Internet Registries from the IANA, and to ISPs from the RIRs is a continual process, and all allocations are made according to demonstrated need under a consistent set of policies. There is no pre-allocation of addresses to any economy or region in the world, meaning that a shortage in any one country or economy because of allocations in another is simply inconceivable.

For example, by July of this year, a total of 74,043 minimum allocation size IPv4 prefixes were allocated, of which APNIC received 12,719, the third largest allocation for that period. In fact, during 2006 APNIC has allocated more address space than any of the other regional registries, and China is currently the fastest growing destination for IPv4 address space.

Whether you believe the pool of IPv4 address spaces will dry up this year or 20 years from now has been made increasingly irrelevant by the deployment of IPv6, the next generation IP addressing scheme.

Even though IPv6 is still relatively new, its adoption has become a government initiative for China, Japan, and Korea, among many other countries. In fact, to date the Asia Pacific region has received the second highest number allocation of IPv6 address spaces, 448 out of a total of 1,577 allocated to the RIRs. In addition, local Internet communities are pushing its adoption.

An IPv6 address is 128 bits, which makes it capable, at least in theory, of letting users put an address on 5×10^{28} (50 octillion) different real or virtual objects. And remember, IPv4, at a mere 4.3 billion still has plenty of address space available.

Of course, this huge number is meaningless, both in terms of the human mind’s ability to comprehend its magnitude, and in how IPv6 will be used. The actual amount of IPv6 address space being used is a tiny fraction of the total theoretical address space.

The primary reason for the Internet engineering community designing this huge amount of space is to facilitate users connecting to the network in ways that were never anticipated when IPv4 addressing was introduced. IPv6 addressing enables the continued growth of existing networks and creates room for innovation in the global Internet.

Just last month, the Board of ICANN ratified a global policy for the allocation of IPv6 addresses by IANA to the regional Internet registries. Under this policy, IANA will allocate /12s to the RIRs, which means that each of the five RIRs will be able to assign more addresses to their users than the combined total of all the IPv4 addresses that have been assigned to date.

In using these addresses, the RIRs are currently assigning a minimum of a /32 prefix to their customers, the local Internet registries, which means a potential 1,048,576 RIR-to-LIR assignments. And this is a tiny fraction of the IPv6 address spaces available.

IPv6 address distribution is the outcome of development through the RIR community’s bottom-up consensus approach, which saw its adoption as a policy development process. That means ICANN’s stakeholders and constituencies have shaped this policy from day one, and it provides certainty to Internet registries and their customers, who include ISPs and users, that demands for allocations of Internet address space can be met for many years to come.

Internationalized Domain Names

One of the most challenging issues for the Internet's security, stability, and growth is internationalized domain names, or IDNs, as they are known.

Historically, Internet domain names were restricted to ASCII characters — that is, a–z, 0–9, and the hyphen).

However, with the increasing use of the Internet in all regions of the world — and by diverse linguistic groups — the need for multilingual content and the capability to support multilingual use of the Internet is still increasing. Of the concerns about multilingualism, some refer to content in numerous languages, alphabets, scripts, and character sets; others to keywords in search and directory systems, and others again refer to domain names.

There is an extensive IDN program under way through ICANN's multi-stakeholder model to internationalise the domain name identifiers. Its purpose is to allow users to register and use domain names based on their local script. This includes users of languages based on right-to-left based scripts, of which the most widespread is Arabic — and also users of languages based on non-alphabetic scripts, of which the largest single contemporary language is Mandarin Chinese.

However, the implementation of IDNs has been complicated by the myriad of technological, policy, and cultural issues that surround it.

To help coordinate all the groups working on these internationalisation issues, ICANN has held IDN workshops around the world and will continue to do so to gather information about the needs and expectations of users and stakeholders, and to inform the Internet community of progress in all aspects of IDN implementation.

As I said earlier, when the Internet was developed it was based on the LDH rule for the domain names. This means that domain names could only contain the letters a–z (L), the digits 0–9 (D), and the hyphen (H).

In 2003, an IETF technical review opened an opportunity for this character set to be expanded at the second level of a domain name.

Standards, protocols, and guidelines have been developed for implementing IDNs in second level domain names. The experience with this implementation is now being reviewed to see whether the same technology can be used with top-level domain names.

For Chinese speaking users, this means the ability to use domain names that consist entirely of Chinese characters. However, the "http://" will remain in Latin characters.

Before all this is possible, technical tests must be performed to ensure that no stability or security issues occur — in other words, we want to make sure that such implementation in the DNS root zone does not adversely affect the way we use the Internet today.

I want to recognize Professor Hualin Qian of the Chinese Academy of Sciences, a member of the ICANN Board, who is co-chairing a President's Advisory Committee of experts on IDNs. This Committee is overseeing the technical test program for IDNs in the Root Zone and its work is expected to continue through to 2007.

However, I want to remind you that before IDNs can be implemented in the Root there are still many stability, intellectual property, and other issues to be resolved before we can take advantage of this advance in Internet accessibility.

Some of these relate to online applications that allow the use of these IDNs. For example, if browsers such as Firefox or Microsoft Internet Explorer are not upgraded, then IDNs cannot be used to access websites. On the plus side, Microsoft Internet Explorer has finally made the second level technology available in its beta-7 version, four years after the registries introduced second-level IDNs in 2003.

We also need to be aware of the opportunities IDNs offer for spoofing end users, utilizing similar looking, yet foreign, characters to those in the end-user's language. This is only one of many implementation challenges which need to be addressed.

ICANN's Generic Names Supporting Organization is working through the implementation policy issues involved in fully liberalizing the introduction of generic Top Level Domains, including in IDNs. ICANN's different constituencies, including the very important Governmental Advisory Committee, will review this work. This work is expected to be completed by the beginning of 2007.

I have dwelt on technical security and stability of the Internet because this is one of ICANN's core values. However, when it comes to internationalisation we are also facing several policy issues. We are working with our supporting organisations, GNSO and ccNSO as well as the GAC, on these issues.

Our vision, when all these obstacles have been cleared, is for any child in China, or any country around the world, to be able to access domain names using their local script.

2. Effective measures to counter spam.

ICANN's mission is to coordinate the Internet's system of unique identifiers. As such it is focused on a narrow technical function.

Many aspects of Internet Governance do not lie within this mission. For instance, ICANN is not responsible for content on the Internet. As such spam is something outside ICANN's remit.

However, there is one technology the introduction of which ICANN is supporting and which may contribute to diminishing somewhat the opportunities to fraudulently interact with users through spam or phishing.

This technology, designed to improve Internet security, is DNSSEC, or DNS security extensions. ICANN has been facilitating the implementation of DNSSEC through the work of its Security and Stability Advisory Committee and through hosting regular information sharing briefings and workshops around the world.

DNSSEC relates specifically to a few parts of DNS transactions, those concerned with initiating transactions between and among devices on the Internet.

One area is called transaction signatures, which concerns itself with authenticating the source of a zone file on transactions between DNS servers such as primary and secondary name servers.

A second area is the authentication of a reply to a DNS query to ensure that the end user gets the answer from a source that has been signed, or verified as true, thus proving that the answer has not been tampered with.

In the case of an answer to the question: “What is the IP address for www.icann.org?” this would give the end users certainty that the answer received is from the correct zone file and hence authentic. A correctly signed or verified signature offers a level of trust in the answer a user receives.

All this is aimed at improving the security of Internet transactions and the transmission of all kinds of data that must be protected. Under the aegis of DNSSEC, users will be assured of greater safety and security for all their Internet transactions.

DNSSEC is only part of the answer that will lead toward a more secure Internet. Beyond building trust in the domain name system we also need to take that same approach toward other parts of the layered system that is the Internet protocol. Secure routing protocols and more secure operating systems, software and hardware are all parts of the solution.

Each is important in its own way.

DNSSEC was not designed to protect comprehensively Internet users from spam and phishing, arguably the biggest tools of thieves making use of the Internet today. While in an ideal world, a technical solution at the core of the infrastructure may be desirable; it also could result in unintended consequences affecting the flow of traffic and desired communications. Spam and phishing are not merely technical issues that are open to technical solutions. They are behavioral aspects relating to the use of the Internet and as a result, they are social and legal issues as well, and must be dealt with as such.

Let me give you two examples.

With respect to phishing, this past July the Anti-Phishing Working Group reported more than 23,670 unique phishing reports. During that same month, 154 brand names were hijacked to try to make phishing campaigns appear more authentic.

This is a record, and the trend appears to be growing at a considerable pace. This translates into increasing potential for Internet users' private information to be stolen, as well as increased legal costs for individuals and businesses alike.

ICANN's experience with spam may resonate with most of you. Of course, all our e-mail addresses are necessarily public, and therefore we are subject to huge volumes of spam along with our legitimate e-mail.

For example, in one recent week we received roughly 1,400,000 e-mails. Of those, about 200,000 cleared the first level of spam and virus checks. That's only 15 percent of the total, which means an 85 percent rejection rate. If you subtract internal e-mail from this equation, the rejection rate for external mail is even higher.

Along the path to our in-boxes, mail continues to be sorted and filtered and much more mail is rejected. In the end, at least 90 percent of our incoming e-mail is spam and virus output.

As you can tell, our IT team has implemented several layers of technical solutions, but even these are no more than a necessary but expensive bandage. So the real solution lies elsewhere.

Recently, at least 19 countries took the offensive in making it illegal to deliver spam, and many other countries are investigating enforcement measures and penalties.

Increased user awareness can also be a major force in combating spam and phishing. Developers are also engaged in applying their best technology.

The Organisation for Economic Co-operation and Development has done much work on spam, including in relation to the development or review of anti-spam legislation, and is currently developing an anti-spam toolkit (**www.oecd-antispam.org**), an instrument that helps governments, regulators and industry players orient their policies relating to spam solutions. The International Telecommunication Union itself has also addressed spam, and numerous governments are adopting anti-spam legislation — the Australian government being an excellent example.

But a more universal approach to solving these problems will have to come from government engagement and through partnerships between governments and the private sector.

3. The protection of Internet Domain Names and Intellectual Property Rights

As to the protection of intellectual property rights, again, ICANN has no stewardship. We are not a legislative body and have no power to create intellectual property law. Through our bottom-up consensus seeking processes, however, our constituencies have helped us develop and implement the Uniform Domain Name Dispute Resolution Policy.

The UDRP was originally intended to provide for the resolution of trademark and service mark disputes in domain-name registrations in the global top-level domains. However, in nearly seven years the UDRP has been such a success that more than 20 country-code top-level domains have adopted the UDRP — or a form it — to resolve domain name disputes.

The UDRP offers a mandatory, low-cost administrative procedure to resolve certain claims — namely, claims of abusive, bad faith registration of domain names identical or confusingly similar to trademarks or service marks. Internet users are bound by the UDRP when they enter into the agreement to register a name in the global top-level domains.

Since its implementation in October of 1999, the UDRP has been the instrument for resolving more than 17,000 claims involving over 40,000 domain names.

The UDRP administrative procedure, a speedy, cost-effective alternative to the courts, is very straightforward and is handled almost entirely online. Proceedings are typically resolved within 45 to 90 days, much faster than with traditional litigation.

Any trademark holder who believes he has a legitimate case first files a claim with one of four ICANN-approved dispute resolution service providers. These service providers are —

The World Intellectual Property Organization, the United Nations agency, based in Geneva, Switzerland. WIPO has heard more than 9,500 UDRP cases since 1999, and if related dispute proceedings are considered, WIPO has resolved more than 25,000 total cases over 33,000 domain names.

The National Arbitration Forum, based in Minneapolis, Minnesota, in the United States is the second largest dispute resolution provider. NAF has heard over 7,000 cases.

The CPR Institute for Dispute Resolution, in New York. CPR has heard more than 140 cases.

And the Asian Domain Name Dispute Resolution Centre, or ADNDRC, which has offices in Hong Kong and Beijing — and newly opened office in Seoul. Tim Cole, ICANN’s Chief Registrar Liaison, and Donna Austin, ICANN’s ccNSO Policy Officer, were present at the opening. Since its establishment in 2001, ADNDRC has heard some 150 cases, offering services in Chinese, Korean, Japanese and English.

Depending on the completion of contract negotiations, the launch of the dot-asia sponsored TLD may result a new wave of domain disputes in the Asia Pacific region, and dispute resolution service providers will have their work cut out for them.

Dispute resolution service providers assign an impartial arbitrator or, in some cases, a three-member panel for each case. Arbitrators review the submissions from the complainant asserting trademark rights in the domain name, and the respondent who has registered the domain name.

After reviewing the submissions from both parties, relevant law and prior decisions, the panel issues a written opinion, which is delivered to the parties and also posted on the service provider’s website to ensure that the outcome is open to the public. Such transparency is fundamental to the success of the UDRP.

Of the 17,000 cases heard in the seven years the UDRP has been in effect, complainants have won more than 83 percent of the time, leading to the transfer or cancellation of the domain name. This result is due in part to the large number of cases that are uncontested by the respondent. In cases where a respondent defended its rights and legitimate interests in the registered domain name or names, the result has been more balanced, with over 50 percent of contested decisions resulting in transfer to the complainant.

There have been a number of related dispute resolution policies develop out of the UDRP. As an example, a number of new gTLDs have adopted sunrise dispute resolution policies, and these policies share their fundamental structure with the UDRP.

When new top-level domains are launched, most registry operators offer a limited sunrise period. This is the time when anyone with a registered national trademark can apply through a registrar for a top-level domain name corresponding to the trademark.

At this time, and for a period specified by the registry operator — which is typically 120 days — any third party can challenge a registration based on criteria usually set forth by the individual registry operator.

As with the UDRP, the challenge procedure is administered by a dispute resolution service provider such the WIPO. Between 2001 and 2002, the dot-info registry used a sunrise period to resolve over 15,000 domain name disputes.

The disputing parties have the choice of trying the case in a court of law, or they can submit it for resolution to the UDRP or through a dispute resolution process selected by the operator and modelled on the UDRP.

More and more we are seeing the UDRP’s simple, straightforward, quick and equitable processes being adopted or adapted throughout the top-level domains. We are, in fact, seeing this dispute resolution process being applied across the Internet.

There is a substantial argument to be made in favour of sponsored TLDs, which can impose stricter eligibility requirements, thus reducing the problems of cyber squatting and fraud that have become rife in unsponsored gTLDs, and by extension limiting the potential for dispute. The creation of industry exclusive spaces — and the enforcement of this exclusivity — also vastly mitigates the need for defensive registrations.

Still, when challenges arise, the UDRP has proven to be a successful mechanism is in place for resolving disputes.

4. Protection of children from unhealthy Internet content

Protecting our children from websites containing offensive or harmful content is a concern for all of society. Issues of content, though, are not within ICANN's charter to coordinate the Internet's naming and addressing system and have nothing to do with the interconnectivity of single global Internet.

That being said, an array of child protection solutions is being tried, with varying degrees of success.

One such attempt involved several advocates proposing controlling content through special top-level domains. But the laws defining what constitutes harmful or offensive content vary from country to country, and even within a country or a culture. The use of specialised Top Level Domains has foundered on the rocks of this international diversity.

For example, when ICANN was asked to consider approving the dot-kids domain, one of the stumbling blocks became the difficulty in distinguishing between harmful and beneficial content for what would be a globally available top-level domain.

After much debate, the United States adopted an alternative approach that placed dot-kids under the shelter of its country code top-level domain, which gave us "kids-dot-US."

So while dealing with child protection issues in relation to domain names on a national level may work, "all the problem material under one generic Top Level Domain, or all the child-suitable content under one generic Top Level Domain" approaches proved not scalable on a global level.

As I am sure other speakers will explore, other solutions being implemented include addressing content on the layers above ICANN's remit through software filters that can be installed on individual computers or by Internet service providers or at the discretion of parents. Of course in different countries with differing traditions, such technical approaches are also being supported by legislation.

But as I have said several times already, issues of content are not ICANN’s business.

Conclusion

In summary, ICANN is just one of many organisations involved in making sure that the Internet operates optimally and is available for all users. Although we have a vested interest in the issues affecting continuing global interoperability, governance and accessibility, ICANN has a clear core responsibility — the security, stability, and responsible evolution of the Internet.

It is the stakeholders, communities, and operators who ensure our successes, who innovate and who resolve the issues. ICANN’s responsibility is to make sure all these entities have a voice in the vitality and longevity of the Internet system of unique identifiers.

The Internet’s success will depend on maintaining the values that made it the unique medium we rely on today — and those values thrive in an environment that fosters innovation on the edge and global interoperability at the core.