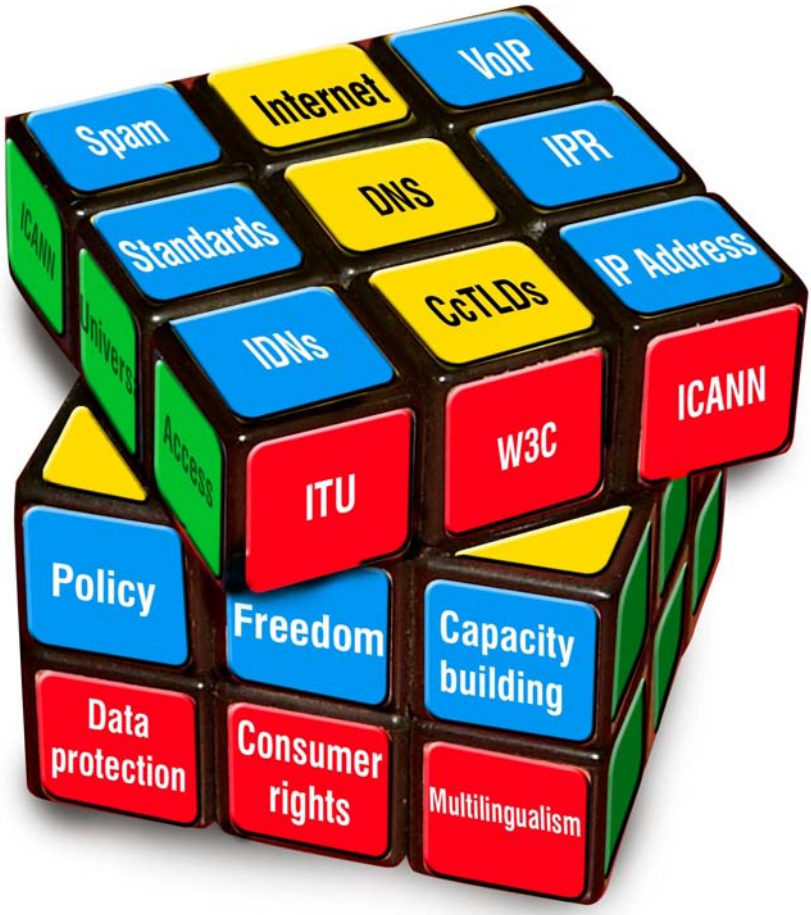
ELSEVIER

UNDP



Internet Governance

A Primer

Akash Kapur

Foreword by

VINTON G. CERF

Asia-Pacific Development Information Programme
e-Primers for the Information Economy, Society and Polity

Internet Governance
A Primer

Akash Kapur

Foreword by

V I N T O N G. C E R F

Asia-Pacific Development Information Programme
e-Primers for the Information Economy, Society and Polity

Web: www.apdip.net
Email: info@apdip.net

ELSEVIER
A division of
Reed Elsevier India Private Limited
17A/1, Lajpat Nagar IV,
New Delhi 110 024
Tel: 91-11-26447160
Fax: 91-11-26447156
Website: www.asiaelsevier.com

ISBN-10: 81-312-0076-6
ISBN-13: 978- 81-312-0076-6

Academic Press, Butterworth-Heinemann, Digital Press, Focal Press, Morgan Kaufmann, North Holland and Pergamon are the Science and Technology imprints of Elsevier.

Printed and bound in India.

TABLE OF CONTENT

FOREWORD

Since its origins over 30 years ago, the Internet has become a major new global telecommunications infrastructure. It is no wonder, then, that it has become a central topic in the more general discussion being held under the auspices of the Information Society. A World Summit on the Information Society (WSIS) was first held in December 2003 in Geneva. At that Summit, a number of Millennium Development Goals (MDGs) were discussed, focused on harnessing Information and Communications Technology (ICT) for the benefit of the world's population. The Internet, seen as a prototype for the technologies that would underlie the Information Society, understandably became a focal point (and a flashpoint) of discussions. Ultimately, in response to debates over the concept of "Internet governance", a Working Group on Internet Governance (WGIG) was established, with the objective of defining the term and providing input to the second phase of the World Summit, planned for Tunis in November 2005. The Working Group released its report on 18 July 2005 and offered a definition of Internet governance as well as some options for approaches to it. The primer you have before you is intended to provide background on the Internet and its operation as a contribution to the dialogue underway in preparation for the next Summit.

The Internet is a global, distributed system of hundreds of thousands, if not millions, of independently operated and interconnected computer communication networks. All of these networks use a standard set of protocols, sometimes referred to as the TCP/IP protocol suite. TCP and IP are the core protocols of the Internet and had their origins in research sponsored by the US Defense Advanced Research Agency in 1973. It is a system that, by design, is relatively insensitive to national boundaries.

For most of its existence, the Internet has been developed in the private sector with very light oversight on the part of the US Government. The official roll-out of the system occurred on 1 January 1983 in the US and at locations in the UK and Norway. By 1994, the Internet was becoming available to the public through commercial networks, and by 1995, a collection of commercial, interconnected public Internet backbones had replaced the private, US Government-sponsored backbone. The scene was set for the so-called "dot-com boom" of the late 1990s. During this period, massive amounts of capital went into "Internet" companies, many of them bereft of serious business models other than a plan to go public. By April 2000, the bubble had burst. But the Internet continued to grow, even during the financial winter following the madness. Amidst the hyperbole, some very successful Internet businesses thrived or were born (e.g., Amazon, eBay, Google). Not counting early research in the 1970s, Voice over Internet Protocol (VoIP) arrived in 1993 but did not really take off until 10 years later, threatening to disrupt the century-old business model of the local and inter-exchange carriers. As the network and its applications became more widespread, and as the global economy began to rely upon its operation, governments began to realize that this new infrastructure, and what was done with it, might be tactically and strategically important to the well-being of their citizens.

The Government of Tunisia called for the second phase of WSIS, not focused solely on the Internet, but on the more general notion of a global economy interlinked in a web of information and the ability to process it with powerful, programmable and often portable tools. As the discussions unfolded in Geneva in 2003 and in regional fora, debates ensued as to the meaning of "governance" in this online environment. Particular focus was placed on Internet governance and the role that the Internet Corporation for Assigned Names and Numbers (ICANN) plays in that arena.

In the course of the WSIS debates, there have been calls for increased governmental oversight and even regulation of the Internet. It is important to recall that this is a network of hundreds of thousands of networks, not a single entity run by a single organization. It has operating components around the world. It has over a billion users. It is, by design, distributed and its components operated by a vast range of government, private sector and academic organizations. Few would dispute the importance of the Internet and its content to a wide swath of modern society. It is therefore vital that in the debates surrounding the perceived abuses of the Internet, we do not destroy all that is so beneficial in this system of systems.

One of the central reasons for the Internet's success thus far has been its largely apolitical management.

It seems important that any modifications to the general oversight and operation of the Internet avoid unnecessary and disruptive politicization. The Internet should remain a key infrastructure and not become a political football, subject to disputes between or among countries. We should build on the existing systems and bodies that have thus far served the Internet community with reasonable success. With few exceptions, most of the public policy issues associated with the Internet lie outside the purview of ICANN and can and should be addressed in different venues. For example, 'spam' and its instant messaging and Internet telephony relatives, 'spim' and 'spit', are pernicious practices that may only be successfully addressed through legal means, although there are some technical measures that can be undertaken by Internet Service Providers (ISPs) and end users to filter out the unwanted messages. Similarly fraudulent practices such as 'phishing' and 'pharming' may best be addressed through legal means. Intellectual property protection may, in part, be addressed through the World Intellectual Property Organization (WIPO) and business disputes through the World Trade Organization (WTO) or through alternative dispute resolution methods such as mediation and arbitration.

As these examples suggest, there can be little doubt that the development of a global Information Society will require extraordinary cooperation, collaboration and coordination. The Internet and its many players illustrate this observation and draw attention to what is possible when a spirit of cooperation can be fostered in the long term.

Only through understanding the full range of players in the Internet arena, their roles, responsibilities, authorities and limits of capabilities can we fashion reasonable outcomes for Internet governance and, more generally, an agenda for the development of an Information Society. This primer represents contributions towards the dialogue that is needed to frame Information Society goals and the methods to achieve them. The participants in these dialogues have an opportunity to help shape a constructive approach to the opportunities before us. We can but hope that they will take up the challenge and pursue the MDGs in a positive and successful fashion.

Vinton G. Cerf
Chairman of the Board, ICANN

PREFACE

At the start of 2005, there were an estimated 750 million Internet users worldwide. This figure is expected to grow exponentially in the coming years, particularly in the Asia-Pacific region, home to over half the world's population. In fact, the Asia-Pacific region already contributes a larger share of users (about one-third of the total) than either North America or Europe.

Inevitably, such numbers will have a profound impact on the structure and use of the Internet. In turn, this impact will have a transformative effect on development around the world. Making the Internet work for sustainable human development, therefore, requires policies and interventions that are responsive to the needs of all countries. It requires a strong voice from different stakeholders and their constructive engagement in the policy-making processes related to Internet governance.

Achieving these goals is a challenge, especially for developing countries who participate in the governance process at a disadvantage. Most of the foundational rules of the Internet are already well-established, or under long-term negotiation. Newcomers to the Internet have had little opportunity to generate awareness among stakeholder groups, mobilize the required policy expertise and coordinate strategies for effective engagement.

Developing countries are further challenged by the global nature of the Internet, which means that many areas of governance require cooperation at the global level, often in fora dominated by the developed world. Furthermore, participating in conferences and meetings at these fora is often expensive, or otherwise difficult for stakeholders from developing countries.

In sum, the continuing march of Internet governance threatens to leave behind developing countries. Fortunately, such an outcome is not inevitable. The Open Regional Dialogue on Internet Governance (ORDIG) is a response to this threat, and an attempt to transform the challenges of governance into an opportunity. Since October 2004, ORDIG has gathered and analyzed perspectives and priorities through an extensive multi-stakeholder and participatory process that has involved more than 3,000 people in the Asia-Pacific region. This represents the first step in greater involvement by the region, and particularly by traditionally under-represented nations.

ORDIG activities thus far have included a regional online discussion forum involving more than 180 participants; a multilingual survey on Internet governance that collected 1,243 responses from 37 countries; a series of sub-regional consultations; and a variety of research on various topics and issues such as access costs, voice over Internet protocol, root servers, country code top-level domains, internationalized domain names, IP address management, content pollution, and cybercrime.

Based on these activities and research, ORDIG has produced a report entitled, "Voices from Asia-Pacific: Internet Governance Priorities and Recommendations", which was considered by the High Level Asia-Pacific Conference for WSIS in Tehran, 31 May-2 June 2005, and was tabled at the Fourth Meeting of the UN Working Group on Internet Governance in Geneva in June 2005.

This primer is another important output. It is designed to help all stakeholders (government, private sector and civil society) gain quick access to basic facts, concepts and priority issues, laying the foundation for a comprehensive understanding of Internet governance issues from a distinctively Asia-Pacific perspective.

We welcome and encourage feedback from any constituency in the Asia-Pacific region. For more information on ORDIG, please visit the online knowledge portal at www.igov.apdip.net or contact info@igov.apdip.net.

Shahid Akhtar
Programme Coordinator, UNDP-APDIP

INTRODUCTION

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

— John Perry Barlow, "A Declaration of the Independence of Cyberspace", 1996

Almost a decade has passed since Barlow wrote his famous Declaration of Independence. Those were heady times. Netscape's phenomenal Initial Public Offering (IPO) had taken place a year earlier, launching a thousand (often short-lived) fortunes, and apparently transforming the social, economic and even political landscape. Every week seemed to herald a new innovation, a new technology or company that appeared to vindicate Barlow's utopian vision. Indeed, as Lawrence Lessig argued in his influential book, *Code and Other Laws of Cyberspace,* the rise of the Internet was accompanied by a euphoria akin to that which followed the collapse of the Berlin wall[1].

Since that time, the Internet has significantly matured. Today it is no longer a novelty or a curiosity; and, while significant economic opportunities remain, the get-rich frontier mentality of the 1990s is a fading memory. Indeed, for many users, particularly those in developed countries and urban centres, the Internet is so woven into the fabric of daily life that it is easy to forget just how special and transformative the network really is. In a sense, the Internet has shifted from the foreground to the background: as a global infrastructure that drives our economic and social life, it is today the engine behind many of the events and developments that we consider most newsworthy or attention-grabbing.

It is easy, given such conditions, to take the Internet for granted. But in fact, for all its staying power and phenomenal growth, the network remains in some senses a delicate, and even fragile, phenomenon. It relies on a bedrock of technical standards that are the outcome of a finely balanced consensus among users, government officials, business, and members of the disparate technology communities. Its global reach – what experts call the network's global seamlessness – must always navigate the shoals of competing legal jurisdictions and various concerns over national sovereignty. More generally, a host of agreements, laws, treaties, institutions, technical protocols, and non-binding precedents function in a tenuous coalition to ensure the smooth functioning and stability of the network.

Put together, it is these various forces, which collectively determine what can and cannot happen on the network, that constitute the broad concept of Internet governance. In what follows, we offer an overview of that concept, discussing its history, the issues at stake, and the various actors involved. One of the challenges, in any such discussion, is providing some conceptual clarity to what is often a nebulously defined field. As we shall see, there exist a multitude of competing definitions of Internet governance, and a similarly vast range of actors. Moreover, the issues at stake are so broad and varied that it is difficult to discuss them in any systematic manner, especially in a brief and general primer such as this one.

Section I, therefore, attempts to provide some definitions, and offers an analytical scheme by which to conceptualize the topic at hand. Internet governance, it suggests, can be understood through a metaphor of "layers" – a division of issues and actors into three broad categories, each of which corresponds to a different facet of the network. As the text explains, there exist many possible layers. This primer chooses to divide the network into three layers: infrastructure, logical, and content.

Section II addresses some of the specific issues at stake in Internet governance. It also discusses some of the actors – the bodies, institutions and fora – involved in these issues. In order to provide a certain

[1] Lessig, Lawrence (1999), *Code and Other Laws of Cyberspace*. New York: Basic Books, p. 3.

amount of order to the crowded field of issues and actors, the discussion is organized by the previously mentioned layers.

Section III discusses an issue of particular relevance to readers in the Asia-Pacific region: the interaction of Internet governance and development. It attempts to show how governance decisions can have social and economic ramifications, and it suggests some steps that can be taken to enhance developing country participation in Internet governance.

Section IV returns to the broader picture. It explains a number of concepts, and evaluates some models for governance. Finally, Section V, the Conclusion, offers some best practices, and considers the future of Internet governance.

I. BACKGROUND AND KEY CONCEPTS

What is "governance"?

The term governance often gives rise to confusion because it is (erroneously) assumed that it must refer solely to acts or duties of the government. Of course, governments do play an important role in many kinds of governance. However, in fact, the concept is far broader, and extends beyond merely the State. For example, we have seen increasing reference recently to the notion of "corporate governance", a process that involves oversight both by the State and by a host of non-State bodies, including corporations themselves.

Don McLean points out that the word governance derives from the Latin word "gubernare", which refers to the action of steering a ship.[2] This etymology suggests a broader definition for governance. One important implication of this broader view is that governance includes multiple tools and mechanisms. Traditional law and policy are certainly among those mechanisms. However, as we shall see throughout this primer, governance can take place through many other channels. Technology, social norms, decision-making procedures, and institutional design: all of these are as equally important in governance as law or policy.

What is "Internet governance"?

This broader view of governance is particularly important when it comes to discussions of Internet governance. In recent years, the notion of Internet governance has become hotly contested, a subject of political and ideological debate. Many divisions can be identified:

- **Technical or holistic?** Some people feel that Internet governance is a purely technical matter, best left to programmers and engineers; others argue for a more holistic approach that would take account of the social, legal and economic consequences of technical decisions.

- **What is the place of governments?** Another division is between those who would give greater (or even sole) authority to national governments, and those who would either include a wider range of actors (including civil society and private sector) or eliminate government altogether. The traditional role of national governments is also challenged by the global nature of the Internet and the resulting importance of supra-national entities. In recent years, questions regarding participation by governments in these entities have become more frequent, with some arguing that the relevance of governments has diminished, and others suggesting a need for greater government participation.

- **Evolutionary or revolutionary?** A further split can be identified between those who believe existing institutions and laws can be modified to manage the Internet (the "evolutionary" approach), and those who believe that an altogether new system is required (the "revolutionary" approach).

Leaving aside the merits of these various positions, the disagreement itself suggests a certain conceptual confusion. It shows that despite over a decade of debate and discussion, Internet governance remains a work in progress, a concept in search of definition. Still, this primer begins from the premise that certain principles can be established to lay down a working definition of Internet governance.

It was precisely in search of such a working definition that, as part of the United Nations-initiated WSIS, a Working Group was established in 2004 and asked to develop a definition of Internet governance. In its report, issued in June 2005, WGIG proposed the following definition:

[2] http://www.itu.int/osg/spu/forum/intgov04/contributions/itu-workshop-feb-04-internet-governance-background.pdf

> *Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.*[3]

For the purposes of this primer, it is the broad and holistic view indicated by this definition that will be used to discuss Internet governance. Two points in particular stand out and will recur in what follows. First, that Internet governance includes a wider variety of actors than just the government; actors from the private sector and civil society are also important stakeholders. And second, that Internet governance refers to more than just Internet domain name and address management or technical decision-making. Indeed, the report of the WGIG goes on to make it clear that Internet governance "also includes other significant public policy issues, such as critical Internet resources, the security and safety of the Internet, and developmental aspects and issues."[4] These and a variety of other issues will be considered throughout this primer.

What are "layers" and how are they relevant to Internet governance?

One way to conceptualize this more holistic approach is with reference to "layers" of governance. This method was originally proposed by law professor Yochai Benkler, who argued that modern communications networks should be understood as a series of "layers" rather than as an assorted bouquet of different technologies. Benkler lists three such layers: a "physical infrastructure" layer, through which information travels; a "code" or "logical" layer that controls the infrastructure; and a "content" layer, which contains the information that runs through the network.[5]

Today, it has become fairly common to conceptualize the Internet in this fashion. Some would change the names of the layers, and others would include additional layers.[6] The important point, however, is not which specific layers we choose, but the more general point that the Internet can be broken up into discrete analytical categories; and that, consequently, Internet governance itself takes place on multiple levels (or "layers"). In taking a holistic approach to governance, therefore, it is critical that we consider multiple layers.

In this primer, we focus on the three original layers mentioned by Benkler: infrastructure, logical, and content. Each of these layers, displayed in Figure 1, is discussed in greater detail in Section II. That section will also discuss the range of actors involved in governance at each layer (see also Appendix 1).

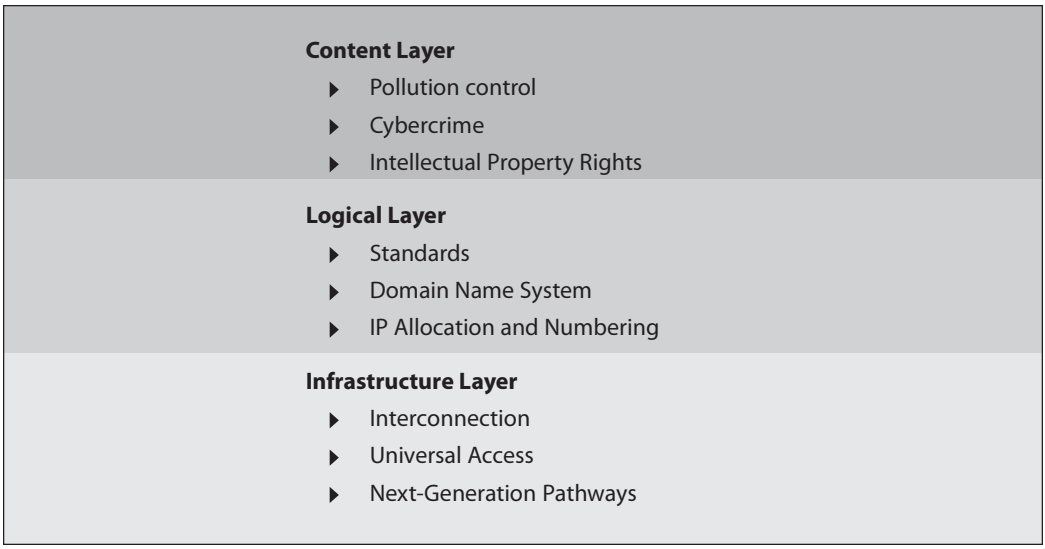


Figure 1 Internet Governance Issues by Layer

[3] WGIG (2005), p. 4. Available at: http://www.wgig.org/docs/WGIGREPORT.pdf
[4] Ibid.
[5] Benkler (2000).
[6] See, for instance, Abbate (1999), or Werbach (1997). Fransman (2002) adopts an interesting critique of the layers model.

What is ICT and what is its relevance to the Internet?

ICT is an acronym that, unpacked, means "Information and Communications Technology". As defined on Wikipedia,

> ICT is the technology required for information processing. In particular the use of electronic computers and computer software to convert, store, protect, process, transmit, and retrieve information from anywhere, anytime.[7]

The use of ICT as a general term is sometimes criticized for a lack of precision, but it is becoming increasingly common given the growing reality of digital convergence. Convergence refers to the phenomenon by which various different forms of digital content (voice, data, rich media like movies and music) can now not only travel along the same physical infrastructure but also be managed and manipulated together by the same systems. It will be covered more fully in Section IV, but what is important to understand here is that, in discussing the Internet, we are in fact discussing several underlying technologies and means of access. This is particularly relevant at the infrastructure layer, where a variety of technologies are deployed. Indeed, the Internet is accessed through a range of infrastructures – traditional telecommunications, cable, satellite, and various wireless methods. Internet governance will therefore have an impact on all these underlying technologies.

Why is the Internet difficult to govern?

The conceptual confusion over the meaning of Internet governance also stems from the fact that there exists no single central authority or mechanism – no traditional form of "governance" – with responsibility for all aspects of the network. This lack of a single authority is, in part, due to historical reasons but also due to the network's technical architecture, which makes it very difficult to exert control. Unlike traditional networks (a telephone network or an early office LAN, for example), the Internet is not reliant upon a central server. Instead, the Internet is a network of autonomous networks, and control rests with the various distributed facilities that, together, make up the collaborative resource referred to as the Internet. For this reason, the Internet is said to be empowered at the edges (i.e., at the individual facilities); it is also sometimes defined as an end-to-end (e2e) network.[8]

The e2e nature of the network is largely a result of its technical design, and particularly of its packet-based data transfer. Using the TCP/IP (Transmission Control Protocol/Internet Protocol) suite, messages on the Internet are broken up into individual packets of data; the network is generally neutral with regard to these packets, and simply routes them using the most efficient path available, without regard to content or origin. This means that intelligence on the Internet rests at the edges: the power to innovate, to create new applications and services or types of content, rests with individual users. The network is also said to be "dumb" with regard to the content that it carries; as long as data packets fit into the basic TCP/IP protocol, the network simply routes them along, without discrimination or control.

The Internet's open standards[9] and e2e model are at the root of its tremendous success and power to drive innovation. However, they are also why the Internet is so hard to manage. On a neutral network, there exists no gatekeeper or central authority to verify the contents of a packet. Viruses, spam, pornography, voice packets (from phone calls), and innocuous email messages: all of these are treated equally. In addition, the fact that multiple pathways exist to route packets from one source to another makes it very difficult for any party to block information; the packets will simply find another route.

This dilemma – the same technical architecture that allows the Internet to flourish also permits a number of harmful activities – is at the heart of many current debates over Internet governance. While the need for some form of control to limit harmful content is widely recognized, there is also widespread agreement that governance mechanisms should facilitate and not compromise the Internet's core technical architecture. In particular, solutions must be found that maintain the principle of e2e and the underlying open standards upon which it is based.

---

[7] http://en.wikipedia.org/wiki/Information_and_Communications_Technology

[8] For more on the end-to-end principle, see http://en.wikipedia.org/wiki/End-to-end_principle

[9] The Internet's standards, particularly TCP/IP and HTML, are generally considered "open" because their specifications are freely available to all. This means that any developer or user can create new applications or services that work with existing applications and services. It is in part this open and enabling environment for innovation that has contributed to the rapid spread of the network.

What is the history of governance on the Internet?

As noted, there exists no central authority on the Internet. Instead, there exists a multitude of actors, institutions and bodies, exerting control or authority in a variety of ways, and at multiple levels. This does not necessarily imply anarchy, as some may suggest; these participants in general have formal and well-defined roles, and they address specific tasks or responsibilities. Section II contains a more detailed discussion of some of these actors and the issues they address. Here, we identify certain key milestones in Internet governance.[10]

Somewhat surprisingly, given the Internet's eventual distance from the state, the network actually began as a government project. In the 1960s, the US Defense Department sponsored the development of the ARPANET by the Defense Advanced Research Projects Agency (DARPA). ARPANET was a distributed network that was designed to foster communication between research centres. Soon, this network, which remained under the control of the US government, was being used by a wider set of users, particularly in the academic community. In the 1970s, DARPA also developed a mobile packet radio network and a packet satellite network. These were conceptually integrated into an Internet in 1973. In 1983, the operational Internet was launched. The National Science Foundation Network (NSFNET) joined the Internet in 1986, spreading access to the Internet to an international community of users.

The Internet Activities Board was formed in 1984 and was made up of a number of task forces. One of these became the Internet Engineering Task Force (IETF) in 1986. It was created to manage the development of technical standards for the Internet. It represented early seeds of "governance" on the Internet, albeit of a unique kind. IETF governed through a consultative, open and co-operative approach. Decisions were made by consensus, and involved a wide variety of individuals and institutions. This freewheeling and decentralized decision-making process remains in many ways the hallmark of Internet governance; it accounts for a significant amount of resistance to any attempt by national governments to exert control over the network.

The Domain Name System (DNS) was developed in the mid-1980s. It was managed by the Internet Assigned Numbers Authority (IANA) at the University of Southern California's (USC's) Information Sciences Institute under US Government contract for many years. The root servers of the DNS were operated voluntarily by 13 different organizations. The root zone file, defining the top level domains of the DNS was distributed by IANA to the root server operators. In 1994, the US Government outsourced the management of the DNS to a private entity, Network Solutions. This led to a considerable degree of dissatisfaction among other members of the Internet community, who feared that the network would become too commercialized. A long process of conflict and deliberation led ultimately to the creation, in 1998, of ICANN, a non-profit corporation charged with managing the Internet's DNS. ICANN inherited the responsibilities of IANA in the course of its creation. Please refer to Appendix 2 for more information regarding the roles and functions of ICANN and IANA.

The creation of ICANN, in many ways, initiated the latest round of debates over Internet governance. Although created with primarily a technical mandate (i.e., managing the DNS, the allocation of Internet address space, and the recordation of parameters unique to the Internet protocol suite), ICANN quickly became embroiled in a host of controversies. Among other things, critics charge the organization with a lack of democracy and transparency, with being too close to the US Government, and with a perceived exclusion of voices from the developing world.[11]

Recently, controversy over the need for and nature of Internet governance has combined with changes in the underlying nature of the network itself to suggest that a new model of governance may be required. These changes include the tremendous growth of the network, and the increasing reliance of our social, economic and even political lives on what WGIG calls a "global facility."[12] Together, all these events have called into question the relatively informal, consensual and trust-based models of governance that currently exist, and have led to exploration of new or modified governance models.

In 2002, the UN General Assembly took an important step towards such a new model when it called for

[10] For more on the history of the Internet, see Berners-Lee (2000). A good collection of resources is also available at http://www.isoc.org/internet/history/. See, in particular, the "Brief History of the Internet" by Vint Cerf (http://www.isoc.org/internet/history/cerf.shtml).

[11] In its defence, ICANN has struggled with the difficulty of balancing the expectations of multiple stakeholders from different sectors and geographies, and more generally with the challenge of, as it were, conceiving a new form of governance for a highly unique and original entity (i.e., the Internet).

[12] WGIG (2005), p. 4.

a global conference, WSIS that would consider alternatives and ways to increase participation by developing countries. The first WSIS meeting was held in 2003, in Geneva, where representatives adopted a Declaration of Principles and a Plan of Action.[13] A follow-up meeting is scheduled for November 2005 in Tunis.

For the moment, the WSIS process remains incomplete, and its final outcome is not yet clear. Nonetheless, certain issues have risen to the top of the agenda, and are likely to feature prominently in future discussions. These include debates over the respective roles and authority of ICANN, the International Telecommunications Union (ITU) and, especially, national governments. Many developing countries, in particular, would like to see the role of States extended, while others remain wary of granting governments too much control. In addition, questions regarding participation by developing countries and the Internet's role in fostering human and social development are also on the agenda. We discuss these issues more fully later, in Section III.

Should there be governance on the Internet?

The Internet's architectural and ideological foundations – open standards, e2e, empowered users, absence of control – have from the start bred a certain libertarian streak that rejects any attempt to exert control, particularly by the government. Since the very success of the network stems from an absence of the control, the argument goes, government intervention would only stifle the network.

The most famous expression of this extreme form of libertarianism remains John Perry Barlow's "Declaration of the Independence of Cyberspace," quoted in the Introduction. At the start of that manifesto, Barlow declares that:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[14]

Today, it is apparent that his vision was somewhat utopian. Nonetheless, many less radical observers continue to believe that the Internet's success depends on keeping governance (by the State, or by any other authority) to a minimum. Some observers have invoked traditions of the commons, or the public forum, to envision a virtual space where ideas are exchanged freely, without rules, without regulation, and without controls.

These ideas are important to acknowledge because the Internet's success does, to a significant extent, depend on its free and open culture. Nonetheless, it is also clear that the absence of rules can be as detrimental to this commons as the existence of bad rules; anarchy is as harmful as stifling regulation. The right question is, therefore, not whether there should be governance but rather what constitutes good governance. The goal for any governance mechanism should be to balance rules and freedom, control and anarchy, process and innovation.

[13] For more information, see http://www.itu.int/wsis/

[14] The Declaration is available at: http://homes.eff.org/~barlow/Declaration-Final.html

II. ISSUES AND ACTORS

What are some of the issues involved in Internet governance?

As we have seen, Internet governance encompasses a range of issues and actors, and takes place at many layers. Throughout the network, there exist problems that need solutions, and, more importantly, potential that can be unleashed by better governance. It is not possible here to capture the full range of issues. This section, rather, seeks to provide a sampling. It describes the issues by layers, and it also discusses key actors for each layer. A more extensive description of actors and their responsibilities can be found in Appendix 1; Figure 1 also contains a representation of issues by layer.

Most importantly, this section attempts to make clear the real importance of Internet governance by drawing links between apparently technical decisions and their social, economic or political ramifications. Indeed, an important principle (and difficulty) of Internet governance is that the line between technical and policy decision-making is often blurred. Understanding the "real world" significance of even the most arcane technical decision is essential to understanding that decision and its processes, and to thinking of new ways to structure Internet governance.

What are some of the governance issues at the infrastructure layer?

The infrastructure layer can be considered the foundational layer of the Internet– it includes the copper and optical fibre cables (or "pipes") and radio waves that carry data around the world and into users' homes. It is upon this layer that the other two layers (logical and content) are built, and governance of the infrastructure layer is therefore critical to maintaining the seamlessness and viability of the entire network. Given the infrastructure layer's importance, it makes sense that a wide range of issues requiring governance can be located at this level. Three, in particular, merit further discussion.

Interconnection

The Internet is a "network of networks"; it is composed of a multitude of smaller networks that must connect together ("interconnect") in order for the global network to function seamlessly. In traditional telecommunications networks, interconnection is clearly regulated at the national level by State authorities, and at the international level (i.e., between national networks) by well-defined principles and agreements, some of which are supervised by the ITU. Interconnection between Internet networks, however, is not clearly governed by any entity, rules or laws. In recent years, this inherent ambiguity has become increasingly problematic, leading to high access costs for remote and developing countries, and in need of some kind of governance solution. Indeed, in its final report, the WGIG identified the ambiguity and uneven distribution of international interconnection costs as one of the key issues requiring a governance solution.[15]

On the Internet, access providers must interconnect with each other across international, national or local boundaries. Although not formalized, it is commonly said that there are three categories of access providers in this context: Tier 1 (large international backbone operators); Tier 2 (national or regional backbone operators); and Tier 3 (local ISPs). In most countries, there is some regulation of interconnection at national and local levels (for Tiers 2 and 3 ISPs), which may dictate rates and other terms between these providers. Internationally, however, there is no regulation, and the terms of any interconnection agreement are generally determined on the basis of negotiation and bargaining. In theory, this allows the market to determine interconnection in an efficient manner. In practice, however, unequal market position, and in particular the important positions occupied by Tier 1 providers, means that the larger providers are often able to dictate terms to the smaller ones, which in turn must bear the majority of the costs of connection.

[15] WGIG (2005), p. 5

This situation is particularly problematic for developing countries, which generally lack ownership of Tier 1 infrastructure and are often in a poor position to negotiate favourable access rates. By some accounts, ISPs in the Asia-Pacific region paid companies in the United States US$ 5 billion in "reverse subsidies" in 2000; in 2002, it was estimated that African ISPs were paying US$ 500 million a year. One commentator, writing on access in Africa, argues that "the existence of these reverse subsidies is the single largest factor contributing to high bandwidth costs".[16]

It should be noted that not everyone would agree with that statement, and that high international access costs are not by any means the only reason for high local access costs. A related – indeed, in a sense, the underlying – problem is the general lack of good local content in many developing countries. It is this shortage of local content, stored on local servers, that leads to high international connectivity costs as users are forced to access sites and information stored outside the country. Moreover, as we shall discuss further later, the lack of adequate competition policies and inadequately developed national markets also play a significant role in raising access costs for end-users. Increasing connectivity within regions has reduced some of the concerns for the costs of connection to major backbones, as has absolute cost of undersea optical cable services.

Actors Involved

This opaque setup – in effect, the absence of interconnection governance at the Tier 1 level – has created a certain amount of dissatisfaction, and some initial moves towards a governance solution. One of the first bodies to raise the issue of interconnection pricing was the Asia-Pacific Economic Cooperation Telecommunications and Information Working Group (APEC Tel), which, in 1998, questioned the existing system (or lack thereof) of International Charging Arrangements for Internet Services (ICAIS). In addition, Australia, whose ISPs pay very high international access charges due to remoteness and relative lack of competition, has also expressed unhappiness with the current arrangement.

Regional groups such as APEC Tel have played an important role in putting today's shortcomings on the agenda. However, the main body actually dealing with the issue is ITU, where a study group has been discussing governance mechanisms that could alleviate the current situation. Three main proposals appear to be on the table, with the chief disagreement being between larger industry players who would prefer a market-driven solution; and smaller industry players and developing countries, who would prefer a system that resembles the settlement currently used in international telecommunications. Under this system, the amount of traffic carried by operators is measured in terms of call-minutes and reconciled using previously agreed-upon rates. In the case of inter-provider Internet connections, however, there is no such thing as a "call minute," since all traffic flows by way of packets which are not identified with specific calls. While packets can be easily counted, it is not necessarily clear which party, the sender or receiver, should be charged for any particular packet, particularly when the source and destination for those packets may not reside on the individual providers who are exchanging traffic.[17]

An added difficulty is that the settlement system relies on negotiated and often protracted bilateral agreements, whereas the Internet seems to require a global, multilateral solution. Identifying the appropriate global forum, however, has proven difficult: the issue does not fall under ICANN's remit, and progress at the ITU has been slow. Some have suggested that interconnection charges should be considered a trade-related matter that could be taken up under WTO. For the moment, the lack of a global forum to deal with this issue represents perhaps the most serious obstacle to its resolution.

As noted earlier, it should also be reemphasized that the lack of an international settlement regime is not the only reason for high access costs. Often, poor (or absent) competition policies within countries also contribute to the problem, leading to inefficient markets and inflated costs for ISPs. Thus, a holistic approach to the problem of interconnection and access costs would address both the international and the local dimensions of the problem. For example, some countries have taken positive steps in this regard by de-licensing or drastically reducing entry barriers for ISPs. We discuss these issues further later in Section IV.

[16] Bell, Richard (2002), "The Halfway Proposition: Background Paper on Reverse Subsidy of G8 Countries by African ISPs," Draft 4, p. 7. Available at: http://www.afrispa.org/HalfwayDocs/HalfwayProposition_Draft4.pdf

[17] These difficulties, it should be added, are only growing, as an increasing number of traffic carriers (including traditional telecommunications operators) are moving towards Voice over Internet Protocol (VoIP), which makes the very concept of "call-minutes" increasingly anachronistic.

Universal Access

Another key area of governance concerns access, and in particular the notion of universal access. This notion is somewhat hard to define; in fact, one of the important tasks for governance would be to clarify between several competing definitions.[18] Outstanding issues include whether universal access should cover:

- access for every citizen on an individual or household basis, or for communities (e.g., villages and small towns) to ensure that all citizens are within reach of an access point;
- access only to basic telephony (i.e., narrow-band), or access also to value-added services like the Internet and broadband; and
- access only to infrastructure, or also to content, services and applications.

In addition, any adequate definition of universal access must also address the following questions:

- **How to define "universal"?** Universal access is frequently taken to mean access across geographic areas, but it could equally refer to access across all gender, income, or age groups. In addition, the term is frequently used almost synonymously with the digital divide, to refer to the need for equitable access between rich and poor countries.
- **Should universal access include support services?** Access to content or infrastructure is not very useful if users are unable to make use of that access due to the fact that they are illiterate or uneducated. For this reason, it is sometimes argued that universal access policies must include a range of socio-economic support services.

Each of these goals, or a combination of them, is generally widely held to be desirable. However, the realization of universal access is complicated by the fact that there usually exist significant economic disincentives to connect traditionally underserved populations. For example, network providers argue that connecting geographically remote customers is financially unremunerative, and that the required investments to do so would make their businesses unsustainable. For this reason, one of the key governance decisions that must be made in any attempt to provide universal access is whether that goal should be left to market forces alone, or whether the State should provide some form of financial support to providers.

When (as is frequently the case) States decide to provide some form of public subsidy, then it is essential to determine the appropriate funding mechanism. Universal service funds, which allocate money to providers that connect underserved areas, are one possible mechanism. A more recent innovation has been the use of least cost-subsidy auctions, in which providers bid for a contract to connect underserved areas; the provider requiring the lowest subsidy is awarded the contract.

In addition to funding, the governance of universal access also encompasses a range of other topics. For instance, definitions of universal access need to be regularly updated to reflect technological developments – recently, some observers have suggested that universal service obligations (traditionally imposed only on fixed-line telecommunications providers), should also be imposed on cellular phone companies, and possibly even on ISPs. Interconnection arrangements, rights-of-way, and licensing policies are other matters that are relevant to universal access. The range of issues suggests the complexity of an adequate governance structure – but it also suggests the importance of such a structure.

Actors Involved

Since traditional universal access regulation involves fixed-line telephony, national and international telecommunications regulators are usually the most actively involved in governance for universal access. At the international level, the ITU-D, the development wing of ITU, plays an important role in developing policies, supporting various small-scale experiments in countries around the world, and in providing training and capacity building to its member states.

Most of the policies concerning universal access, however, are set within individual countries, by national governments and domestic regulatory agencies. In India, for example, the Department of

[18] Given the range of possible definitions, it seems clear that the issue of universal access raises governance issues at various layers. Access to infrastructure is, however, considered key, as it is foundational and essential for access at other layers.

Telecommunications (DOT), in consultation with the Telecommunications Regulatory Authority of India (TRAI), administers a universal service fund that disburses subsidies to operators serving rural areas. The Nepalese government has extended telecommunication access in its eastern region through least cost-subsidy auctions that award licenses to private operators that bid the lowest for a government subsidy. And in Hong Kong, universal service costs are estimated and shared among telecommunications operators based on the amount of international minutes traffic carried by them.

In addition to these traditional telecommunications authorities, international institutions and aid groups have begun taking an increasing interest in the subject of universal access. Both the World Bank (WB) and the United Nations (UN), for example, devote significant resources to the issue, as do several non-governmental organizations (NGOs). For example, WB is providing US$ 53 million to fund the eSri Lanka project that aims to bridge the access gap between the western province and the northern, eastern and southern provinces. The project will subsidize the building of a fibre-optic backbone and rural telecentres. Similarly, the International Development Research Centre (IDRC) has funded several projects that consider optimal approaches for achieving rural connectivity (e.g., through the use of Wireless Fidelity (WiFi), or by setting up village telecentres).

One important venue where governance (and other) issues related to universal access are being discussed is WSIS. At its inception, the representatives of WSIS declared their

> common desire and commitment to build a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes.[19]

WSIS is likely to increase the interest of international aid agencies in the subject of universal access. In the future, as convergence becomes an increasing reality, multilateral bodies like the UN, ITU and others are likely to become more involved in developing appropriate governance mechanisms.

Next-Generation Pathways

Technology evolves at a rapid pace, and this evolution often brings great benefits to the Internet. However, the process of adopting new technologies can also be complicated, and is a further area requiring governance. Two issues, in particular, can benefit from governance.

The first concerns decisions on when to deploy new technologies. Many members of the technical community (and others) would argue that such decisions should simply be left to consumer choice. But governments often feel otherwise. For example, some governments have resisted the use of IP technology for phone calls, fearing the resulting loss of revenue to incumbent telecom operators. Likewise, many governments have yet to de-license the necessary spectrum for Wi-Fi networks, often citing security concerns. States may also choose to prioritize some technologies (e.g., narrowband connectivity) over others (e.g., more expensive broadband) in an effort to pursue social or developmental goals.

Such decisions are often met with scepticism, but the issue is not whether governments are right or wrong in resisting certain next-generation technologies. What matters is to understand that the decision on introducing new pathways is a governance decision: it is the product of active management by the State, and, ideally, by other involved stakeholders. Thus, a comprehensive approach to Internet governance would include mechanisms and steps to introduce next-generation pathways in a smooth and effective manner.

Next-generation technologies also require governance to ensure that they are deployed in a manner that is harmonious with pre-existing (or "legacy") systems. Such coordination is essential at every layer of the network, but it is especially critical at the infrastructure layer. If new means of transmitting information cannot communicate with older systems, then that defeats the very purpose of deploying new systems. For example, much attention has been given in recent years to the promise of broadband wireless technologies like third generation (3G – for the cellular network) and Worldwide Interoperatibility of Microwave Access (WiMax – which is a wireless backbone technology that could potentially extend the reach of wireless Internet connectivity). Such network technologies are useful to the extent that they are compatible with existing communications networks. As with the decision on *when* to introduce new

[19] http://www.itu.int/wsis/docs/geneva/official/dop.html

pathways, then, governance solutions are also required to decide *how* to introduce them, and in particular to ensure that standards and other technical specifications are compatible with existing networks.[20]

Actors Involved

As with other the topics discussed here, the governance of next-generation pathways is a broad-ranging process that involves a range of stakeholders. National governments are of course important, and play a determining role in deciding which technologies are adopted. This role, however, is often supplemented by advice from other groups. For example, ITU and other multilateral organizations play a key role in recommending the deployment of new technologies to national governments. In addition, industry groups sometimes play a role in lobbying for certain technologies over others. To balance their role, it is also important for governments to take into account the views of consumer groups and civil society.

Finally, standards bodies like IETF, the International Standards Organization (ISO) and others have an essential role to play, particularly in ensuring compatibility between new and legacy systems. In the case of standards based on open source, it is also possible for consumer and user groups to have a greater say over which technologies are adopted, and how they can promote social and other values.

What are some of the governance issues at the logical layer?

The logical layer sits on top of the infrastructure layer. Sometimes called the "code" layer, it consists of the software programs and protocols that "drive" the infrastructure, and that provide an interface to the user. At this layer, too, there exist various ways in which governance can address problems, enhance existing processes, and help to ensure that the Internet achieves its full potential.

Standards

Standards are among the most important issues addressed by Internet governance at any layer. As noted, the Internet is only able to function seamlessly over different networks, operating systems, browsers and devices because it sits on a bedrock of commonly agreed-upon technical standards. TCP/IP, discussed earlier, is perhaps the most important of these standards. Two other key standards are the HyperText Mark-up Language (HTML) and the HyperText Transfer Protocol (HTTP), developed by Tim Berners-Lee and his colleagues at CERN in Geneva to standardize the presentation and transport of web pages. Much as TCP/IP is the basis for the growth of the Internet's infrastructure, so HTTP and HTML are the basis for the phenomenal growth of the World Wide Web. Other critical standards include Extensible Mark-up Language (XML), a standard for presenting information on web pages, and IPv6 (Internet Protocol, version 6, the successor to the current IPv4), used in Internet-addressing systems (see discussion below).

The centrality of standards to the Internet means that discussions over the best mechanism to manage and implement them are as old as the network itself. Indeed, long before the current governance debate, standards were already the product of *de facto* governance, primarily by consensus-driven technical bodies. This need for governance occurs because standards rely for their effectiveness on universal acceptance, which, in turn, relies on groups or bodies to decide upon and publish standard specifications. Without such control, the Internet would simply fragment into a Babel of competing technical specifications. Indeed, such a spectre haunts the future of HTML and XML, which over time has become increasingly fragmented due to competing versions and add-ons by private companies.

Another important issue concerns what some perceive as the gradual "privatization" of standards. While many standards on the Internet have traditionally been "open" (in the sense that their specifications have been available to all, often without a fee), there have been some indications of a move towards fee-based standards. For example, in 2001, the World Wide Web Consortium (W3C), a critical Internet standards body, raised the ire of the Internet community when it proposed endorsing patented standards for which users would have to make royalty payments; the proposal was later withdrawn, but it raised significant concerns that such moves could reduce the openness of the network.

Finally, standards also require governance so that they can be updated to accommodate new technologies

[20] Of course, the need for compatibility with existing systems should not overshadow the fact that new (and potentially disruptive) technologies can also play a potentially valuable role through a process that economists sometimes refer to as "creative destruction". Thus while it is essential to ensure network seamlessness, it is also essential to ensure that new technologies are not burdened by undue compatibility requirements; any requirements should be restricted to impose only reasonable compatibility.

or needs of the Internet community. For example, ongoing network security concerns (driven by the rise of viruses, spam, and other forms of unwanted content) have prompted some to call for new specifications for TCP/IP that would include more security mechanisms. Likewise, some feel that the spread of broadband, and the rise of applications relying on voice and rich media like movies, require the introduction of Quality of Service (QOS) standards to prioritize certain packets over others.

Currently, for example, the network does not differentiate between an email or a phone call, which is why Internet telephony remains somewhat unreliable (voice packets can be delayed or dropped along the way). However, the introduction of QOS standards, which could discriminate between packets, could mean a departure from the Internet's cherished e2e architecture. This difficult dilemma – balancing the competing needs of openness with flexibility and manageability – is an example of the importance of adequate governance mechanisms that are able to reconcile competing values and goals.

Actors involved

Currently, Internet standards are determined in various places, including international multi-sectoral bodies, regional bodies, industry fora and consortiums, and professional organizations. This wide range of venues is emblematic not just of the variety of actors involved in Internet governance (broadly defined), but also of the range of issues and interests that must be accommodated. Industry representatives, for example, are often far more concerned with speed and efficiency in decision-making, while civil society representatives would sacrifice a certain amount of speed in the name of greater consultation and deliberation.

Amidst this variety of actors, three in particular are critical to the development of core Internet standards:

- **The Internet Engineering Task Force (IETF):** IETF, a large body with open participation to all individuals and groups, is the primary standards body for the Internet. Through its various working groups, it sets standards for Internet security, packeting, and routing, among other issues. Probably the most important standards that fall under IETF are the TCP and IP protocols.

  In addition to being one of the most important groups, IETF has also been a quintessential Internet decision-making body. Its open participation, consultative decision-making processes, and relative lack of organizational hierarchy have made it a model for an inclusive, yet highly effective, system of governance that is unique to the online world. Until recently, most of IETF's work took place informally, primarily via face to face meetings, mailing lists and other virtual tools. However, as the organization's membership (and the Internet itself) grew in size and complexity, certain administrative changes were introduced to streamline – and, to a certain extent centralize – decision-making. The Internet Activities Board (now the Internet Architecture Board (IAB)) made standards decisions until 1992 when this task became the responsibility of the Internet Engineering Steering Group (IESG). Pleases refer to Appendix 2, 'Internet Standards', for more information on IETF and other standards bodies.

- **International Telecommunication Union-Telecommunication Standardization (ITU-T):** ITU-T is the standard-setting wing of the ITU. It operates through study groups whose recommendations must subsequently be approved by member-states. As one of the oldest standards bodies, and as a member of the UN with an intergovernmental membership body, the ITU-T's standard recommendations traditionally carry considerable weight. However, during the 1990s, with the rise of the Internet, ITU-T (at that time known as the International Telegraph and Telephone Consultative Committee, or CCITT), found its relevance called into question due to the increasing importance of new bodies like IETF. Since that time, ITU-T has substantially revamped itself and is today a key player in the standards-setting community.

  ITU-T and IETF do attempt to work together, but they have a somewhat contentious relationship. While the latter represents the open and free-wheeling culture of the Internet, the former has evolved from the more formal culture of telecommunications. IETF consists primarily of technical experts and practitioners, most of them from the developed world; ITU-T is made up of national governments, and as such can claim membership (and the resulting legitimacy) of many developing country states. Their disparate cultures, yet similar importance, highlights the necessity (and the challenge) of different groups working together to ensure successful governance.

- **World Wide Web Consortium (W3C):** W3C develops standards and protocols that exist on top of core Internet standards. It was created in 1994 as a body that would enhance the World Wide

Web by developing new protocols while at the same time ensuring interoperability. Among others issues, it has developed standards to promote privacy (the P3P platform), and a protocol that would allow users to filter content (PICS). W3C also works on standards to facilitate access for disabled people.

The consortium is headed by Tim Berners-Lee, sometimes referred to as the "inventor of the World Wide Web" for his pioneering work in developing key standards like HTML and HTTP. It is a fee-based organization, with a significant portion of its membership made up by industry representatives.

Management of the Domain Name System

The coordination and management of the DNS is another key area requiring governance at the logical layer. In recent years, the DNS has been the focus of some of the most heated (and most interesting) debates over governance, largely due to the central role played by ICANN.[21]

Understanding the DNS

In order to understand some of the governance issues surrounding the DNS, it is first necessary to understand what the DNS is, and how it functions. Operating as a lookup system, the DNS allows users to use memorable alphanumeric names to identify network services such as the World Wide Web and email servers. It is a system that maps names (e.g., www.undp.org) to a string of four numbers separated by periods called IP addresses (e.g., 165.65.35.38).

Until 2000, the Internet had eight top-level domain names: .arpa, .com, .net, .org, .int, .edu, .gov and .mil. These domains are called generic top-level domains, or gTLDs. As the Internet grew, there were increasing calls for more top-level domain names to be added, and, in 2000, ICANN announced seven new gTLDs: .aero, .biz, .coop, .info, .museum, .name, and .pro. Another series of new gTLDs have also been announced recently, although not all of them are yet operational.

In addition to these gTLDs, the DNS also includes another set of top-level domains known as country code top-level domains, or ccTLDs. These were created to represent individual countries, and include two-letter codes such as .au (Australia), .fr (France), .gh (Ghana), and .in (India).

Actors Involved

ICANN, a non-profit corporation formed to manage the DNS by the US government in 1998, is the main body responsible for governance of the DNS. At its founding, ICANN was upheld as a new model for governance on the Internet – one that would be international, democratic, and include a wide variety of stakeholders from all sectors.

Almost from the start, however, ICANN has proven to be controversial, and its many shortcomings (perceived or real) have led some observers to conclude that a more traditional system of governance, modeled after multilateral organization like ITU or the UN, would be more appropriate for Internet governance. Indeed, although not always explicitly mentioned, one sub-text of the WSIS process is, precisely, such a rethink of governance models. Many developing countries, in particular, would like to see a greater role for national governments, and a distancing of core DNS functions from the US government, under whose aegis ICANN still functions.

ICANN's missteps and mishaps cannot be fully documented here. They include a short-lived attempt to foster online democracy through direct elections to ICANN's board (the effort was troubled from the start and the elections no longer take place). They also include a variety of decisions that have led many to question the organization's legitimacy, accountability and representation. To be fair to ICANN, its many troubles are probably indications not so much of a single organization's shortcomings, but rather of the challenges in developing new models of governance for the Internet.

ICANN's troubles also shed light on the difficulty of distinguishing between technical decision-making and policy decisions which have political, social, and economic ramifications. ICANN's original mandate

[21] The debate and discussion surrounding ICANN cannot be addressed in detail here. For a closer look at ICANN's history and some of the relevant issues, see www.icannwatch.org. Milton Mueller also provides a good overview of ICANN in *Ruling the Root: Internet Governance and the Taming of Cyberspace* (MIT, 2004).

is clear: technical management of the DNS. Esther Dyson, ICANN's first chair, has argued that

> ICANN does not "aspire to address" any Internet governance issues; in effect, it governs the plumbing, not the people. It has a very limited mandate to administer certain (largely technical) aspects of the Internet infrastructure in general and the Domain Name System in particular.[22]

Despite such claims, ICANN's history shows that even the most narrowly defined technical decisions can have important policy ramifications. For example, the decision on which new top-level domain names to create was a highly charged process that appeared to give special status to some industries (e.g., the airline industry). In addition, ICANN's decisions regarding ccTLDs have proven contentious, touching upon issues of national sovereignty and even the digital divide. Indeed, one of the more difficult issues confronting governance of the DNS is the question of how, and by whom, ccTLDs should be managed. Long before the creation of ICANN, management of many ccTLDs was originally granted by IANA to volunteer entities that were not located in, nor related to, the countries in question. As a result, some countries (e.g., South Africa) have taken legal recourse to reclaim their ccTLDs. To be fair, many of these assignments were undertaken at a time when few governments, let alone developing country governments, had any interest or awareness of the Internet. The DNS was created in 1984, long before the creation of ICANN in 1998. ICANN's relationship with country operators has also sometimes proven difficult due to the oversight of the organization by the US government.

This has led to a situation in which many country domain operators have created their own organizations to manage regional TLDs. For example, European domain operators have created their own regional entity, the Council of European National TLD Registries (CENTR). While not quite such a dramatic development yet, regional entities do raise the frightening prospect of Internet balkanization, in which a fragmented DNS is managed by competing entities, and the Internet is no longer a global, seamless network. To remedy this problem, ICANN created a supporting organization of ccTLDs called the country code supporting organization or ccNSO. All ccTLD operators have been invited to join this organization, including all the participants in CENTR. Significant progress has been made in achieving this objective.

IP Allocation and Numbering

As mentioned, IP addresses are composed of sets of four numbers (ranging from 0 to 255) separated by periods – this is just a representation of a 32-bit number that expresses an IP address in IPv4. In fact, every device on the network requires a number, and numbering decisions for IP addresses as well as for other devices are critical to the smooth functioning of the Internet.

Several governance steps have already been taken in the realm of numbering. One of the most important areas of governance concerns recent moves to address a perceived shortage of IP addresses. Under the current protocol, IPv4, there exist some 4.2 billion possible unique IP addresses. The number may appear large, but the proliferation of Internet-enabled devices like cell phones, digital organizers and home appliances – each of which is assigned a unique IP number – could in theory deplete the available addresses, thereby stunting the spread of the network.

In addition, as we shall see below, the shortage of IP space has been a particular concern for developing countries.

To address this potential shortage, two steps have been taken:

- First, the technical community has developed a new protocol known as IPv6. This protocol, which would allow for some 340 undecillion (3.4×1038) addresses, essentially solves the shortage problem. IPv6 also introduces a range of additional features not currently supported in IPv4, including better security, and the ability to differentiate between different streams of packets (e.g., voice and data).

- Second, the technical community also introduced a process known as "Network Address Translation" (NAT), which allowed for the use of private addresses. Under NAT, individual computers on a single private network (for example, within a company or university) use non-unique private addresses that are translated into public, unique IP addresses as they leave the

[22] Cited at http://cyber.law.harvard.edu/is99/governance/introduction.html#_ftn10

private network boundary. Many Internet architects find this to create a serious erosion of the Internet's end-to-end principles.

An additional example of governance in the realm of numbering can be found in recent efforts to develop a shared platform for the Public Switched Telephone Network (PSTN) and the IP network. These efforts have been led by the IETF, which has developed a standard known as ENUM. Essentially, ENUM translates telephone numbers into web addresses, and as such "merges" the DNS with the existing telephone numbering system. Although not widely deployed yet, it offers potential in several areas. For example, it should allow telephone users, with access only to a 12-digit keypad, to access Internet services; it should also make it significantly easier to place telephone calls between the PSTN and the Internet using VoIP.

Actors Involved

The main body involved in the distribution of IP numbers is IANA. IANA allocates blocks of IP address space to the Regional Internet Registries (RIRs)[23] , which allocate IP addresses and numbers to ISPs and large organizations. Currently, the issue of how numbers will be allocated under IPv6 has become a matter of some contention. In particular, it appears possible that national governments, which have not shown much interest in IP allocation thus far, may henceforth play a greater role. Unless this is done with great care, the basic need to constrain the growth of routing tables could be seriously affected.

Although the IANA distributes IP space, it was the IETF, in consultation with industry and technical groups that played the leading role in developing IPv6. As noted, the IETF has also been at the forefront of ENUM development. However, given the bridging role played by ENUM between the Internet and existing telephone systems, organizations more traditionally involved in telecommunications governance have also claimed a role. In particular, as the international authority for telephone codes, the ITU has been involved in the application of ENUM; the IETF design specified a key role for the ITU in validating the topmost levels of delegation for ENUM domain names. In addition, as PSTN numbering still remain largely the domain of national regulators, it seems likely that any widespread deployment of ENUM will by necessity involve governments too.

What are some of the governance issues at the content layer?

For average users, the content layer is their only experience of the Internet. This is where the programs and services and applications they access on an everyday basis exist. This does not mean that governance on the content layer is the only area relevant to average users. As should be clear by now, the three layers are inter-dependent, and what happens at the content layer is very much contingent on what happens at the other layers. For example, without an effective mechanism for ensuring interconnection, it would be impossible – or at any rate fruitless – to use a web-browser at the content level.

Nonetheless, governance at this layer is a matter of critical (if not singular) importance for users. Here, we examine three issues of particular importance:

Internet Pollution

Pollution is the generalized term used to refer to a variety of harmful and illegal forms of content that clog (or pollute) the Internet. Although the best known examples of pollution are probably spam (unsolicited email) and viruses, the term also encompasses spyware, phishing attacks (in which an email or other message solicits and misuses sensitive information, e.g., bank account numbers), and pornography and other harmful content.

From a minor nuisance just a few years ago, Internet pollution has risen to epidemic proportions. By some estimates, 10 out of every 13 emails sent today is spam.[24] Such messages clog often scarce bandwidth, diminish productivity, and impose an economic toll. According to one study, spam results in an annual Euro 10-billion loss just through lost bandwidth.[25] Similarly, in the United States, the Federal Trade Commission (FTC) announced in 2003 that up to 27.3 million Americans have been victims of

[23] On 24 October 2003, the four Regional Internet Registries (RIRs) – APNIC, ARIN, LACNIC and RIPE NCC – entered into a Memorandum of Understanding (MoU) to form the Number Resource Organization (NRO). The purpose of the NRO is to undertake joint activities of the RIRs, including joint technical projects, liaison activities and policy co-ordination. Source: http://www.nro.net/about/index.html

[24] Gelbstein, E. and Kurbalija, J., "Internet Governance: Issues, Actors and Divides," *Diplo,* p. 62. Available at: http://www.diplomacy.edu/isl/ig/

[25] *Ibid, p. 62*

some form of identity theft within the past five years, and that in 2002 alone, the cost to businesses of such theft amounted to nearly US$ 48 billion.[26] It should be made clear that the losses are a consequence of the creation of new credit card accounts by the identity thieves, not necessarily the stealing of money from the individual victims of identity theft.

In addition to the economic damage, pollution also damages the Internet by reducing the amount of trust average users have in the network.[27] Trust is critical to the Internet's continued growth. If users begin fearing the openness that has thus far made the network such a success, this would slow the spread of the network, damage the prospects for e-commerce, and possibly result in a number of "walled gardens" where users hide from the wider Internet community.

Actors Involved

One of the reasons for the rapid growth of pollution is the great difficulty in combating it. Spam and viruses exploit the Internet's e2e architecture and anonymity. With few exceptions, unsolicited mailers and those who spread viruses are extremely difficult to track down using conventional methods. In this sense, pollution represents a classic Internet challenge to traditional governance mechanisms: combating it requires new structures and tools, and new forms of collaboration between sectors.

A variety of actors and bodies are involved in trying to combat spam. They employ a diverse range of approaches, which can be broadly divided into two categories:

- **Technical approaches:** Technical solutions to spam include the widely deployed junk mail filters we find in our email accounts, as well as a host of other detection and prevention mechanisms. Yahoo and Microsoft, for example, have discussed implementing an e-stamp solution that would charge tiny amounts for legitimate emails to be accepted in an inbox. Although such proposals are likely to encounter opposition, they address the underlying economic reality that spam is so prolific in part because it is so cheap (indeed, free) to send unwanted emails.

  A number of industry and civil society groups also exist to develop technical solutions to pollution, and to spam in particular. For example, the Messaging Anti Abuse Working Group (MAAWG) is a coalition of leading ISPs, including Yahoo, Microsoft, Earthlink, America Online, and France Telecom. MAAWG has advocated a set of technical guidelines and best practices to stem the tide of spam. It has also evaluated methods to authenticate email senders using IP addresses and digital content signatures. Similarly, the Spamhaus Project is an international non-profit organization that works with law enforcement agencies to track down the Internet's Spam Gangs, and lobbies governments for effective anti-spam legislation.

- **Legal and regulatory approaches:** These joint industry efforts have led to some successes in combating spam. However, technical efforts to thwart spam must always confront the problem of false positives – i.e., the danger that valid emails will wrongly be classified as spam by the program or other technical tool.

  For this and other reasons, technical solutions have increasingly been supplemented by legal approaches, at both the national and international levels. In the United States, FTC has deemed spreading spyware a violation of federal law, and the CAN-SPAM Act of 2003 makes it a criminal offence to send misleading commercial email. Similarly, in 2002, South Korea addressed the problem of spam originating from its territory by implementing a new antispam law; results have been positive, with the percentage of South Korean commercial emails represented by spam dropping from 90 percent to 70 percent in a three-month period.[28]

  Given the global reach of the Internet, such national approaches clearly need to be supplemented by cross-border co-operation. As Viviane Reding, the EU Information Society Commissioner recently put it: "[The EU] cannot act alone in the fight against spam, as it is essentially borderless."

[26] "National and State Trends in Fraud & Identity Theft January-December 2003," Federal Trade Commission, 22 January 2004. Available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf

[27] According to a 2005 survey of 5,000 American Internet users by Gartner, a consultancy, 42 percent of online shoppers and 28 percent of online bankers have been reducing their activities due to phishing and other online attacks. In addition, the survey also found that 33 percent of online shoppers who said they were concerned by Internet fraud are spending less money as a result; and 77 percent of online bankers are using their bank services less as a result of their concerns. All figures are cited in Richmond (2005, B3).

[28] Williams, M. (2003), "Spam falls after South Korea strengthens e-mail law," *PC World Malta*, 16 September. Available at: http://www.pcworldmalta.com/news/2003/Sep/161.htm

In that context, two worldwide initiatives deserve mention: the Seoul-Melbourne Pact signed by Australia, Korea and several other Asia-Pacific Internet economies; and the London Action Plan, an initiative of the US FTC and the British Department of Trade and Industry, a global think-tank on spam which brings together regulators, civil society and industry stakeholders around the world.

At the multilateral level, the OECD Anti Spam Task Force is currently developing a comprehensive "toolkit" designed to combat spam, while ITU has also been active, organizing thematic meetings on spam and cyber-security and considering the possibility of establishing a global Memorandum of Understanding (MoU) on the issue (perhaps within the context of WSIS).

Ultimately, despite all the efforts to solve it, pollution remains a serious and growing menace. This does not mean that no effective governance solution exists. On the contrary, the issue is rare in uniting a disparate group of stakeholders. Businesses, individuals, governments, and civil society: all are harmed by the proliferation of pollution. Far from being an example of the failure of governance, then, pollution could yet emerge as a model for a truly multi-sectoral collaboration that effectively deploys the range of legal and technical tools available.

Cybercrime

Cybercrime is intimately linked to the issue of online pollution. Indeed, many forms of pollution (e.g., phishing, pharming or unsolicited emails) can be considered examples of criminal activity. Cybercrime also encompasses a number of other actions, notably financial fraud, online pornography, hacking, and security attacks such as the injection of viruses, worms and Trojan Horses, the conduct of denial of service attacks, and a variety of other damaging practices. In addition, terrorism that is facilitated by the Internet has emerged as a major concern in recent years.

Cybercrime involves a range of issues, some of which are also evident in the offline world, and some of which are unique to the online environment. One issue that pertains to both environments concerns the need to balance checks on criminal activity with respect for human rights and civil liberties. Some observers have raised concerns that steps ostensibly taken by governments to limit crime may also facilitate censorship, surveillance and other forms of state repression. Numerous such instances were documented in a 2004 report, *Internet Under Surveillance,* by the civil society group Reporters without Borders.[29]

There are also issues that are unique to (or at any rate more pronounced in) the online world. The difficulty of securing evidence is one such issue: governments have struggled to frame laws that impose reasonable data retention requirements on ISPs and others without imposing undue burdens. In addition, the question of service providers' liability has often proven difficult. While some countries hold providers responsible for criminal transactions conducted on their networks, many providers argue that they cannot possibly monitor all activity and should therefore not be held liable. This issue rose to the fore in late 2004, when the head of eBay India, Avnish Bajaj, was arrested over a pornographic video that had been sold on the company's auction site (this despite the fact that the posting of the video violated the user terms of service provided by the company). Bajaj was subsequently released on bail, but the case led to a significant amount of discussion and debate around the world regarding the criminal liability of service providers.

Finally, the Internet poses new and unique challenges to international legal harmonization: on a global network, national jurisdictions sometimes come into conflict. When a company or provider located in one country offers customers in another country a service, it is not always clear which country's laws should apply. We shall discuss this issue further later, in the section on globalization.

Actors Involved

As might be expected, national governments play a key role in controlling cybercrime. Many countries have now adopted fairly comprehensive legislation for a wide range of crimes. Often, though, laws adopted on a national basis only have limited effect, given the global nature of the network. For that reason, cybercrime is increasingly being addressed through multilateral treaties and agreements that involve several countries. Among the best known of such mechanisms is the Council of Europe (CoE) Convention on Cybercrime, which came into effect in July 2004. The convention, signed by 44 countries,

[29] The report is available at: http://www.rsf.org/rubrique.php3?id_rubrique=433

including all EU nations, is considered the leading international instrument against cybercrime today. The G-8 nations, too, have issued a 10-point action plan for dealing with cybercrime.

Other non-State actors also have a role to play. Industry groups and private companies, for instance, can act by adopting codes of conduct and other self-regulatory mechanisms. Such mechanisms have become increasingly common as a way for ISPs to govern themselves and avoid what they perceive as heavy-handed state regulation. Sometimes, such efforts are also supplemented by the participation of civil society and consumer groups; this is seen as an effective way of ensuring that industry governs itself in a manner that is truly in the public interest.[30]

Intellectual Property Rights

Although it is hardly a new issue, Intellectual Property Rights (IPR) has risen to the top of the Internet governance agenda recently. This is, in large part, because the Internet has made it far easier to impinge on copyright (and, to a lesser extent, other IPR) protections. From the simplest cut-and-paste operation to the more complex process of burning a CD, the ease of duplicating and disseminating information has led some to protest that the Internet is undercutting the incentive to innovate in our society. Others argue that, on the contrary, new laws designed to tighten IPR protections on the Internet are, in fact, undermining the principle of "fair use", which traditionally upholds the rights of consumers to use copyrighted works for non-commercial purposes (e.g., lending a CD to a friend).

IPR is a vast topic – too vast to cover comprehensively in a primer such as this one.[31] A brief overview would identify three distinct (if inter-linked) areas where governance solutions for IPR are required:

Copyright and peer-to-peer networks: Copyright violations, particularly within the music industry, have emerged as perhaps the most important IPR issue on the Internet. The rise of peer-to-peer (P2P) networks like Napster and Kazaa, which connect individual users and allow them to share digital files on a massive scale, has threatened existing business models in the music (and, to a lesser extent, movie and video game) industries. In 2003, worldwide sales of music fell by 7.6 percent in value, a fall that industry representatives attributed primarily (and somewhat questionably) to music downloads and file-sharing.[32]

In response, the music industry, represented by the International Federation of the Phonographic Industry (IFPI) worldwide and the Recording Industry Association of America (RIAA), has begun to file lawsuits against file-sharing networks, and even against individual users of those networks. Between September 2003 and July 2005, the IFPI filed more than 14,000 lawsuits against file-sharers in 12 countries; in the US, the recording industry has sued thousands of users, and settled 600 cases for around US$ 3000 each.[33] Many of the US cases have been filed under the US Digital Millennium Copyright Act (DMCA), which in 1998 strengthened copyright laws and extended their application to the Internet. In Asia, too, governments have enacted a number of statutes and provisions to strengthen IPR provisions. For example, under a recently revised copyright law in Singapore, local ISPs are required to remove websites if copyright owners report a violation on the site.

Such aggressive tactics appear to have had some success, and the downward trend in record sales has slowed somewhat. The apparent change in fortunes has been aided by the record industry's recognition that it needed to change its business model to adapt to the new realities of the Internet. As a result, legal and paid download services have become increasingly popular among consumers. Apple's online music store, iTunes, is perhaps the best known, but a number of other services also exist. The IFPI estimates that legal downloads in the first half of 2005 tripled over the same period in 2004; meanwhile, it also estimates that the number of illegal files available on file-sharing networks rose only 3 percent in the first half of 2005.[34]

Software and Open Source: IPR difficulties within the creative industries have received the most attention, but the related issues of software copyrights and piracy are equally important. They are particularly essential to address in the developing world, where the high prices of software are held

[30] One example of multi-stakeholder self-governance can be found in Malaysia, where the Communications and Multimedia Content Forum, including industry and consumer groups, addresses a range of content issues through a "Content Code". More details can be found at http://www.cmcf.org.my/

[31] WIPO has a good introduction to IPR issues at http://www.wipo.int/about-ip/en/ipworldwide/index.html.

[32] See this discussion by the International Federation of the Phonographic Industry (IFPI), which represents the industry worldwide: http://www.ifpi.org/site-content/statistics/worldsales.html

[33] http://www.cbc.ca/story/arts/national/2005/07/21/Arts/Downloads_050721.html

[34] http://news.zdnet.com/2100-9588_22-5798286.html

responsible by some for perpetuating the digital divide.

This issue in fact pre-dates the rise of P2P networks and file-sharing, but has become more pressing recently for two reasons. First, costly *de facto* operating systems and software packages make it increasingly difficult for companies and other entities to survive in the online world. Second, as a growing number of countries seek to join WTO, and as their obligations under the Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement become effective, pressure has been growing on developing nations in particular to enforce IPR protections more stringently.

Unlike with medicines (which also fall under TRIPS), software companies have shown little inclination to lower the prices of their products. As a consequence, developing countries (and others) have increasingly turned to Free and Open Source Software (FOSS), which is available without license to programmers and users around the world. Linux, in particular, has emerged as a popular alternative operating system, and in some countries local governments have begun mandating (or at least encouraging) their departments to use FOSS. For developing countries in particular, using FOSS can help ensure that their vital technology functions do not grow dependent on expensive foreign software companies.

Domain Names and the Uniform Dispute Resolution Policy (UDRP): IPR protections for software, music and movies existed long before the Internet. But protection for domain names, which have emerged as a vital form of intellectual property in the online world, is a new area of IPR law and policy that has emerged specifically due to the Internet.

During the early and mid-1990s, when the commercial potential of the World Wide Web became apparent, the online world witnessed the birth of a trend known as cybersquatting – a practice by which URLs containing company names or other forms of intellectual property were registered by users and, often, resold to the companies in question for exorbitant sums. Resolving disputes over domain names was difficult, partly due to the lack of legal precedent, and partly due to the international nature of the Internet (i.e., as we shall see later, determining the appropriate national jurisdiction is often difficult).

It was in response to such disputes that ICANN, with the help of WIPO developed its UDRP,[35] a series of guidelines that aimed to circumvent the often cumbersome, expensive and ineffective legal options available. UDRP contains instructions for domain name registrars on when and how to cancel or transfer ownership of domain names in dispute. Some critics have accused UDRP of favouring large corporations and commercial interests. On the whole, though, it has proven a relatively successful alternative to traditional, and predominantly legal, IPR protections.

Actors Involved

As the preceding discussion makes clear, a range of actors and institutions are involved in the IPR governance agenda. The groups involved include national governments, trade associations (like the Recording Industry Association of America – RIAA), multilateral institutions like WIPO and WTO, and international non-governmental organizations like ICANN. In addition, civil society groups like the Electronic Frontier Foundation (EFF) and the Creative Commons movement, both of which seek to increase the amount of non-copyrighted information available in the public domain, are also playing a growing role.

The involvement of these various actors points to the international, and multi-sectoral, nature of IPR governance on the Internet. Increasingly, it is clear that IPR governance cannot be successfully led solely by national governments and legal tools. A range of alternative bodies and mechanisms (e.g., the UDRP process mentioned earlier) will also be essential.

One trend worth highlighting in this context is the increasing reliance on technology in protecting IPRs. Digital rights management (DRM) software, in particular, has become common in recent years, and is used by many companies to control how songs, movies or other content can be accessed and disseminated. Such software has also received legal recognition, for example in the WIPO Copyright Treaty, and in the DMCA Act, which made it a criminal offence to try to break DRM protections. Singapore's recent intellectual property law also treats attempts to circumvent technical protections as a criminal offence. DRM tools are effective, but they are also somewhat controversial: critics argue that they undermine fair-use rights, and give record and other companies too much control in determining how consumers can use material they purchase. For example, DRM software can determine how many times

[35] The UDRP policy is available at http://www.icann.org/udrp/udrp.htm

a song can be played, or on how many different devices it can be stored.

These are complicated issues: existing legal and other protections are still in the process of adapting to the very new environment represented by the Internet. It remains to be seen whether the emergent processes of IPR governance can uphold the critical balance between an inventor's incentive to innovate, and citizens' right of ownership.

III. INTERNET GOVERNANCE AND DEVELOPMENT

What is the digital divide and why does it matter?

The digital divide is the term used to refer to the gap between those who have access to the Internet and its associated technologies and services, and those who do not. Although not specifically about the gap between rich and poor countries – a digital divide can exist within a country between urban and rural areas, for example, or between socio-economic groups – the term is frequently used to refer to the access gap between developed and developing countries.

As Table 1 indicates, the gap is striking, and Internet penetration rates are closely connected to the wealth of a country. Such numbers matter for at least two reasons. First, because in today's global economy, lack of access to the Internet means lack of access to world markets. The digital divide between rich and poor countries prevents the latter from selling their products on a global scale, and restricts the choice of services and goods available.

In addition, the digital divide is important because the lack of computers and Internet sites in poor countries means that these countries have only a limited presence on one the most important (and certainly most dispersed) forms of media ever invented. Thus the digital divide is limiting cultural and regional diversity on the Internet.

Table 1: GNI and Internet Penetration

Country	GNI per capita (US$)	Internet Penetration (%)
Developing Countries		
Fiji	2,690	6.5
Thailand	2,540	12.8
China	1,290	7.9
Philippines	1,170	9.3
Indonesia	1,140	7.0
Viet Nam	550	6.4
India	620	3.6
Pakistan	600	0.9
Sri Lanka	1,010	1.3
Cameroon	560	0.4
Zambia	330	0.6
Developed Countries		
Sweden	35,770	73.6
United States	41,400	68.5
Japan	37,180	60.9
United Kingdom	33,940	59.8
Hong Kong SAR	26,810	70.7
Germany	30,120	57.0
Australia	26,900	67.2
Singapore	24,220	60.2
New Zealand	20,310	56.8
France	30,090	42.3

Source: Internet World Stats (http://internetworldstats.com, Sept 2005).

What is the relationship between Internet governance and the digital divide?

Decisions made in the realm of Internet governance can play a significant role in alleviating or exacerbating the digital divide.[36] Although many of these decisions may appear purely technical, they have important social, political and economic consequences. The areas of governance that impact the digital divide include (but are by no means limited to) the following:

Internationalized Domain Names

Currently, all domain names must be entered in standard ASCII (American Standard Code for Information Interchange) characters, which are designed to support the Latin alphabet. This means that diacritical marks, as well as Asian or other international characters, are not supported. Many developing countries feel that the exclusion of their languages from domain names limits Internet access. Users who are not familiar with English have a difficult time accessing English-language URLs; in addition, the lack of foreign-script support makes it difficult for indigenous businesses and entities to be represented on the Internet.

Implementing IDNs is not a simple task. The IETF has developed standards for non-Latin scripts, but complex technical and governance issues have prevented their adoption. ICANN has also been criticized (perhaps not always fairly) for acting slowly on the issue. Adopting IDNs will require greater coordination between national governments and the technical community. It will also require coordination between nations that share a common script (e.g., China, Korea and Japan) so that appropriate standards can be developed. Private entities will also have to be brought on board. Most existing versions of Microsoft Windows, for instance, do not support existing IDN technical standards without substantial updates (though future versions are said to include support), making it difficult to implement IDNs even if standards were agreed upon. The matter is made even more complex by the fact that domain names are used in contexts that employ ASCII encodings—e.g., in URLs, SMTP for email and so on. Thus, the ease of entering a domain name in a natural language script is made more difficult when it is embedded in a URL. In addition, the " . " is not usually a punctuation character in all scripts.

Country Code Top-Level Domain Names

The use of country-level domain names (e.g., .in, .jp, .sg) is another issue that can determine access in developing countries. In many cases, governments have mismanaged these valuable resources. For example, a recent study suggests that management of Cambodia's ccTLD became less efficient and more expensive when the government assumed control from an NGO. Bangladesh is another country where concerns have been expressed. Poor management of ccTLDs can limit a country's visibility on the Internet. In India, relatively few companies had registered ".in" domain names until recently due to requirements that sites be hosted only on servers within the country; under the new system, registrations in the .in ccTLD are growing rapidly.

Poor management can also represent missed revenue opportunities. Operators in some small developing countries have successfully marketed their ccTLDs as alternatives to ICANN's top-level domain names (Table 2).[37] However, when such domain names are not owned by States and marketed by private companies, the misuse can be considered a violation of a country's collective intellectual property resources.

Table 2: ccTLDs as Alternative Top-level Domain Names

Country Code	Country	Domain Area
TV	Tuvalu	TV stations
MD	Moldova	Medicine and health
FM	Federation of Micronesia	Radio
TM	Turkmenistan	Trademark

Source: Gelbstein and Kurbalija (2005, 44)

[36] Of course, the digital divide is a complex phenomenon that is affected by a variety of forces, including governance at the national level, economic and social development, and geographic or cultural factors. Internet governance can play a role in alleviating the divide, but it is important to acknowledge that, to do so, it must work in tandem with these various other forces.

[37] When commercial entities effectively run ccTLDs as gTLDS, this can introduce a range of complicated governance issues.

Standards

Decisions on technical standards also play an important role in shaping the digital divide. Standards that are proprietary (i.e., whose intellectual property is owned by private entities) can make the costs of access to technology prohibitive by requiring expensive royalty payments. In this context, it is important to remember that the global reach of the Internet depends on the use of open standards, notably TCP/IP, XML and other standards for email, voice over the network, streaming audio and video, collaboration and peer-to-peer exchanges. Such standards have not only made the global network connect seamlessly, they have also made it possible to connect affordably. Problems arise, however, when private standards are used, as developing countries then have to pay for the right to use companies' intellectual property rights.

In addition to affordability, open standards are also important because they allow developing countries to modify and enhance technology for their particular needs. Open source software, for example, can enable adaptation of operating systems and software packages to local languages or conditions. Indeed, the future of access in the developing world may depend to a significant extent on such open, modifiable code. A number of low-cost access devices (e.g., the Simputer, a handheld developed in India, or Nivo, a thin-client developed for African users), rely for their affordability and usability on open source software. More promisingly, Linux and other open source software, which can be modified freely, are being used with growing frequency by governments, companies and individual users in the developing world as alternatives to more expensive proprietary software. A key governance strategy to bridge the digital divide could therefore include steps to encourage FOSS – for instance, by providing training or other forms of support to organizations that use open source software, or by requiring government agencies to adopt operating systems like Linux.

Recently, it has become evident that developing countries (and others) can suffer not just through the overt adoption of proprietary standards, but also through a more subtle process by which private entities "hijack" open standards and, through modifications, turn them into *de facto* proprietary standards. This problem has been apparent, for example, in the regular addition of so-called enhancements by companies to HTML and XML. The result is that many features on certain web pages are only fully accessible, for example, on Microsoft's Internet Explorer.[38] A similar situation has been evident, too, with JavaScript, the programming language that powers many websites. Through a steady stream of additions and modifications by various private companies, this ostensibly open standard has been balkanized into several competing versions.

IP Address Allocation

As noted in Section II, the shortage of IP numbers has been a matter requiring governance solutions. Developing countries, in particular, have been concerned as over 80 percent of existing IP numbers have been allocated to organizations in North America. This anomalous situation largely exists due to the historical development of the Internet, and the fact that early IP allocations were made on a first-come-first-served basis. Since the mid-1990s, however, IP numbers have been managed by RIRs, and have been allocated on the basis of demonstrable need. Figure 2 includes the list of RIRs and the percentage of IP numbers allocated by them since 1999. It shows that the historical anomaly has somewhat righted itself, although concerns for inequalities persist in IP allocation.

The shortage of IP space is likely to be substantially eased with the introduction of a new IP known as IPv6. Concerns, however, persist about methods of allocation that will be adopted for this new protocol: it is imperative for developing countries – especially those currently lacking the technical know-how – to ensure that they receive their equitable share.[39]

Costs of Connection

As Figure 3 suggests, the cost of Internet access is often substantially higher in developing countries than in developed countries. As explained earlier, there are many reasons for this disparity. The ambiguities and disparities in international traffic charges, discussed in Section II, are one reason. Equally important reasons include a lack of infrastructure, inadequate competition policies, under-developed markets, and

[38] For a discussion with examples, see http://news.bbc.co.uk/1/hi/technology/4115806.stm

[39] It should also be noted that equitable is not necessarily equal, and that actual use needs to be taken into account. Poorly crafted assignment policies can lead to explosion of routing tables that could interfere with the operation of the Internet.

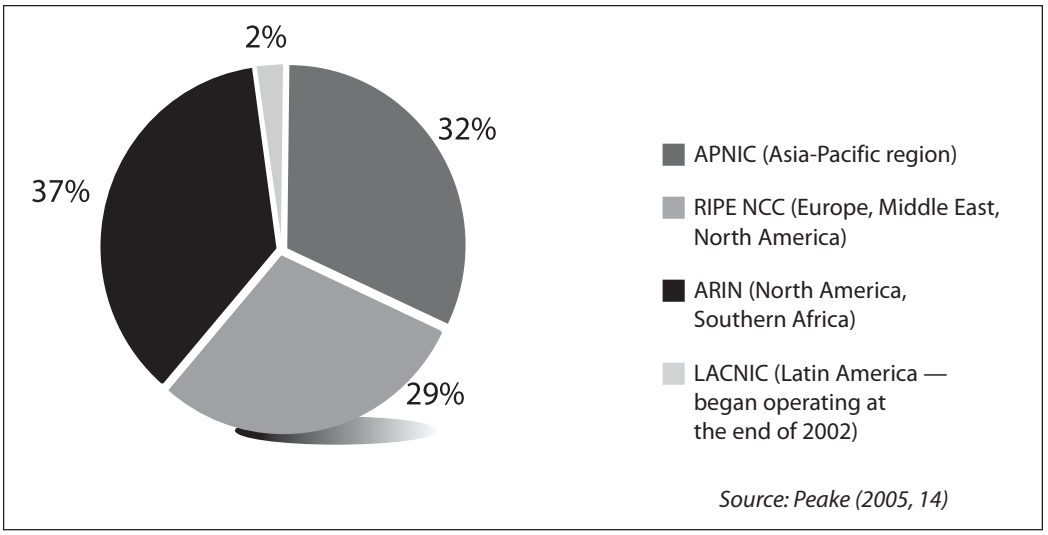


Figure 2 IP addresses allocated since 1999 (percentage by RIR)

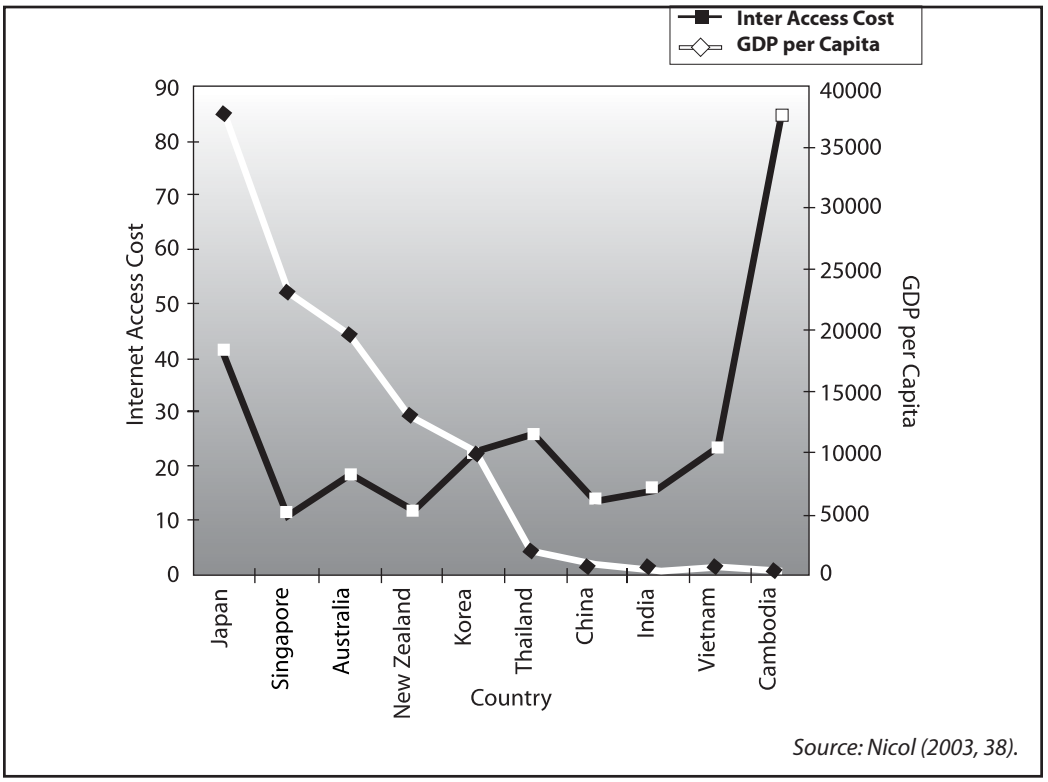


Figure 3 Internet costs and GDP/capita (monthly basis)

predatory pricing by quasi (or actual) monopolies in the ISP market. Addressing all these issues requires a multi-pronged approach that operates at the national, regional, and international levels.

At the national level, the priority should be to foster the development of competitive and open markets for ISPs. One important component of such a strategy is to lower licensing fees and norms; this ensures that new players can enter the market without undue burden, and fosters healthy competition. In addition, ISPs in developing countries often rely on a dominant (sometimes State-owned) telco for access to international bandwidth; this monopoly access to international bandwidth can artificially inflate access prices. Finally, national policies and regulations on interconnection can play a key role. While interconnection terms and prices between network providers are generally best left to the market, in some cases (e.g., when there exists a dominant ISP or telco that can determine interconnection fees)

states may need to impose regulation to ensure a more equitable relationship that permits smaller ISPs to connect at fair prices with larger players. The resulting lower costs, of course, should then be passed on to consumers.

In addition to these national policies aimed at fostering competition, the ambiguities and inequities in the international settlement regime, highlighted by WGIG, are also essential to address. As mentioned, one of the main stumbling blocks is the lack of an appropriate global forum where a fair and equitable system for international rates can be negotiated; identifying such a forum is therefore a critical need.

In the absence of such a forum, many developing countries have taken matters into their own hands by setting up regional Internet Exchange Points (IXPs). Such IXPs keep regional traffic regional – i.e., by routing traffic locally, they reduce the amount of international bandwidth that must be used, and as such also reduce payments to international operators. (Without IXPs, even an email sent from one city to another within a given country could be routed via the United States). Over 150 such IXPs now exist around the world, and the Asia-Pacific region was one of the first parts of the developing world to begin routing a substantial portion of traffic through a regional IXP.

Finally, reducing international access charges will depend on reducing users' dependence on international content. Ultimately, it is the lack of local content, stored on local servers, that increases the consumption of international bandwidth. It is thus critical for governments (and other entities) to make it easier to host content locally, as well as to encourage the development of local content. In many developing countries with non-Latin alphabets, this in turn also requires support for local language fonts and local-language software.

What is the current status of developing country participation in Internet governance?

The preceding list of issues makes it clear that Internet governance impacts developing countries in a variety of ways. Calls for greater participation by the developing world have therefore become an increasingly common feature of debates and discussions over Internet governance. These calls have been accompanied by a growing recognition that, for the most part, developing countries are not adequately represented in most governance fora and, when they are represented, often do not have adequate technical capacity or resources to participate on equal terms.

Perhaps because of its centrality to the governance process, ICANN has come in for particular criticism over its perceived exclusion of developing countries. However, to a greater or lesser degree, such concerns have been expressed with regard to a variety of bodies related to Internet governance. In 2002, the Commonwealth Telecommunications Organization (CTO) and Panos, a non-profit organization, issued a landmark study, *Louder Voices,*[40] in which they listed a number of steps that could be taken to enhance developing country participation in technical governance (see below). With regard to current levels of participation, the study reached three general conclusions:

- First, the study found that developing countries are for the most part represented in *intergovernmental organizations* like ITU and WTO, but that such organizations frequently pay scant attention to the connection between communications policy and development. The study therefore identified a "missing link" between technology policy and development in many important decision-making bodies.

- Second, the study found that developing countries were generally under-represented in *non-traditional decision-making venues*, such as the standards-setting bodies, ICANN and other technical groups. Given the centrality of such groups to the management of the Internet, this represents a serious handicap on developing country participation in Internet governance. Combined with the previous observation, it also explains why many developing countries have been pushing for inter-governmental bodies to play a greater role in Internet governance.

- Third, the study found that, when it comes to *governance decisions led by the market*, developing countries have virtually no representation at all. This is an important shortcoming for many Internet governance decisions are determined by market-driven processes that result in *de facto*

[40] Maclean, Don *et al*. (2003), "Louder Voices: Strengthening Developing Country Participation in International ICT Decision-Making," Commonwealth Telecommunications Organization & Panos, London.

standards. Developing country exclusion from such processes is, of course, simply a reflection of their more general exclusion from global markets.

How can barriers to developing country participation be overcome?

The CTO/Panos study clearly illustrated shortcomings in current systems of Internet governance. That study, as well as a report submitted to the Digital Opportunity Task Force (DOT-Force), a group set up by the G8 at its Genoa Summit in 2001,[41] identified several key steps that could be taken to increase developing country participation. Five of the most important include:

- **Increase policy awareness:** One of the chief obstacles to effective developing country representation is a lack of awareness about policy, policy venues, and even the basic need or relevance of a governance process. Indeed, the CTO/Panos study found a striking lack of awareness when it came to the social and economic impact ICTs can have on development.

  Several steps can be taken to increase awareness. One important way is by developing global ICT policy information resources which would provide, among other things, information on the relevance of ICT activities, as well as dates and information on policy venues. Possible vehicles for this information include a web or email-based newsletter, an annual summary of important issues, a research team to field questions from members, and conferences on particularly significant issues. An e-library, containing relevant information on policy, could also be considered.

- **Build technical and policy capacity:** Developing countries' inadequate technical and policy capacity is a further fundamental barrier to their participation. The CTO/Panos study concluded that the lack of technical capacity is particularly problematic with regard to emerging issues such as migration to IP-based networks, implementation of third-generation mobile communication systems, and e-commerce applications.

  Overcoming such barriers is difficult, given the years of education and experience required. However, capacity building measures do exist. One important mechanism suggested by the study is the establishment of a global network of public and policy research institutes, with offices or "nodes" in developing countries, to work on ICT related issues. These nodes would function as training institutes, and help build policy capacity. In order to ensure the effectiveness of this network, of course, financial support would be required.

- **Provide financial support:** In order to increase developing country representation, a wide variety of financial support mechanisms are required. Funding for the above-mentioned capacity-building network is one possible mechanism. Providing travel fellowships and other means for developing country representatives to attend policy venues (often held in expensive first-world locations) is another.

  However, financial support does not simply involve throwing more money at the problem. According to the CTO/Panos study, financial hurdles often tend to involve ineffective use of resources rather than resource deficiency. Resources are often poorly allocated, for example, with inappropriate people being sponsored to represent stakeholder interests. To address such issues, developing countries need to evaluate current practices and redesign them so as to ensure greater efficiency. It might be helpful, for instance, to develop a code of practice or other accountability mechanisms to ensure efficient use of resources.

- **Strengthen national policy institutions and processes:** Although establishing a global network is important, it is also essential to strengthen capacity at home. National and regional institutions in developing countries are frequently weak on several levels. At the national level, political leadership is often lacking, national ICT strategies are often absent, and coordination between government departments and agencies is often inadequate. At the regional level, coordination between governments and user groups sharing common interests is often lacking. Further weaknesses at this level include poor preparation for international meetings and ineffective use of human and financial resources.

[41] DOT Force (2002), available at Digital Opportunity Task Force (2002), Global policy-making for information and communications technologies: enabling meaningful participation by developing-nation stakeholders. Available at: http://www.markle.org/downloadable_assets/roadmap_report.pdf

One remedial step is to improve information flows and policy coordination between government departments and agencies. Another is to promote sharing of experience and expertise at all levels, including sub-regional and regional. Indeed, such collaboration is perhaps one of the most important steps developing countries can take, as it permits a "sharing of bargaining power" that increases their clout. Importantly, in order for such collectives to be truly effective, they should not be limited to just one sector (e.g., inter-governmental alliances), but be true multi-stakeholder alliances.

- **Facilitate participation in international policy fora:** Finally, if developing country representation is to increase in international institutions, it is essential that such institutions specifically consider developing countries in their organizational structure and processes. For example, meetings can be held in developing regions in order to minimize attendance costs. Scheduling of events should also take into account other international events that might require the participation of the limited talent pool available in developing countries. And finally, internal governance structures (e.g., the allocation of seats or voices on committees, the balance of power between different sub-committees) can be designed in a way to enhance developing country interests. It could be possible, for example, to create advisory committees whose specific goals are to provide input on developing country needs.

IV. MODELS AND CONCEPTS

What is self-governance and what are its limitations?

The concept of "self-governance" drew attention in the early days of the Internet, when it was felt that the network's success depended on keeping the State out. At the same time, it was recognized that some form of control and management would be required to deal with increasingly evident challenges such as information pollution, fraud, and the requirements of standardization. Many experts and users therefore called for a form of regulation in which private and other entities would, in essence, police themselves (sometimes in accordance with broad guidelines laid down by the State). In such a framework, network providers, for example, would not have to deal with intrusive government monitoring, but would nonetheless have to adhere to broadly accepted quality of service standards and other obligations. Advocates of self-governance pointed out that one of its chief advantages would be to shift the responsibility of regulation onto those who had the relevant expertise.

Although popular in the late 1990s, self-governance has since fallen on somewhat hard times. There are at least two reasons for this. First, the concept has always suffered from a certain conceptual lack of clarity. As Monroe Price and Stefaan Verhulst noted in a paper on the related concept of self-regulation: "The Internet is a consummate demonstration of the complexity of determining what ought to be included in the 'self' of self- regulation.... In many discussions, governments have failed to recognize that the Internet industry is not monolithic and that there is no single 'industry' that speaks for the whole of the Internet"[42]. This difficulty in identifying a cohesive "self" has also made it difficult to draft a broad series of guidelines that would apply across sectors and user-categories; in effect, it became clear that a somewhat more detailed level of policing was required than that possible under self-governance.

In addition, and perhaps more importantly, it has become clear in recent years that the Internet cannot be managed without a certain degree of active participation by the State. Governments need not be all-powerful, but they are often essential to help manage critical infrastructure, and to ensure civil liberties and other public values. Indeed, the need for the State to be involved in Internet governance was recognized by WSIS, which in its Declaration of Principles states that: "Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues."[43]

What is multi-sectoral governance?

The failure of self-governance, and the accompanying recognition that action would be required at the many layers described in Section II, have led many in the Internet community to call for a new, multi-sectoral model of governance. As its name implies, multi-sectoral governance begins from the premise that all stakeholders – governments, private companies, civil society (including NGOs and consumer groups) – need to be involved in Internet governance. Only the collaborative participation of each of these actors can address the range of issues outlined earlier.

In its Declaration of Principles, WSIS outlined the following responsibilities for each sector:[44]

- Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues;
- The private sector has had and should continue to have an important role in the development of the Internet, both in the technical and economic fields;
- Civil society has also played an important role on Internet matters, especially at the community

[42] Price, Monroe and Verhurst, Stefaan (2001), p. 11
[43] http://www.itu.int/wsis/docs/geneva/official/dop.html
[44] http://www.itu.int/wsis/docs/geneva/official/dop.html

level, and should continue to play such a role;

- Intergovernmental organizations have had and should continue to have a facilitating role in the coordination of Internet-related public policy issues; and
- International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.

What are some of the challenges to effective multi-sectoral governance?

Despite the obvious benefits, some challenges exist to the ideal of multi-sectoral governance. One of the most significant stems from what could be called *gaps in culture and vocabulary* between sectors. In many ways, each sector speaks a different language, and underlying this linguistic distance is usually a different set of priorities and goals. Historically, for example, the relationship between the private sector and civil society has often been adversial. To take just one issue: while it is clear that both need to work together to ensure privacy, the private sector is likely to continue emphasizing profits (often in the name of greater usability) while civil society groups would, in general, restrict profits in the name of greater individual rights. The State, too, has a somewhat difficult relationship to the private sector, particularly in many developing countries, where the latter has often just emerged from the shadow of heavy government regulation. ISPs, software firms and other companies are likely to be extremely wary of greater State involvement.

In addition to distrust and misunderstanding between sectors, multi-sectoral governance also faces challenges from a *lack of co-operation within sectors*. It is important to keep in mind that civil society, for example, does not represent a uniform block. In fact, smaller and less lavishly funded civil society groups from the developing world often resent the perceived high-handedness of larger NGOs from the developed world. When a consumer group from Europe or the United States speaks at a governance forum, it is hard to make the case that that group represents users in smaller and poorer developing countries. Likewise, governments from developing countries are often at loggerheads with those from the developed world; in the controversy surrounding ICANN, which has often been perceived as dominated by the US government, this is one of the most contentious issues.

Finally, multi-sectoral governance faces the difficulty of finding and working within adequate institutional structures. Few models, and even fewer unequivocally successful models, for multi-sectoral governance exist. Developing the right structures to ensure accountability, representation and legitimacy are key issues that need to be addressed in the coming years if the ideal of multi-sectoral governance is to be realized.

What is the role of average Internet users in Internet governance?

While the roles of the private sector, governments and civil society are usually recognized, discussions of Internet governance typically overlook the importance of average users.

In fact, however, average users have an instrumental role to play in solving (or at least alleviating) many of the most difficult challenges facing the Internet. For example, users are the first line of defence in combating so-called "phishing", in which fraudulent e-mailers direct users to websites that collect and misuse passwords and other private (often financial) information. While many such websites are fairly sophisticated, well-informed and educated users are far less likely to fall prey to such scams. Likewise, informed users are less likely to allow their computers to be used in denial-of-service attacks (a process by which spammers hijack a computer and employ it to send out mass e-mails).

Both these examples suggest the importance of user education and information. Any system of governance that excludes average users is simply limiting its own effectiveness.

How democratic should Internet governance be?

On the face of it, this should be an easy question to answer. As the preceding discussion has shown, including average users is often critical to the success of governance mechanisms. More generally, at a time when the world's polity is moving towards near-universal adoption of democratic processes, it would be strange indeed if the Internet were to remain an exception.

Nonetheless, Internet policy-making does raise some difficult questions regarding the balance between technical expertise and widespread public participation, and more generally between efficiency and democracy. Many Internet bodies (particularly those in the standards-setting arena) are composed of experts who make decisions on the basis of consensus regarding the best technical solutions. Given the high level of technical knowledge required for such decision-making, many feel that opening up such bodies to participation by the general public would limit their effectiveness. After all, the argument goes, what does an average user know about standard-setting, interconnection regimes, or intellectual property? Their participation is only likely to slow the process, or lead to lowest-denominator compromise solutions that harm the Internet.

ICANN, in particular, has been at the centre of the debate over democracy and technical decision-making. ICANN's 2000 "At-Large Elections", in which anyone with an email address could participate in a process to elect board members, were billed as the first instance of true international democracy. A few years later, however, the experiment was felt by some to have been a failure, and the elected board seats were cancelled, replaced by a nominating committee that selects more than half the board and a number of other ICANN leadership positions. Although this change elicited widespread opposition, ICANN defended it as necessary to streamline the organization's decision-making processes. As one ICANN board member put it at the organization's meeting in Montevideo, Uruguay, in 2001: "ICANN is a technical organization, not a democracy."[45]

Such arguments need to be taken seriously. But many civil society and other representatives also argue that considerations of efficiency and technical expertise should not be taken as a license to impose unrepresentative decision-making on the Internet. After all, such considerations could logically be extended to various aspects of political life, too (for example, in the realm of economic decision-making). More generally, as we have seen, user participation and trust is essential to the success of the Internet. This means that a balance must be achieved between both technical and democratic requirements. This balance is likely to be found in institutional structures that permit public participation, but allow decision-making to be guided by, for example, elected technical experts. Education and awareness-building programmes that build technical capacity in average users are also critical.

What is the role of "trust" in Internet governance?

Economists and sociologists now recognize that trust is central to the functioning of any social and economic system. Trust, as defined by the sociologist Niklas Luhmann in a classic work on the subject, mediates risk;[46] or, as another sociologist puts it, trust is "a kind of social glue that allows people to interact" in a coordinated and co-operative fashion.[47]

Trust plays a particularly critical role in the online world. In a famous cartoon, published in 1993 in *The New Yorker* magazine, a dog sitting at a computer states that: "On the Internet, nobody knows you're a dog." The darker side of the anonymity celebrated by the dog is the fact that it also facilitates fraud and other illicit actions. Much as no one can identify a dog, so it is difficult to identify a fraudster hiding behind a fake user name on the other side of the world. Anonymity on the Internet also permits the spread of spam, viruses and other forms of pollution by making it harder to track down perpetrators.

The proliferation of fraud and pollution is a serious problem that risks eroding the trust of Internet users. If that happens – if users stop using e-commerce or email for fear of being cheated or overrun with viruses – then the Internet would be in grave jeopardy. Mechanisms to encourage trust are therefore essential components of any governance toolkit. They are particularly important to the spread of e-commerce in the developing world, where credit card penetration is low and payment is often made by cheque or other non-real-time methods that facilitate fraud.

Mechanisms to enhance trust can, of course, include traditional law-enforcement techniques that punish perpetrators of fraud, and establish laws for tracking down content polluters. However, several non-traditional mechanisms have also arisen that include other sectors. These include third-party verification entities that certify websites. Another common mechanism is the use of online reputation systems, such as those promoted by eBay and other e-commerce sites that allow buyers to rate sellers' reliability and honesty.

[45] http://www.icann-ncc.org/pipermail/discuss/2001-September/003515.html
[46] Luhmann, Niklas (1979), *Trust and Power*. New York: John Wiley, p. 24
[47] Ribstein, Larry (2001), "Law V. Trust," *Boston University Law Review* (81), p. 553

What is the relationship between globalization and Internet governance?

The Internet is one of the key drivers of globalization. It is largely because of email, cheaper international IP telephony, and the ease of publishing content for a global audience that the world feels smaller than ever before.

At the same time, the Internet is itself in many ways affected by globalization. Indeed, some of the key challenges confronted on the Internet are the results of globalization. For example, the sprawl of the network across national legal systems and jurisdictions is part of what makes it very difficult to manage (or "govern") the network. When users in one country download information posted in another country, national jurisdictions frequently collide. Perhaps the most famous instance of this occurred in 2000, when a French court demanded that Yahoo! remove Nazi memorabilia from an online auction site; while sale of the memorabilia was legal in the United States (where the seller was based), it was illegal under French hate-speech laws. Earth Station 5 (ES5), a file-sharing network that has been accused of facilitating copyright infringement, also illustrates the problem of jurisdiction; operated from the West Bank and Gaza, the network exists in a legal no-man's land, safely beyond the reach of most state authorities.

Confusion over jurisdictions (which often reflect clashing social and cultural norms in different countries) makes it difficult to manage the Internet in a cohesive manner. Many experts feel that effective Internet governance relies on greater legal harmonization at the national level, for example, in treaty-based or other multilateral organizations. But even were such harmonization achieved, the Internet makes it complicated to enforce and implement an international governance system. For one thing, the Internet's technical architecture, and particularly the anonymity it confers, makes it difficult to track down perpetrators, especially if they are located in another country. In fact, the architecture makes it difficult even to know in which country a user is located. Faced with the French court's ruling, Yahoo! argued that it was impossible to comply as it had no way of identifying the location of its users. Removing the auction items altogether, the company reasoned, would amount to imposing French laws on a global audience.[48]

Such difficulties have, to an extent, been mitigated by the rise of geo-location devices that make it more feasible to identify where users are based. But it is still easy for users with even a modicum of technical knowledge to sidestep such technologies. And geo-location techniques are themselves controversial; many people fear that they permit an unhealthy level of control on the network.

Ultimately, successful Internet governance will depend on finding solutions to such thorny problems raised by globalization. A number of governance bodies, notably treaty-based entities like WIPO, WTO and ITU, have always taken an international approach to governance, but they need to contend with a very different problem: the need to remain sensitive to local laws, norms and sentiments. It is unlikely that any one-size-fits-all model of Internet governance will prove sufficient. Successful governance will depend on finding the right balance between the global and the local – a process that development experts call "glocalization".

What is convergence and why does it matter?

Although a somewhat contested notion, convergence broadly refers to the gradual erosion of boundaries between different forms of communication. This process is driven by the digitalization of media: because different types of content (e.g., voice, data and images) can today be broken up into bits and bytes, this means that they can be transmitted along the same networks. Although convergence remains a work in progress, many users already use a single broadband line to send email, listen to music, engage in telephony, and watch movies or TV.

Convergence is a powerful force that is redefining the landscape of Internet governance. Two important consequences in particular can be highlighted:

First, the blurring of lines between means of communication also implies a gradual blurring of lines between governance bodies and responsibilities. In an era of convergence, it no longer makes much sense to have separate systems for governing, say, telecommunications and television. Indeed, a growing number of countries have introduced legislation or already have systems in place to install so-called "super-regulators" that would govern across media sectors. Singapore, for example, was one of the first countries in the world to create a converged regulatory body, the Info-Communications Development

[48] Ultimately, in fact, Yahoo! was able to implement technology that restricted the sale of such items to all but a very small minority of French users.

Authority of Singapore (IDA), which in 1999 merged regulation of telecommunications with information technologies. Malaysia, too, has a converged regulatory body, the Malaysian Communications and Multimedia Commission; and India's Communication Convergence Bill, which was passed by parliament but is currently pending, similarly envisions a cross-sectoral regulator.

This union of governance functions is not restricted to oversight by national governments. At the international level, too, there is growing awareness that multilateral organizations and other groups whose responsibilities have hitherto been restricted to a single form of media may need to widen their horizons. ITU, for instance, has gradually widened its responsibilities beyond pure telecommunications; today it is intimately involved in a number of Internet and, more generally, ICT-related issues. The work surrounding ENUM, which involves IETF, ITU and other bodies, is another example of attempts to establish a governance framework across distinct media categories.

This convergence of governance functions, like the underlying convergence of technologies by which it is driven, is still incomplete. Turf-fighting and lack of cross-sectoral technical capacity continue to slow it down. Nonetheless, it is an inevitable process that is already having dramatic effects on the landscape of Internet governance, and is likely to continue having such effects in the future.

How can Internet governance adapt to technological change?

Convergence is but one (albeit dramatic) instance of the rapidity with which technology changes. Just a decade ago, it would have been virtually unimaginable for a user in Asia to purchase and download music across a global network from America. Yet today this happens on a regular basis, and in the process, raises difficult questions regarding governance. We have seen some of these questions in our discussions of globalization and convergence.

Such questions and challenges are only likely to intensify in the coming years. As technology continues to change ever more rapidly, existing governance bodies and institutions have two options. They can either re-tool their systems each time a new technology comes along, or they can create systems today that are flexible enough to accommodate new technologies as they emerge. The first response is called "reactive regulation", and is generally considered an unsatisfactory and inefficient form of governance. It means that governance is always one step behind technology, and it can lead to governance systems that lack coherence or unity. In addition, it leads to a form of "technological determinism," in which our laws and governance systems are shaped (i.e., determined) by technology rather than by broader social, political and economic goals.

To avoid such reactive responses, governance structures should be shaped, to the greatest extent possible, so that they are "technology neutral". This means that they remain broad, and flexible enough to accommodate new technologies as they are developed. Laws need to be framed not with reference to any specific technology, but rather with reference to a society's underlying values and socio-political goals.

Consider, for instance, the issue of universal access. Universal access policies that are narrowly tailored to a specific technology (e.g., fixed-line telephony) are unlikely to fulfill their underlying motive (i.e., providing access to as many people as possible). This is because they leave new, potentially cheaper and more flexible, technologies out of their ambit. As cheaper wireless technologies emerge on the market and become viable methods for access, it no longer makes sense to exclude them from universal service obligations or government subsidies aimed at boosting access. For this reason, universal access policies need to be drafted in as broad and technology neutral manner as possible, with reference to the wider goal of providing access, not to the specific technologies deployed towards that goal.

V. CONCLUSION: BEST PRACTICES AND LOOKING FORWARD

What best practices can we identify?

The preceding discussion covers a wide variety of issues and governance possibilities. In an attempt to synthesize this broad-ranging discussion, six general principles (or Best Practices) can be identified for Internet governance:

- ***Multi-stakeholder alliances***: We have seen that, on a number of issues, Internet governance is most effective when it includes a diversity of actors. Spam, cybercrime, standards, and much more: all of these require participation by national governments, the private sector, civil society, and consumer or citizen groups. All steps should therefore be taken to develop mechanisms and institutions that bring together these various actors and harness their skills through multi-stakeholder alliances.

- ***Foster participation:*** In order to be accountable and representative, Internet governance needs to be seen as the outcome of a truly participatory process. All affected stakeholders should have a voice, and special care must be taken to include traditionally under-represented groups such as women and developing countries. Importantly, these steps should be substantive and meaningful: in practical terms, this means supplementing procedural mechanisms with capacity-building, education and resource support.

- ***International approach:*** The Internet is a global network, and its governance similarly requires a global approach. Nation-specific mechanisms are often ineffective, or even harmful to the seamlessness of the network. It is therefore essential to develop institutions, bodies, fora and treaties that deal with governance issues in an international and coordinated manner.

- ***Technology neutral approach:*** Part of the Internet's success stems from its openness to new means of communication: as long as a technology respects the network's core standards and protocols, it can join the network. Internet governance must take a similarly technology neutral approach, encouraging the process of convergence, and ensuring that no particular technology is given regulatory precedence over another. This is particularly important for developing countries, where wireless and IP technologies hold great promise for bridging the digital divide.

- ***Maintain original architecture:*** All governance measures must respect the underlying architecture of the Internet, and particularly the e2e principle and the use of open standards. This underlying architecture is at the root of the network's phenomenal spread and success, and should be considered non-negotiable in whatever discussions or outcomes result from WSIS and any other process.

- ***Supplement law:*** Finally, and to return to our discussion at the start of this primer, it must be kept in mind that governance means more than just government and government policy. This also implies that traditional State law should be supplemented and enhanced by other, non-legal, mechanisms. Such mechanisms can include innovations like open source, the use of self-governance and codes of conduct, and the general use of technology to supplement law. The important point is that law is but one tool in the arsenal of effective Internet governance.

What is the future of Internet governance?

As this primer was being finalized, WGIG had just issued its report. The report includes a number of recommendations regarding those issues it considers at the top of the governance agenda. It also recognizes concerns with existing models of governance, and suggests four models for the future. The WGIG is itself agnostic with regard to the choice of models.

In many ways, then, it is clear that Internet governance remains a work in progress, with its final dispensation and shape unlikely to emerge in the immediate future. While it is always difficult (and dangerous) to make predictions, some likely trends can, however, be identified. In particular, it appears likely that in the future national governments may play a greater role in Internet governance, although it should be noted that many actors remain wary of granting States too much power. In addition, steps will most likely be taken to enhance participation, particularly by developing countries. Generally, there will be a concerted effort to enhance the Internet's role as a tool for social and economic development – and, concomitantly, to enhance the scope of Internet governance beyond the merely technical.

These changes are likely to be evolutionary rather than revolutionary. Nearly everyone involved in the WSIS process recognizes that changes to Internet governance must be made cautiously, without disrupting the underlying architecture, and without breaking a system that, whatever its imperfections, does in fact function rather well. For this reason, discussions over governance are likely to extend well beyond the November 2005 meeting in Tunis. The current process of reappraisal and the search for alternatives represent just the beginning of a more general discussion that will, no doubt, continue for several years, if not decades.

WORKS CITED AND SUGGESTIONS FOR FURTHER READING

Abbate, Janet (1999), *Inventing the Internet*. Cambridge, MA: MIT Press.

Baird, Zoe and Verhulst, Stefaan (2004), "A New Model for Global Internet Governance". Paper available for download at: http://www.markle.org/downloadable_assets/ahs_global_internet_gov.pdf

Berners-Lee, Tim (2000), *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web*. New York: HarperBusiness.

Digital Opportunity Task Force (2002), *Global Policymaking for Information And Communications Technologies: Enabling Meaningful Participation by Developing-Nation Stakeholders*. Available at: http://www.markle.org/downloadable_assets/roadmap_report.pdf

Fransman, Martin (2002), "Mapping the evolving telecoms industry: the uses and shortcomings of the layer model", *Telecommunications Policy* (26), p. 473

Gelbstein, E. and Kurbalija, J. (2005), "Internet Governance: Issues, Actors and Divides", GKP Issues Paper, Diplo Foundation. Available at: http://www.diplomacy.edu/isl/ig/

Internet Governance Project (2004), *Internet Governance: The State of Play.*

Available at: www.InternetGovernance.org

Lessig, Lawrence (1999), *Code and Other Laws of Cyberspace*. New York: Basic Books.

Maclean, Don *et. al.* (2003), "Louder Voices: Strengthening Developing Country Participation in International ICT Decision-Making", London: Commonwealth Telecommunications Organisation & Panos.

The Markle Foundation (2003), "Guide to International ICT Policy Making", New York. Available at: www.markle.org

Mueller, Milton (2004), *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT.

Nicol, Chris (2003), *ICT Policy: A Beginner's Handbook*. The Association for Progressive Communications. Available at: http://www.apc.org/books

Open Regional Dialogue on Internet Governance (2005), "Voices from Asia-Pacific: Internet Governance Priorities and Recommendations", An ORDIG Paper for the UN Working Group on Internet Governance and the World Summit on the Information Society. Bangkok: UNDP-APDIP. Available at: http://www.apdip.net/news/ordigdocs

Peake, A. (2005, *forthcoming*), "Internet governance and the Asia Pacific: Urgent issues for the region", in Chin, S.Y. (ed.), *Digital Review of Asia Pacific*, Penang: Southbound. Available at: http://www.digital-review.org).

Price, Monroe and Verhulst, Stefaan (2000), "In Search of the Self." Working paper available at http://papers.ssrn.com/sol3/paper.taf?abstract_id=216111

Richmond, Riva (2005), "Internet Scams, Breaches Drive Buyers Off the Web, Survey Finds", *Wall Street Journal Online*, Jun. 23, p. B3.

Saltzer, Jerome *et. al.* (1984), "End-to-end arguments in system design", *ACM Transactions on Computer Systems 2*, 4 (November 1984), pp 277-288. An earlier version appeared in the Second International

Conference on Distributed Computing Systems (April, 1981) pp 509-512.Thierer, Adam (2003), *Who Rules the Net? Internet Governance and Jurisdiction*. Washington: Cato Institute.

Werbach, Kevin (1997), "Digital Tornado: The Internet and Telecommunications Policy", OPP Working Paper Series No. 29. Washington: FCC. Available at http://www.kentlaw.edu/legalaspects1/aspectsofe-commerce(ac)/readings/digital%20toronado.pdf

Whitt, Richard (2004), "A Horizontal Leap Forward – Formulating a New Policy Framework Based on the Network Layers Model," global.mci.com/about/publicpolicy/presentations/horizontallayerswhitepaper.pdf

Working Group on Internet Governance (2005), *Report of the Working Group on Internet Governance.* Available at: http://www.wgig.org/docs/WGIGREPORT.pdf

APPENDIX 1: SELECTED ORGANIZATIONS INVOLVED IN INTERNET GOVERNANCE

ORGANIZATION	FUNCTION
APEC TEL - Asia Pacific Economic Cooperation in Telecommunications and Information Working Group http://www.apectelwg.org/	▸ Consists of 23 countries in the Asia-Pacific region ▸ Promotes development of Internet infrastructure, including Network Access Points, in the APEC region ▸ Promotes policy and regulations intended to stimulate trade and investment for the ICT sector in the region ▸ Involved in capacity building through ICT training ▸ Founded in 1990, headquarters in Singapore
ATU - African Telecommunications Union http://www.atu-uat.org/	▸ Forum of 46 African countries and 10 Associate Members (comprising telecom operators) ▸ Lobbies on behalf of its members for globally allocated ICT resources such as Internet addresses ▸ Represents the interest of African countries at international forums ▸ Supports policy harmonization amongst its member States and promotes regional market integration ▸ Founded in 1977, headquarters in Nairobi, Kenya
CENTR - Council of European National TLD Registries http://www.centr.org/	▸ Association of top-level country code domain registries, primarily in Europe, but also open to non-European ccTLD managers ▸ Lobbies on behalf of ccTLDs at Internet governing bodies like ICANN ▸ Advises European governments and EU on ccTLD policy and regulatory matters ▸ Founded in 1998, headquarters in Brussels, Belgium
CERN - Conseil Européen pour la Recherche Nucléaire http://public.web.cern.ch/	▸ A fundamental physics research organization of 20 Europeans countries focused on particle physics ▸ HTML, HTTP and the World Wide Web were developed here ▸ Founded in 1954, headquarters in Geneva, Switzerland
CERT - Coordination Center http://www.cert.org/	▸ Funded by the US federal government to coordinate between Internet security experts during serious attacks on the Internet ▸ Conducts vulnerability analysis of Internet infrastructure and informs the larger Internet community of possible dangers ▸ Founded in 1988, headquarters in Carnegie Mellon University, Pittsburgh, USA ▸ There are many similar organizations formed in many jurisdictions around the world in emulation of this concept
CITEL - Inter-American Telecommunications Commission http://www.citel.oas.org/	▸ Composed of 35 member states in the Americas and 200 associate members ▸ Evaluates regulatory, technical and legal mechanisms to promote harmonization across member States ▸ Develops regional standards for value-added networks ▸ Promotes coherence of certification procedures for telecommunication equipment ▸ Founded in 1923, headquarters in Washington DC, USA
CoE - Council of Europe http://www.coe.int/	▸ Distinct from the EU, this organization has as members 46 countries from Europe ▸ It was founded, among other things, to develop continent-wide agreements to standardize member countries' social and legal practices ▸ Finalizing world's first international convention on cybercrimes ▸ Promotes e-governance and data protection ▸ Founded in 1949, headquarters in Strasbourg, France

ORGANIZATION	FUNCTION
Creative Commons http://creativecommons.org/	▸ Non-profit organization funded by foundations and led by experts in cyberlaw and IPR ▸ Offers non-restrictive licenses to owners of creative work to share their work on the Internet ▸ Developed Web application to allow creative works to be made available in the public domain ▸ Founded in 2001, hosted at the Stanford Law School, California, USA
DITE -Division on Investment, Technology and Enterprise UNCTAD http://www.unctad.org/Templates/StartPage.asp?intItemID=2983&lang=1	▸ Part of the United Nations system, this division focuses on foreign direct investment and technology ▸ Produced study on intellectual property rights and its impact on developing countries ▸ Assists developing countries to building international competitiveness ▸ It runs programmes to encourage the use of new technologies ▸ Founded in 1964, headquarters in Geneva, Switzerland
EFF - Electronic Frontier Foundation http://www.eff.org/	▸ Non-profit organization composed of lawyers, IT experts and volunteers ▸ Defends civil liberties in cyberspace ▸ Active in a broad spectrum of rights issues in cyberspace including: File-sharing, Digital Rights Management, Internet governance, privacy and surveillance, spam and intellectual property rights ▸ Founded in 1990, headquarters in San Francisco, USA
ETSI - European Telecommunications Standards Institute http://www.etsi.org/	▸ Non-profit European standards body for telecommunications and ICTs ▸ Composed of 688 members from 55 countries inside and outside Europe, including manufacturers, network operators, administrations, service providers, research bodies and users ▸ Works closely with ITU for developing telecom standards ▸ Part of consortium that developed IPv6, 3G and GSM standards ▸ Founded in 1988, headquarters in Sophia-Antipolis, France
GAC - Governmental Advisory Committee of ICANN http://gac.icann.org	▸ Composed of representatives of national governments, multinational and treaty organizations attached to ICANN ▸ Provides policy input to ICANN on ccTLD names ▸ Conveys concerns of governments on how ICANN's policies interact with national laws or international agreements ▸ Founded in 1999, with a secretariat staffed at various times by the Australian government, the European Commission and potentially others
GBDe - Global Business Dialogue on E-commerce http://www.gbde.org/	▸ Business initiative led by CEOs to develop global policy framework for e-commerce ▸ Promotes harmonization of country regulations for uniform treatment of e-commerce activities ▸ Developed recommendations for micro-payments and secure online transactions ▸ Founded in 1999, headquarters in Vermont, USA
GICT - Global Information & Communication Technologies http://info.worldbank.org/ict/	▸ Spearheads the World Bank's efforts to expand access to ICT infrastructure in developing countries ▸ Provides policy advice to governments in the area of telecom liberalization, e-commerce and e-government ▸ Provides loans to subsidize the extension of the ICT infrastructure in rural and poor areas by private sector operators ▸ Founded in 1995, headquarters in Washington DC, USA

ORGANIZATION	FUNCTION
IAB - Internet Architecture Board http://www.iab.org/	▸ A 13 member technical reference group under ISOC, officially appointed by the ISOC Board, nominated by IETF ▸ Provides guidance and advice to ISOC and ICANN, among others, on technical, architectural and procedural matters related to the Internet ▸ Provides oversight of the process used to create Internet standards and protocols ▸ Issues guidelines on future strategies as they relate to the Internet's architecture ▸ Founded in 1984, virtual group
IANA - Internet Assigned Numbers Authority http://www.iana.org/	▸ IANA created in the earliest days of Internet development and run by Jonathan Postel until his untimely death in 1998. It functioned under the guidance of the IAB ▸ Integrated into the ICANN organization on its founding in 1998 ▸ Allocates Internet address space to RIRs ▸ Oversees the operation of the root name servers ▸ Oversees the DNS including creation of new TLDs, redelegation of ccTLDs. Updating of the root zone file ▸ IANA was an extension of the original ARPANET "Numbers Czar" position occupied by Jonathan Postel in 1969. Upon its creation around 1975, it was operated by USC Information Sciences Institute, Marina del Rey, CA until it was integrated with ICANN
ICANN - Internet Corporation for Assigned Names and Numbers http://www.icann.org/	▸ Coordinates the Internet's systems of unique identifiers: domain names, IP address, protocol port and parameter numbers ▸ Oversees the distribution of unique identifiers ▸ Fosters competition within domain name registry industry ▸ Creates new top-level domain names, delegation of ccTLDs ▸ Oversees the DNS root name server system ▸ Founded in 1998, headquarters in Marina del Rey, California, USA
ICCP - Committee for Information, Computer and Communications Policy, OECD http://www.oecd.org/department/0,2688,en_2649_34223_1_1_1_1_1,00.html	▸ Arm of the OECD, composed of 30 developed countries, that addresses issues arising from the "digital economy" ▸ Produces research publications and statistics to contribute to more informed ICT policy-making among member States ▸ Analyses the broad policy framework underlying the "e-economy", the information infrastructure and information society ▸ Founded in 1947, headquarters in Paris, France
IEEE - Institute of Electrical and Electronic Engineers http://www.ieee.org	▸ A non-profit technical association of engineers numbering 360,000 from 175 countries ▸ It is a leading technical authority and standards body for telecommunication, computer engineering and other areas ▸ Developed 802.11b developed for the Wireless LAN or WiFi ▸ Founded in 1961, headquarters in New York, USA
IESG - Internet Engineering Steering Group http://www.ietf.org/iesg.html	▸ Group composed of members from IETF and functions under ISOC ▸ Provides the final technical review of Internet standards ▸ Issues the final approval of specifications as Internet standards ▸ Responsible for day-to-day management of the IETF and monitors quality of its output ▸ Founded in 1989, virtual group

ORGANIZATION	FUNCTION
IETF - Internet Engineering Task Force http://www.ietf.org/	▸ Structured as a loosely self-organized group of people whose leadership is appointed by IAB and functions under ISOC ▸ Concerned with developing, testing and implementing new Internet technical standards ▸ The technical work gets done in its working groups organized by topic (routing, transport, security, etc.) ▸ Proposes standards to IESG for final approval ▸ Founded in 1986, secretariat operated since 1988 by CNRI in Reston, Virginia, USA
Information Society and Media Directorate-General, EU http://europa.eu.int/comm/dgs/information_society	▸ A unit of the EU that produces research and policy initiatives in the area of Information Society technologies ▸ Initiated eEurope Action Plan touching number of areas including broadband, e-business, e-government, spam, privacy and data protection, and security for adoption by EU member States ▸ Headquarters in Brussels, Belgium
ISO - International Organization for Standardization http://www.iso.org	▸ Composed of national standards institutes from 148 countries ▸ The world's largest developer of standards ▸ Its principal activity is the development of technical standards ▸ Developed two-letter code standard for representing country name on which country top-level domain names are based ▸ Founded in 1947, headquarters in Geneva, Switzerland
ISOC - Internet Society http://www.isoc.org/	▸ International organization composed of 100 organizations and 20,000 individuals that addresses technical and policy challenges facing the Internet ▸ Organizational home for groups responsible for the Internet's architecture and standards-IAB, IETF, IESG, and IANA, etc. ▸ Provides forums to discuss the future evolution of the Internet ▸ Sponsors training workshops in developing countries ▸ A global clearinghouse for information on the Internet ▸ Founded in 1992, headquarters in Reston, Virginia, USA
ITU-D - International Telecommunication Union Development Bureau http://www.itu.int/ITU-D/	▸ The development arm of the ITU, composed of member States and private organizations like telecom operators and equipment manufacturers ▸ Provides assistance to developing countries in the field of ICTs ▸ Helps developing countries evolve telecommunication policies and strategies ▸ Mobilizes technical, human and financial resources needed for extending network infrastructure and services ▸ Supports initiatives to bridge the digital divide ▸ Founded in 1989, headquarters in Geneva, Switzerland
ITU-R - International Telecommunication Union Radiocommunication http://www.itu.int/ITU-R/	▸ The arm of ITU, composed of member states and private organizations, that deals with the allocation of finite telecommunication resources ▸ Allocates bands of the radio frequency spectrum, frequency and satellite orbits for a variety of services including fixed and mobile telephony, broadcasting, amateur radio, space research, meteorology, global positioning systems, etc. ▸ Developed the IMT 2000 standard for broadband mobile Internet and wireless data transmission ▸ Founded in 1992, headquarters in Geneva, Switzerland

ORGANIZATION	FUNCTION
ITU-T - International Telecommunication Union - Standardization http://www.itu.int/ITU-T/	▸ The standardization arm of ITU, composed of member States and private organizations like telecom operators and equipment manufacturers ▸ Provides global telecommunication standards by issuing recommendations ▸ Issues standards from numbering plans and accounting rates to the functioning of circuit-switched networks, packet-based voice and data networks ▸ Founded in 1992, headquarters in Geneva, Switzerland
MINC - Multilingual Internet Names Consortium http://www.minc.org/	▸ A non-profit, non-governmental, international organization that focuses on developing and promoting multilingual Internet domain names and keywords ▸ Composed of individual members from all continents of the world and from different sectors – industry, academia, research, government, investors and international organizations ▸ Promotes internationalization of Internet names standards and protocols by coordinating with other international bodies like ICANN, ITU, IETF and as well as language groups ▸ Founded in 2000, headquarters in Jordan
NRO - Number Resource Organization http://www.nro.net	▸ Formed in 2003 by the four RIRs – APNIC, ARIN, LACNIC and RIPE NCC ▸ The purpose of the NRO is to undertake joint activities of the RIRs, including joint technical projects, liaison activities and policy coordination ▸ Aims to protect the unallocated Number Resource pool; promote and protect the bottom-up policy development process ▸ Acts as a focal point for Internet community input into the RIR system
RIPE NCC http://www.ripe.net/	▸ A non-profit membership organization that supports the infrastructure of the Internet through technical co-ordination in its service region ▸ The RIPE NCC service region consisting mainly of ISPs, telecommunication organizations and large corporations located in Europe, the Middle East, Central Asia and African countries ▸ Acts as a RIR and allocates and assigns IP address space and other Internet numbers to its members ▸ Founded in 1992, headquarters in Amsterdam, the Netherlands
SIP forum- Session Initial Protocol forum http://www.sipforum.org/	▸ The forum is made up of individuals, network engineers, application developers and other Internet professionals ▸ Focus is on developing global Internet communications based on Session Initiation Protocol (SIP) ▸ Advances the adoption of products and services based on SIP, namely Internet technologies such as IP phones, PC clients, SIP servers and IP telephony gateways ▸ Explicitly not a standards-setting body. IETF defines the core SIP protocol ▸ Founded in 1996, headquarters in Stockholm, Sweden

ORGANIZATION	FUNCTION
UN ICT Task Force - United Nations Information and Communication Technologies Task Force http://www.unicttaskforce.org	▸ A UN task force supported by the Heads of State and governments of all UN member States ▸ Formulates strategies for the UN to use ICTs for development ▸ Launched initiatives to bridge the global digital divide ▸ Established Working Group on ICT governance for helping developing countries play a role in global ICT policy-making ▸ Founded in 2001, headquarters in New York, USA
UNDP-ICTD – United Nations Development Programme-Information, Communication Technologies for Development http://sdnhq.undp.org/it4dev/	▸ ICTs for development is a crucial component of UNDP's global development strategy ▸ Assists developing countries in designing and implementing strategies for leveraging ICTs for development ▸ Supports WSIS activities through substantive contribution and logistical help ▸ Assists developing countries to make use of Free/Open Source software ▸ Links deployment of ICTs to poverty reduction strategies ▸ Founded in 1992, headquarters in New York, USA
UNESCO CI - United Nations Educational, Scientific and Cultural Organization - Communication and Information Sector http://portal.unesco.org/ci/en	▸ Embedded within UNESCO, its programmes focus on promoting universal access to ICTs, especially in developing countries ▸ Promotes multilingualism on the Internet ▸ Supports initiatives to fight poverty through ICTs ▸ Founded in 1990, headquarters in Paris, France
W3C - World Wide Web Consortium http://www.w3.org/	▸ The Consortium consisting of 350 members is mainly composed of organizations and government entities ▸ Develops Web application standards and guidelines to allow hardware and software used to access the Web to work together ▸ Developed simple mechanism to add style (e.g. fonts, colours, spacing) to Web pages via Cascading Style Sheets (CSS) ▸ Launched Web Accessibility Initiative to make the Web accessible to all regardless of physical disabilities ▸ Developed XML that allow interoperation between different software applications, running on a variety of platforms ▸ Founded in 1994, collaborative headquarters in Sophia-Antipolis, France, MIT, Massachusetts, USA and Keio University in Japan
WGIG - Working Group on Internet Governance http://www.wgig.org/	▸ WGIG is a working group of WSIS tasked with developing a working definition of Internet governance and to identify public policy issues surrounding this topic ▸ The group's final report will be presented in the second phase of WSIS meeting in Tunis, November 2005 ▸ Founded in 2004, located within the UN Secretariat in Geneva, Switzerland
WIPO - World Intellectual Property Organization http://www.wipo.int/	▸ One of the specialized UN agencies consisting of 181 member States tasked with protecting intellectual property rights globally ▸ Promotes the protection of intellectual property (inventions, literary and artistic works, and symbols, names, images, and designs used in commerce) throughout the world through cooperation among States and other international organizations ▸ Played an early role in trademark disputes relating to domain names ▸ Co-developed with ICANN UDRP used to arbitrate trademark-based domain name disputes ▸ Founded in 1979 , headquarters in Geneva, Switzerland

ORGANIZATION	FUNCTION
WSIS - World Summit on Information Society http://www.itu.int/wsis/	▸ Summit conducted in two phases by UN and ITU to discuss strategies to bridge the digital divide between developing and developed countries ▸ Participants at the Summit consisted of UN member States, civil society groups and the private sector ▸ First phase of Summit discussed how to establish the foundations for an Information Society globally ▸ Explored strategies for using ICTs for promoting development goals of the Millennium Declaration ▸ Set up a number of working groups that are exploring issues related to Internet governance, intellectual property rights, management of the DNS, etc. ▸ Founded in 2001, rotating summits, no permanent headquarters
WTO - World Trade Organization http://www.wto.org/	▸ A global international organization consisting of 148 countries dealing with the rules of trade between nations ▸ Forum where trade agreements are negotiated and signed ▸ Has mandate to examine all trade-related issues relating to global electronic commerce ▸ Negotiated telecommunications agreement which liberalized telecom markets globally and introduced greater competition ▸ Founded in 1995, headquarters in Geneva, Switzerland

APPENDIX 2: ADDITIONAL BACKGROUND

Roles and functions of ICANN and IANA

The Internet Corporation for Assigned Names and Numbers (ICANN) was created in 1998 to institutionalize the oversight of the Internet's system of unique numbers and identifiers. The task had been the responsibility of Dr Jonathan Postel, a researcher who was deeply involved in the development of the Internet and who served as the Internet Assigned Numbers Authority (IANA) for over a quarter of a century. ICANN is a multi-stakeholder organization responsible for the "bottom-up" development of technical policy for the management of the unique names, numbers and identifiers associated with the Internet and the accreditation of the operators of certain key Internet functions. The IANA function is incorporated into the ICANN operation.

Due to its role in the initial development of the Internet, the US Government has played a key role in the oversight of the IANA function and more generally, ICANN. There is a Memorandum of Understanding (MoU) that guides ICANN's progress towards independent operation. The present MoU expires in September 2006 and it is expected that ICANN will operate as an independent entity assuming it is able to fulfill all of the obligations set forth in the MoU. In the interim, the US Government, by way of the Department of Commerce (DOC), National Telecommunications and Information Agency (NTIA), has the responsibility and authority to approve changes to the Domain Name Root Zone file. In all the years of IANA operation, the US Government has not rejected any recommendations for such a change.

Every device on the Internet has an Internet address (either a 32-bit or 128-bit number). The addresses are assigned on the basis of network topology so as to minimize the amount of information that has to be exchanged throughout the Internet to effect the routing of Internet packets from one place to another. IANA allocates blocks of Internet address space to the five RIRs who in turn allocate address space to ISPs or assign address space to qualified end users. There are five RIRs: APNIC (Asia/Pacific Rim), LACNIC (Latin and Central America), AFRINIC (Africa), RIPE-NCC (Europe), and ARIN (North America). The five RIRs, for purposes of developing global allocation policies, work together as the Number Resource Organization (NRO). Their recommendations come to ICANN for approval and adoption. The Executive Council of the NRO serves as ICANN's Address Supporting Organization and is responsible for appointing two of the members of ICANN's board of directors.

The Internet's DNS is used to translate domain names into Internet addresses. In rough terms, there are two major classes of domain names in the Internet system. The now-familiar 'www.icann.org' style of domain name is an example of a generic domain name and .org is a TLD. The other class is the country code domain name such as 'www.denic.de', where "de" stands for "Deutschland" or Germany. There are scores of generic top level domains (.com, .net, .org, .int, .edu, .mil, .gov, .arpa, .info, .biz, .museum, .jobs, .mobi, .travel, .cat, .coop, .aero, .post with others still pending). There are on the order of 200 country code TLDs (ccTLDs) such as .fr, .uk, and so on. The set of top level domains and the computers that translate domain names into Internet addresses form the distributed DNS. There is a central list of all top level domain name servers and this is called the Root Zone File. This list is replicated in Root Servers that are located throughout the Internet. IANA maintains the Root Zone File and provides updates to the Root Server operators as needed. There are 12 Root System Operators who are responsible for 13 Root Servers. By means of a special Internet routing system called "anycast" there are actually as many as 100 replicas of the Root Servers in operation throughout the Internet.

ICANN has extensive contractual relationships with most of the generic TLDs (exceptions being .mil and .gov which are operated by the US Government, .arpa and .int which are largely operated by IANA). ICANN has responsibility for delegating operation of the ccTLDs although with some exceptions, it does not have contractually documented oversight. Redelegation of the operation of a ccTLD is a responsibility of the IANA and very carefully structured processes and procedures are employed when such a redelegation is needed.

ICANN has a Country Code Name Supporting Organization (CCNSO) with membership drawn from the operators of ccTLD registries. ICANN also has a Generic Name Supporting Organization (GNSO) whose membership includes domain name registry operators, domain name registrars, ISPs, business community members and non-profit organizations. The CCNSO and GNSO each help to develop policy for adoption by the ICANN board and each appoints two directors to the Board of ICANN. The CEO of ICANN is an ex

officio member of the Board. The remaining eight directors of ICANN are appointed by a nominating committee whose membership is drawn broadly from the global Internet community.

In addition to its supporting organizations, ICANN has a number of advisory committees including the At-Large Advisory Committee (ALAC), charged with helping to organize policy input from civil society; the Root Server System Advisory Committee (RSSAC); the Security and Stability Advisory Committee (SSAC); and the Governmental Advisory Committee (GAC). The latter has membership from about 100 countries and is responsible for providing public policy input to the ICANN board.

Internet standards

In the early period of Internet development, an Internet Activities Board (IAB) was created by DARPA to oversee the standardization of Internet protocols. Later, the details of protocol development fell to IETF that spun out of the IAB. An Internet Research Task Force (IRTF) was also created to pursue advanced concepts not yet ready for standardization. In 1992, ISOC was formed to provide an institutional home for IETF, IRTF and IAB (renamed at that time the Internet Architecture Board). In addition, with the advent of the World Wide Web in 1989, W3C was formed to pursue further development of the standards and technologies of the World Wide Web. Other standards organizations also contribute technology that supports the Internet, notably IEEE andITU among others, such as regional and national standards bodies.

The Internet Society, in addition to supporting the IAB, IRTF and IETF also supports the Request For Comment (RFC) editor. The Request for Comment series of documents, founded in 1969 during the development of a predecessor to the Internet, the ARPANET, comprises the standards documentation for the Internet. The IANA maintains tables of Internet parameters that are referenced by the RFCs. The Internet Society has other outreach activities, including scores of chapters around the world and education and training programmes that promote technical competence in Internet implementation and operation.

ABOUT THE AUTHOR

Akash Kapur (www.akashkapur.com) is a consultant and writer based in South India and New York. He has written on technology, politics, literature and other topics for *The Atlantic Monthly, The Economist, The New York Times*, *The New Yorker*, *Slate, Wired* and several other publications. He has consulted on technology and development related issues for The Markle Foundation, UNDP, the US Trade and Development Agency (USTDA), and other organizations. Akash has a BA (summa cum laude) in Anthropology from Harvard University, and a DPhil (Law, specialized in technology law) from Oxford University, where he attended as a Rhodes Scholar.

APDIP

The Asia-Pacific Development Information Programme (APDIP) is an initiative of the United Nations Development Programme (UNDP) that aims to promote the development and application of new Information and Communication Technologies (ICTs) for poverty alleviation and sustainable human development in the Asia-Pacific region. It does so through three core programme areas, namely, Policy Development and Dialogue; Access; and Content Development and Knowledge Management.

In collaboration with national governments, APDIP seeks to assist national and regional institutions in the Asia-Pacific through activities that involve awareness-raising and advocacy, building capacities, promoting ICT policies and dialogue, promoting equitable access to tools and technologies, knowledge sharing, and networking. Strategic public-private sector partnerships and opportunities for technical cooperation among developing countries are APDIP's key building blocks in implementing each programme activity.

www.apdip.net

Also available from UNDP's Asia-Pacific Development Information Programme

e-Primers for the Information Economy, Society and Polity:

- e-Commerce and e-Business
- e-Government
- Genes, Technology and Policy
- ICT in Education
- Information and Communication Technologies for Poverty Alleviation
- Legal and Regulatory Issues in the Information Economy
- Nets, Webs and the Information Infrastructure
- The Information Age

www.apdip.net/publications

e-Primers on Free/Open Source Software:

- Free/Open Source Software – A General Introduction
- Free/Open Source Software – Education
- Free/Open Source Software – Government Policy
- Free/Open Source Software – Localization

www.iosn.net

UNDP

IDRC CRDI

Canada

world summit on the information society
Geneva 2003 - Tunis 2005

Asia-Pacific Development Information Programme

www.apdip.net

UNDP Regional Centre in Bangkok
United Nations Service Building
3rd Floor, Rajdamnern Nok Avenue
Bangkok 10200, Thailand

Tel: +66 2 288 1234; 288 2129
Fax: +66 2 280 0556