

PROVISIONAL DRAFT (SUBJECT TO CHANGE), 14 JULY 2005

The Emerging Internet Governance Mosaic: Connecting the Pieces

by

William H. Dutton
Oxford Internet Institute

Malcolm Peltu
Oxford Internet Institute

OII Forum Discussion Paper No. 5
Oxford Internet Institute
University of Oxford
1 St Giles, Oxford OX1 3JS
United Kingdom
July 2005

FOREWORD

An international forum entitled *The Struggle Over Internet Governance: Searching for Common Ground* was held at the University of Oxford on 5-6 May 2005. It brought together a group of knowledgeable and experienced participants, encompassing a broad range of perspectives, to explore key questions relating to Internet governance and regulation such as:

- What policy issues are relevant to Internet governance and which, if any, require enhanced or new governance processes or structures?
- How should the Internet be best steered in the future to sustain the continuing growth of Internet use?
- Which governance models and institutions are likely to be most effective in balancing the different perspectives and interests of government, private enterprise and civil society to address global, regional and local needs?
- What are appropriate models for Internet-related legislation and regulation and how best can wider policy implications be taken into account in developing appropriate Internet technology standards and protocols?
- What forms of capacity building support should be prioritized to facilitate more effective governance of the Internet?

The forum was co-organized by the Oxford Internet Institute (OII) and Berkman Center for Internet and Society. This report, one of a series of OII forum-based discussion papers, highlights key insights for Internet governance policy and practice, drawing primarily on discussions at the event and position papers and other contributions from participants.¹

We are indebted to all Forum participants (see Appendix I). Their expert, lively and questioning contributions provided a rich source for the paper, even where specific individuals could not be credited. The authors take sole responsibility for the interpretation of this material, while acknowledging the invaluable expert contribution from many participants in helping them to produce their analysis. Desiree Miloshevic and Emily Taylor played a key role in selecting participants and Christian Ahlert in his detailed comments on earlier drafts of the paper. We also greatly appreciate the financial support, participation and encouragement of the forum's sponsors: Afiliias, the *Economist*, Nominet UK and the Public Internet Registry. Special credit is due to the OII events and technical teams—especially Lucy Martin, Laura Oultram and Adham Tamer—for the smooth running of the event.

Professor William H. Dutton
Director, Oxford Internet Institute, University of Oxford

John Palfrey
Executive Director, Berkman Center for Internet and Society, Harvard Law School

¹ See <http://www.oii.ox.ac.uk/collaboration/?rq=specialevents/20050505> for copies of the position papers and other background to the forum.

EXECUTIVE SUMMARY

The first phase in Geneva in 2003 of the World Summit on the Information Society (WSIS) and the subsequent establishment by the United Nations of the Working Group on Internet Governance (WGIG) clearly indicated broad agreement that the Internet is a valuable tool that can be used by individuals, communities, business and governments for social and economic transformation and development.² The phenomenal growth in Internet use and the placing at users' fingertips of substantial 'communicative power' to command knowledge, economic and technological communication resources (Dutton 2004a) has interwoven the Internet and related information and communication technologies (ICTs) into the fabric of life in many areas of the world. This opens important opportunities to address a wide range of issues, such as those covered by the UN Millennium Development Goals (MDGs).³

The forum on which this paper is based discussed numerous governance issues arising from this global phenomenon. The authors identified the following as the most significant themes and suggestions to emerge from these discussions.

1. Applying different solutions for different Internet governance issues

The governance of issues related to the Internet is multi-layered, fragmented, complex and generally highly distributed. The Internet is not one technology but an assembly of many technologies at different levels. Governance is also not one process, but several at different levels and in overlapping arenas addressing specific issues. This means different government models and agencies that involve many different institutional, group and individual stakeholders will continue to be needed to address different governance issues.

2. Preventing fragmentation of the emerging Internet governance mosaic

The Internet's rapid growth was supported by highly flexible, decentralized and pluralistic governance arrangements involving many different institutions and individuals. Rapid and continuing growth in the uses and misuses of the Internet, and the industries and government activities linked to it, has created a danger that pieces of the ever-more complex emerging Internet governance mosaic will become too fragmented to manage the Internet effectively. However, attempts to centralize control are likely to stifle the innovation that has given the Internet its momentum.

3. Understanding how to manage Internet governance complexities is key

This paper proposes a three-level categorization of Internet governance issues raised at the forum and elsewhere, in order to understand the bigger picture into which this mosaic fits, and as a framework to help manage coordination between different areas:

- *Type I: Internet-centric*, concerned with protecting and advancing the Internet's core open architecture and operational infrastructure, including the preservation of its independence from undue influence by particular stakeholders.

² See www.unesco.org/wsis for more on the WSIS and www.wgig.org for more on the WGIG.

³ See www.un.org/millenniumgoals for details of the MDGs.

- *Type II: Internet-user centric*, focusing on the uses and misuses of the Internet with a prime governance aim of avoiding unnecessary constraints that could stifle the collaborative creativity, continued innovation and ability to adapt to rapid change that has underpinned and fuelled the Internet's popularity.
- *Type III: Non-Internet centric*, encompassing a vast range of wider international policy issues, such as human rights, cultural and linguistic diversity, intellectual property and the addressing of digital divides in unequal access to Internet services and the knowledge of how to use and manage them effectively.

4. Balancing interests in multi-stakeholder processes is inherently political

Recognition of the Internet's global importance is leading to growing demands from governments, private enterprises, non-governmental organizations (NGOs), communities and individuals around the world to be stakeholders and partners in its governance processes. The forum strongly confirmed recommendations from the WSIS and elsewhere for such multi-stakeholder, consensus seeking processes. Participants agreed the decentralized, borderless and technically complex nature of the Internet means that neither traditional intergovernmental governance processes nor purely technical governance would be suitable models, as they both lack sufficient accountability and are open to capture by special interests. However, some sharp differences of opinion at the forum illustrated the inherently political nature of trying to balance stakeholders' conflicting and complementary views, values and interests. Tensions between some 'good' Internet governance principles identified at the forum can also make it difficult to achieve a consensus. Realistic rather than Utopian policy goals acknowledging these tensions should therefore be set.

5. Coordinating the bigger picture to shape effective Internet governance

A key future Internet governance requirement will be to improve coordination between different governance organizations, using different models and processes, in a way that does not harm the network's growth. For example, an independent advisory coordinating group or forum with appropriate expertise could help to identify, alert and link relevant agencies to aspects of the bigger picture that may otherwise be missed or underplayed—but leave it to those organizations closest to an issue to arrange an appropriate way of dealing with it.

Structure of this paper

The next section highlights key Internet governance issues raised at the forum in relation to the authors' three-tier typology. The distinctive design and governance characteristics that underpin the global Internet phenomenon are then outlined, to indicate valuable governance lessons that can be built on. The crucial need for balance in inherently political multi-stakeholder processes is then addressed. This is assisted by an analytical framework for understanding the dynamics underlying such processes, which involve outcomes from decisions taken by many actors within overlapping and interacting policy arenas. The conclusion recommends an approach to improving international coordination of Internet governance activities. Appendix I lists participants and Appendix II is a glossary of terms and abbreviations.

1. THE KEY ISSUES ADDRESSED BY INTERNET GOVERNANCE

Classifying the emerging Internet governance mosaic

Forum discussions highlighted an enormous variety of related convergent and divergent pathways across the ever widening terrain encompassed by Internet governance issues. It is this diversity that poses one of the greatest threats to Internet governance: a fragmentation into different technical, application, policy and governance specializations that breaks up any coherent picture of what is trying to be achieved in governance processes related directly or indirectly to the Internet. One of the strongest themes that emerged from the forum was therefore the need for better coordination between the different agencies, structures and processes dealing with the ‘devil in the detail’ of specific parts of the bigger picture. As a step towards this, the authors have analyzed forum discussions to produce the broad classification of Internet governance issues identified in Table 1.

Table 1: Categories of Internet governance issues

<i>Type</i>	<i>Key issues</i>	<i>Examples</i>
I: Internet Centric	Development of core technical Internet infrastructure and Web standards and protocols. Sustains efficient, reliable Internet operations and timely adaptability to continuing and often rapid technological and other changes affecting the Internet.	<ul style="list-style-type: none">• Standards setting for the Internet and World Wide Web.• Assigning Internet addresses• Routing messages between senders and receivers.• Smooth and secure Internet operations and development of core systems and services.
II: Internet-User Centric	How use or misuse of the Internet by individuals, groups and organizations—for legal or illegal, appropriate or inappropriate behaviour—is defined and policed. Deals with policies generally set by local, regional and national jurisdictions, with international aspects developed through communication and negotiation among jurisdictions.	<ul style="list-style-type: none">• Unsolicited ‘spam’ e-mail.• Violations of users’ privacy, data protection.• Fraud and other cybercrimes.• Malicious attacks on the stability or security of systems on the Net• Employment of Internet ‘chat. rooms’ by paedophiles to contact young people.• Unwanted exposure to pornographic Web content.
III: Non-Internet Centric	Policy and practice anchored in bodies and jurisdictions not concerned primarily with Internet-related issues. Provides local and international policy contexts where developments in Internet infrastructure and use intersect with wider existing governance processes that shape more detailed Internet-related policies.	<ul style="list-style-type: none">• Political expression, censorship.• Copyright, intellectual property rights (IPR), trademarks.• Closing digital divides, meeting UN MDGs.• Human rights, cultural and linguistic diversity.• Transmitting content through telecommunications carriers.

There are many overlaps and much interaction between the three governance types. This growing intersection between Internet use and wider policy issues at global and local levels was crystallized by Martin Boyle of the UK Department of Trade and Industry: ‘Cyberspace can’t be divorced from everyday life’.

For instance, unwanted spam e-mail can raise serious concerns at all three levels in Table 1: the potential of some spam to disable specific Web sites affects the Type I Internet-centric level; Type II issues include the fraudulent solicitation of money through spam; and at the wider Type III non-Internet centric level, digital divides can be exacerbated because the extra costs and special high-tech resources required to deal with and prevent spam are unevenly distributed among different countries, regions and social groups. The names and numbers given to Internet entities, such as domain names used in Internet addresses, may seem to be a clear Type I Internet-centric issue to be managed by the Internet Corporation for Assigned Names and Numbers Internet (ICANN). But, the registration of a well-known trademark as a domain name with the intention of selling it back to the owner, called 'cybersquatting', has led to governance issues that are also the concern of international organizations—like the World Intellectual Property Organization (WIPO)—and national and international legislation and regulations which also cover more traditional trademark and related concerns.

Within each issue type, there is also growing multi-layered fragmentation. For example, Internet pioneer Steve Crocker, Chair of ICANN's Security and Stability Advisory Committee and Trustee of the Internet Society (ISOC), told the forum that protocol discussions could take place in one room when there were just four Internet nodes, in early Internet days over thirty years ago. Now, few hotels can accommodate the hundreds of working groups attending meetings of the Internet Engineering Task Force (IETF), a large international community of network designers, operators, vendors and researchers responsible for the evolution of the Internet's architecture.

Such scaling up has made it more complex to obtain and implement agreements at a technical level, while growth in the Internet's use and broader social impacts has led to the need for wider inputs to technically-oriented Internet governance issues. Though often criticized, ICANN has recognized this by establishing an At-Large Advisory Committee (ALAC) for the global individual Internet user community and the Governmental Advisory Committee (GAC) for governments. Yet, the relationship between users at large, governments and technical and business communities is still a process of continued re-definition of roles, rights and duties.

The way the cybersquatting issue was addressed demonstrates that it is possible to coordinate a coherent response to overcome fragmentation—provided the relevant governance bodies are aware of the problem and are willing to collaborate to achieve a mutually-acceptable approach. The solution in this case was through an international arbitration mechanism, the Uniform Dispute Resolution Policy (UDRP). Policies for this were developed by WIPO in consultation with relevant stakeholders and agreed by its Member States, but their implementation depends on ICANN (Jones 2005). Unease was also expressed about the UDRP process at the forum because implementation of the policy agreed by WIPO's Member States had to depend on ICANN, which is a not-for-profit corporation based on the laws of California. This indicates the complexity and political sensitivity involved in reaching such an accommodation.

A view that different governance models and agencies will be needed to address different governance issues was one of the clearest areas of common ground at the forum. This raises the crucial question of how these dispersed and diverse

governance process can be coordinated, particularly as the innovative nature of Internet technology and use keep extending and changing critical issues of all three Internet governance types, and the dynamics of the interplay between them.

Governance layers for the technical infrastructure

Different types of issues identified in Table 1 could be grouped into different subsets when viewed from particular viewpoints. For instance, a useful reference point in Forum discussions was a ‘thick–thin–thick’ layered model of Internet standards and protocols described by Crocker (see Table 2). The thin layer in the middle consists of a relatively few but vital Type I Internet-centric governance issues at the core of the Internet’s architecture and stability, which are covered by ICANN’s main responsibilities. The top layer includes the protocols underpinning the vast range of Internet applications that have numerous deep and diverse implications for wider Types II and III user and international policy issues. The lower layer relates to the telecommunications media carrying the Internet’s data. This is decoupled by the Internet’s design from the Internet’s infrastructure, and therefore can be depicted in Table 1 as dealing with non-Internet centric issues.

Table 2: Layers of Internet standards and protocols

Application protocols supporting the vast, ever-changing range of Internet applications. Of these, e-mail and a few other basic uses command most attention as they are what everyone sees, but there are also a few dozen vital protocols essential to smooth Internet operation (e.g. assigning a certain port when a new computer is connected). On top of these are many other protocols that continually emerge and die as they are debated in the hundred working groups of the IETF and other bodies, such as the World Wide Web Consortium (W3C), which is developing standards to support the Web.

Core infrastructure: routing of data packets; address assignment; domain name translation.

Telecommunications carrier protocols and standards. This includes the infrastructure that supports the movement of Internet data bits over wired and wireless media. It involves huge industries and rapid technological innovation, which has led to falling costs and an ever-expanding range of multimedia transmission options. The Internet Protocol (IP) standards supporting this layer have been impervious to this rapid change, allowing a smooth expansion in the range of applications and use of its continuously changing technologies.

Source: Summarized from forum comments by Steve Crocker

Maintaining the stability and security of the thin central layer is critical to avoiding a breakdown of Internet operations because it covers three essential capabilities: moving data packets as quickly as possible through the network; using the addresses associated with each packet and related routing mechanisms—such as Internet Exchange points and the logical assignment of IP-addresses by Regional Internet Registries (RIRs)—to guide and control the communication pathways taken by packets; and the Domain Name System (DNS) that translates between alphabetic and numerical versions of Internet addresses (e.g. those ending ‘.com’), via a hierarchical structure with ‘root servers’ at the top.

Crocker believes a disproportionate amount of governance attention has been given to the thin Internet-centric layer, which he said forms a relatively small part of what happens on the Internet and is the layer with the most mature governance structures, although they may be imperfect and still nascent. In contrast, he highlighted what he called the 'largely non-existent' governance mechanisms at the applications layer, even though this is where the most unpredictable changes that reverberate across the world are triggered. However, mention was made during the forum of some mature governance structures that have a role to play in addressing issues raised at the these wider user and policy governance levels. For instance, national legislation like the US CAN-SPAM Act of 2003 has led to prosecutions for sending spam and WIPO's Copyright Treaty and Performances and Phonograms Treaty include provisions relating to digital content. Yet, no good coordination mechanism exists between technical bodies—such as the IETF and W3C—and governments and users.

This paper focuses on the wider governance issues in the upper layer of Table 2, while highlighting the continuing significance of the core middle layer and acknowledging that an appropriate telecommunication infrastructure is also an essential foundation.

Key unresolved and emerging governance issues

A number of emerging and longer-term developments were flagged as being likely to require new approaches that cannot fit easily within existing Internet governance strategies. Crocker highlighted distributed denial of service (DDOS) as one of the most urgent of these. It occurs when a vast number of computers simultaneously send messages to a targeted Website to overwhelm its communication capacity and disrupt its services. An attack typically uses 'zombie' software infiltrated into numerous computers without their owners' knowledge, where they act as unwitting accomplices under the control of their creator. Some operational procedures exist to help overcome DDOS attacks, but Crocker said he knows of no clear technical or control mechanism or governance process to prevent them. Robert Shaw (2005:50), policy advisor to the International Telecommunication Union, sees an opportunity to establish more secure networks in emerging international Next Generation Network (NGN) standards. However, Scott Bradner of Harvard University believes the speed of innovation in optical fibre communications could have already outdated these standards. He therefore fears NGN could create unnecessary quality-of-service controls that reduce the reliability and manageability of high-performance networks.

New forms of Internet naming systems also pose new problems. For instance, multilingual internationalized domain names (IDNs) and the possible introduction of an 'author naming' system to help identify individual Internet users are other developments for which fresh governance approaches are likely to be needed.

Even though these issues appear to be 'Internet-centric', they are actually related to semi-political processes affecting wider user and social Type II and III issues, as their successful implementation relies on convincing end-users to adopt these naming systems. This is illustrated by the development of Digital Object Identifiers (DOI), a naming system that is increasingly being used by publishers and other multimedia content producers to allocate location-independent names to entities on the Internet, thus avoiding the need for detailed Web address that could change.

Norman Paskin (2005) of the International DOI Foundation notes that the DOI scheme currently operates mainly through proxy server translation to DNS-based Web addresses, though the underlying 'Handle' protocol is not DNS-based and offers significant additional functionality when deployed as a native protocol running on the Internet's TCP/IP standard.⁴ However, he argues that the IETF Request For Comments (RFC) review process saw the DNS element as a preferred technology rather than treating Handle as a complementary solution to naming entities on the network. He warns that the current dominance in Internet governance and funding of organizations reliant on DNS 'may be problematic in introducing complementary alternative naming mechanisms'. Others claim the Internet's openness allows DNS and DOI to coexist, with the DOI free to steer its own course.

Looking further into the future, David Clark of the Massachusetts Institute of Technology (MIT) foresaw an era of wireless sensor networks based on intelligent computer chips embedded in books, food tins, cars, along roads, in buildings and numerous other locations. Interconnecting the sensors could give individuals, groups and companies access to environmental information of a scale that was once available only to governments. It should also open unprecedented opportunities for continuous, automatic tracking of the location of individuals. New governance challenges raised by such embedded sensor networks could include a new degree of privacy intrusion through location-informing sensors and dealing with potentially hostile government attitudes to private infrastructures that gather weather, traffic or biohazard data in a way that was previously the preserve of public agencies.

Governance within and across national borders

Mary Rundle of Harvard's Berkman Center and Stanford's Center for Internet and Society described their joint project to spur transparency and public discourse in international Internet governance (Box 1).

Box 1: Net Dialogue for understanding international Internet governance

Net Dialogue is an online tool whose Website aims to serve as a model for how to bring international Internet governance into line with key elements of the WSIS (2003) Declaration of Principles, namely transparency and multistakeholder input. It seeks to aid understanding of how international organizations are dealing with international Internet governance issues, such as applicable jurisdiction and cross-border coordination. Topics on the site have been organized into eight initial groups, reflecting general areas of governance that regimes have dealt with throughout history: security; monetary authority; foreign commercial relations; property; infrastructure; jurisdiction; relations between private parties; and relations between person and state. It is a collaborative effort, growing according to inputs from interested stakeholders through its promotion of public dialogue. Users can easily navigate through any category to discover relevant governance institutions, processes and regulations. Additional issues can be added, while still maintaining a simple classification structure.

Source: www.netdialogue.org and *Net Dialogue* (2005)

⁴ IP is the protocol used to address and forward individual packets of data within the Internet. TCP (Transmission Control Protocol) helps to control the flow of packets between computers in the Internet in what is known as a TCP/IP network.

OII Director Bill Dutton identified two main dimensions of international governance relating to the Internet: collaboration in dealing with legal issues that cross national borders and the differential impact of use that may affect lesser developed countries through the entrenchment and extension of digital divides.⁵ There was much agreement at the forum that this is likely to require 'light touch' global and regional coordination and stewardship, primarily to fulfil enabling functions such as: avoiding the capture of key Internet resources by forces with narrow interests; promoting freedom of expression; and supporting capacity building in Internet infrastructure, use and governance.

A priority for international Internet governance identified at the forum is the preservation of the Internet's independence and openness from unwelcome state interference or domination by predatory corporations competing for control of this valuable global resource. To help achieve this, Katz (2005) would like international governance bodies to support open standards and principles of due process, consensus and openness in accreditation processes for the growing web of standards-setting bodies, which include trade associations, professional consortia, formal national organizations and globalized movements such as the Open Source Initiative (www.opensource.org).

The way digital divides can influence Internet governance was illustrated in a discussion on spam that suggested anti-spam tools might be lessening spam concerns in some countries. However, Dutton pointed out that such technical fixes are not evenly distributed worldwide. In developing countries with limited bandwidth, there is also still substantial use of slow dial-up Internet connections rather than always-on broadband, which raises user frustrations and costs caused by spam to a much higher level than in more technologically developed areas. Tom Vest of the Packet Clearing House pointed out that currently countries on the eastern coast of Africa do not even have the potential for broadband accessibility.

Governments in developing countries are often a major source of ICT knowhow, infrastructure development and capacity building, together with the private sector, universities and NGOs. They also generally view Internet access as a key to many areas of economic and social development, for example to help meet UN Millennium Development Goals. These factors were mentioned by those at the forum who feel it is unrealistic to expect governments to stand aside from active participation in Internet governance processes, as some would prefer. Given developing countries' financial, political, cultural and other constraints, building a better understanding between them and developed countries could be valuable in establishing realistic expectations about what can be achieved by developing countries in terms of Internet-related regulations such as freedom of speech, human rights and IPR.

Comments at the forum reflected more widely expressed concern about the US government's control over the 'root servers', a core infrastructure of the Internet, such as in being the ultimate policy authority for authorizing changes or modifications to the key 'root zone file'. Some argue that the provision of services based on these entries is already independent of the US government. The contention of others that fears about US government 'control' are more one of perception than reality was

⁵ A perspective from an emergent economy on digital divide issues was provided to the forum by González Mijares (2005).

countered by comments that—even if this is correct—perceptions must be treated as reality in international politics. The US government was generally felt to have been even-handed to date in instigating the Internet and supporting its openness and independence principles. However, as indicated below in a discussion relating to Table 5 in Section 3, there is a continuing political struggle over who controls and manages the root servers.⁶

The status of ICANN as a not-for-profit corporation was also the focus of some differences of opinion, discussed at the forum particularly in the context of the cybersquatting UDRP. For example, Shaw commented: ‘When sovereign states come together in a long consultation process and they reach a decision about what they want to do, they might then have to pass their proposal to a private corporation like ICANN, which decides it wants to go through its own processes and evaluate whether this is a good thing to do. This poses a fundamental question: Do sovereign states decide whether it should be implemented or someone else?’. Others emphasized that ICANN has proven to be an appropriate and resilient structure for governing the transnational operations of the Internet and that judgements about the status of such a governance organization should be based on its practical suitability for fulfilling its remit.

2. THE INTERNET’S DISTINCTIVE GOVERNANCE APPROACHES

How the Internet’s design influenced its governance evolution

Forum participants recognized that the Internet evolved with the support of highly flexible and innovative governance arrangements. Organizations that emerged from this unplanned process—such as current bodies like ICANN, IETF, W3C or the Internet Architecture Board (IAB)—are open, collaborative organisations.⁷ They resemble a fluid and loosely linked network of individuals and institutions under a common structural framework, rather than a hierarchical organization. At present, there is no single organization steering Internet-centric policies, but there are a few which control key technical resources and many that can exercise a limited level of control on a regional basis. According to Reagle (1999), this has meant ‘there have been few formal Internet institutions that real world governments could coerce because institutions of Internet policy are voluntary, decentralized, and non-coercive themselves! There are few choke points others can grab hold of and few mechanisms for delegating the coercive implementation of external policies.’

The forum emphasized that a key overall issue now facing Internet governance is how, as suggested by Vest (2005), such institutional arrangements that have so far successfully insulated this essential technical resource from political and commercial manipulation can be preserved and, where necessary, strengthened. However, the growing complexity of Internet-centric technologies and governance processes, and of their intertwining with wider social, economic and political policies and interests, is making it increasingly difficult to coordinate all the interrelated elements relevant to the overall picture of what is involved in the governance of Internet-related issues.

⁶ For an excellent overview of the politics of the Internet and the root servers, see Mueller (2002).

⁷ See: OECD (2005: 16-25) for a summary of the evolution of the Internet; Simonelis (2005) for an overview of major Internet governance bodies; and Shaw (2005) for a comparison of Internet governance approaches with those of earlier telecommunications innovations.

The Internet's technical design has been a significant influence in shaping the way it has been nurtured and managed, using governance processes that are very different to other communication media. For instance, the network of network that comprises the Internet runs above the infrastructure of highly-regulated telecommunications carriers (the bottom layer in Table 2). This has allowed rapid innovation without much regulatory interference (Cerf 2004), particularly by users exercising their communicative power 'at the edges of the Net'. One of numerous examples of this flowering is Skype's voice-over-IP (VoIP) telephony service, which gained 100 million users in just two years (www.skype.com).

An example of the governance implications of an Internet design choice is its 'end-to-end' (e2e) capability, which allows users anywhere in the world to communicate with each other provided they are interconnected through networks that conform to basic Internet protocols. This allows all types of multimedia data to flow through the Internet, compared for example to the way telephone lines carry only voice or analogue broadcast channels transmit only radio or television. Another difference from more traditional media is that the Internet imposes no constraints on the uses to which the information flowing through it are put, or how users interconnect and interact with other parts of the network.

In these ways, intelligence and control is decentralized and transferred to users, who can use their new communicative power to reconfigure access to people, information, services and other technologies (Dutton 2004a). Jonathan Zittrain, Co-Director of the Berkman Center, cited two examples of the astonishing collaborative creativity sparked at the edges of the Net: Wikipedia (www.wikipedia.com), a collective encyclopaedia editable by anybody at any time, which has converged into entries that have become far more useful than originally seemed possible for such a venture; and eBay (www.ebay.com), where anyone can put almost anything up for online auction. Skype is another example.

Such design foundations have assisted Internet-centric governance organizations to navigate through, and steer, the astonishing growth of the Internet. Nevertheless, as highlighted at the forum, there is growing concern about whether they can still manage effectively even technical core resources of the Internet, let alone the wider implications of their application and use. For instance, the way in which the e2e design enables the Internet to be largely independent of geographical constraints raises urgent international policy questions about national sovereignty, legal jurisdiction, the management of economic resources and human rights issues such as control over political expression and access to diverse cultural and linguistic resources.⁸ The rapidly changing dynamics of these kinds of issues was illustrated by Shaw's (2005) highlighting of a shift in the 'global telecommunications epicentre' from North America and Western Europe to the Asia-Pacific region, which now has the largest share of Internet users after trailing far behind just a few years ago.

⁸ For example, Post and Johnson (1996) comment: 'Cyberspace does not merely weaken geographical boundaries, it obliterates them entirely (at least in cyberspace), because geographical location itself is both indeterminate and irrelevant for transactions on the Internet. (...) and the physical location of the constituency is unknown.'

Learning from the Internet's success

A flavour of early Internet days was captured by Crocker's discussion of his work at the University of California, Los Angeles, in helping to build the first node on the US Department of Defense's Arpanet, the precursor of the Internet. In addition to defining the original suite of protocols, he said that the teams he worked with had 'even more importantly defined the architecture for creating protocols'. This included starting the Network Working Group, which was eventually transformed into the IETF. Crocker also recalled: 'We wrote down our ideas with much trepidation because we didn't want anyone to mistakenly think our proposals were assertions of how things had to be. So we called them Requests for Comments'. This bottom-up, collaborative, consensus-seeking 'traditional' Internet governance style has proved to be resilient. However, Crocker acknowledged that these processes are becoming unwieldy as the Internet grows and the 'design space closes'.

Internet design principles have stood the test of time even more successfully. Clark, another forum participant who was an Internet pioneer, recently explained to an OII-MIT Workshop that the Internet architecture he had helped to design is crucially 'optimized for change and to be open to unknown applications'.⁹ The successful expansion of the Internet while accommodating many unexpected and often dramatic innovations in technologies and applications is a testament to the success of this design foundation.

The community involved in these developments, coming largely from technical and academic research backgrounds, shared a commitment to maintain the openness, stability and independence of the technology as a shared resource for the benefit of all. This commitment is still seen by many as the cornerstone of good governance of the Internet as its uses have diversified and impacts have escalated. The continuing relevance of early Internet approaches confirms a comment by Pablo Hinojosa, Vice Chair, ICANN GAC: 'Much can be learnt from reading detailed ICANN by-laws as the engineers who developed them were doing very avant-garde political science'.

Many fear that pressure for new forms of global Internet governance, driven largely by wider user and social concerns, could lead to additional structural layers and over-restrictive regulation that constrain the Internet's vibrant collaborative creativity and continuing growth. As noted by Pindar Wong, an ISOC Trustee and former ICANN Board member: 'If we define what we mean by Internet governance today, we may accidentally define what it is not tomorrow.' A major reason for such caution is the success to date of the Internet's original values (e.g. openness) and governance processes (e.g. transparent multi-stakeholder collaboration).

Identifying appropriate Internet governance principles

The continuing relevance of the Internet's historical design and governance legacy was reflected in frequent citing at the forum of many specific 'good Internet governance principles'. For instance, Pindar drew on his experience in helping to develop key Internet organizations in the Asia Pacific region to summarize an overall aim of Internet governance: 'There were inevitable winners and losers for the specific

⁹ See www.oii.ox.ac.uk/collaboration/?rq=specialevents/20050415 for more on the OII-MIT workshop 'New Approaches to Research on the Social Implications of Emerging Technologies'.

approach chosen, but we all pulled together when we recognized that we would all ultimately get a better result if we were all committed to common principles.’ Main examples of more specific principles are summarized in Table 3, which shows the relationship between early Internet approaches and those likely to be required in the future to address wider user, social and economic issues. It also illustrates how some early Internet concepts can take on substantive new dimension in wider governance contexts, as illustrated by one of the Internet governance axioms articulated by Kenneth Cukier (2005a: 4) of the *Economist*: ‘The open network is akin to an open society: a matter of human freedom’. The principles outlined in Table 3 offer broad guidelines for policy makers rather than a prescription for curing all Internet governance problems, as indicated by the numerous unresolved and hotly-debated issues raised at the forum.

Table 3: Internet design and good governance principles

<i>Principle</i>	<i>Internet design</i>	<i>Internet-centric governance</i>	<i>Wider governance aspects</i>
Optimized for adaptation to unpredictable change	Minimal core architecture to accommodate application and technological innovations.	No harm to core architecture, principles. Agile institutions for timely responses to user and ICT changes.	Light regulatory touch that does not threaten Internet growth. Timely responses to social, economic, cultural and technical changes.
Independent	No central control or dominant communication gatekeeper.	Devolved, self-governing, bottom-up decision making, accountable to Internet community; no dominant stakeholder.	No dominant stakeholder. Support for user autonomy and creative, cultural, linguistic and applications diversity.
Open	Public availability of core Internet standards and protocols. Application and content independent.	Pluralistic, transparent collaborative processes with multiple public and private stakeholders. Open entry into Internet-related markets.	Transparent multi-stakeholder processes. Wide Internet access at equitable costs. Human capacity building. Open society concepts such as freedom of speech.
End-to-end interoperability	Unrestricted transfer of data packets from sender to receiver. Content, application, user, technology independent.	Protection of the e2e principle globally. Avoidance of technical or regulatory interoperability barriers.	Prioritizing the e2e principle in international Internet governance, while acknowledging national rights and responsibilities.
Subsidiarity: decisions at the most appropriate, efficient level	‘Shared ownership’ of core architecture by Internet community as a whole.	Efficient coordination of decentralized collaborative processes.	Multiple models for different issues. Efficient global coordination to avoid fragmentation of governance mosaic.
Operationally pragmatic	Stable, secure, efficient operation of core architecture.	Focus on what works in sustaining integrity and performance of core architecture.	No threat to sustainable Internet operations. Governance with the support of the governed.

3. UNDERSTANDING MULTI-STAKEHOLDER PROCESSES

Seeking balanced governance

Zittrain depicted the increasing entwining of cyberspace and everyday life in terms of a move in Internet development, use and governance 'from informality to formality, from backwater to mainstream and from collaborative to the competitive or the mercenary in the management of the collective reality on the Internet'. This momentum is creating continuing pressures to rethink governance mechanisms to manage implications of the Internet's widening range of use, including the need to respond to growing pressures from many stakeholders for a say in policy decisions related to the three types of governance issues identified in Table 1.

These pressures are coming from diverse and often conflicting viewpoints, such as: governments seeking to safeguard or subjugate their citizens; enterprises wanting to dominate or more fairly compete in Internet markets; users seeking benefits or protection from certain Internet applications; and experts striving to maintain the integrity of the architecture or undermine it maliciously. Such conflicting views make Internet governance an inherently political process as it seeks to create consensus among multiple stakeholder with different perceptions and interests. Urs Gasser of the Berkman Center suggested this is possible if policy makers emphasize that governance, like law, has enabling functions in addition to constraining roles.

Cukier's (2005b) summary report on the forum articulated a key consensus view among participants: 'Internet governance, like all political questions, involves achieving the right balance; finding the golden mean. As discussions unfold over time, there has been a marked move to the middle, and extreme positions have softened.' He identifies a number of dimensions where striking the right balance is essential, such as between the elements shown in Box 2.

Box 2: Areas of Internet governance where a fair balance is needed

- Public sector and private sector (stakeholders)
- Control and flexibility (political approach)
- Stability and experimentation (technical innovation)
- Centralization and decentralization (network design; governance approach)
- Top-down and bottom-up (procedures)
- Formal and informal (processes)
- Closed versus open (communications architecture; political institutions)
- Legal restrictions and permissive, laissez-faire (rules)
- Political inclusion and technical competence (values and influence)

Source: Cukier (2005b). www.oii.ox.ac.uk/collaboration/?rq=specialevents/20050505

Addressing inherent tensions

In addition to the tensions between good governance principles summarized in Table 3, as cyberspace and the real world intertwine there is likely to be many conflicts—as well as shared aims—between government, commercial, community and individual stakeholders. Such tensions are the main challenges to achieving a balanced approach in multi-stakeholder Internet governance process, as illustrated in Table 4. These examples indicate why even agreeing a broad set of good governance principles, which could be a useful exercise in its own right, is unlikely to avoid the need to understand and address the difficult realities created by such tensions.

Table 4: Tensions arising from governance principles and competing interests

<i>Type</i>	<i>Description</i>	<i>Examples/potential solutions</i>
Democracy–speed	Efforts to make Internet governance ever more democratic, accountable and transparent could counteract the need for timely responses to rapid ICT and Internet change.	Once, a few experts could decide on Internet standards and implement them quickly. Now, a hundred IETF working groups and thousands of experts are involved. Difficulties in implementing change that challenges substantial user and ICT industry investments are shown by delays in introducing the latest Internet version, IPv6 (Dutton 2004b).
Privacy–trust	An open design enables the user creativity that gives special value to the Internet. But it has also undermined cybertrust by allowing malicious intrusions. User protection mechanisms could stifle innovation and threaten personal privacy.	Eddan Katz of Yale University argued that increased user identification as a protection mechanism should be accompanied by strong limitations on linking user identity with other sources of information. Crocker suggested a compromise: limiting the amount of identification required for different activities to allow a proportionate response, depending on the type of threat.
Subsidiarity–fragmentation	Fragmentation between experts and agencies could result from devolved decision making by those closest to an issue, leading to inefficient coordination and oversight and threats to national sovereignty.	The UDRP process for cybersquatting formulated by WIPO and implemented by ICANN illustrates how a governance process can be agreed despite fragmentation of responsibilities (Jones 2005). The growing number of IETF Working Groups indicates increasing fragmentation at the Type 1 Internet-centric level.
Consensus–competition	Multi-stakeholder, multi-institutional processes can create tensions between actors with different goals as they compete and cooperate to achieve their own aims while negotiating a consensus on wider aims.	Bradner highlighted tensions arising from business models of the telecom carriers that seek profits from content running on their networks. Lucinda Jones of WIPO pointed to benefits derived from shared goals, such as content providers' desire to make content available securely over expanded networks to reach more consumers.
Commons–commerce	The original concept of an openly accessible Internet 'global information commons' is challenged by growing commercialization of content in the open Internet marketplace.	Protecting and charging for content has become more common as the Internet's value as a global resource has grown. However, new forms of 'permissive licensing' are emerging where authors and creators make their works more openly available while maintaining some ownership and control (Uhlir 2005: 60–1).

Wong pinpointed a characteristic dilemma reflecting such tensions: ‘We are working together to keep the Internet providing value for everyone who connects to it because we believe it is for everyone. But that openness is also the source of many problems.’ WGIG member Don MacLean (2005: 31) elaborated on this two-edged Internet characteristic: ‘As well as putting power in the hands of users whose only desire is to communicate, to learn, or to manage transactions more efficiently, we have seen that the Internet puts power in the hands of those whose intent is to invade privacy, to cause mischief, to deceive and to steal. As well as creating opportunities for individual users and groups to create content, develop services, and exercise fundamental freedoms, the Internet creates opportunities to monopolize markets, control access to information, and deny basic human rights. As well as enriching the comparatively well-to-do people who have easy and affordable access, the Internet further impoverishes and disadvantages those who do not.’

Underlying dynamics of multi-stakeholder decision making in multiple arenas

Dutton (2005) has defined a framework to help understand the processes underlying the tensions illustrated in Table 4. This is based on the concept of an ‘ecology of games’, where a ‘game’ is defined an arena of competition and cooperation structured by a set of rules and assumptions about how to act to achieve a particular set of objectives (Dutton 2004a).¹⁰ Internet governance can then be seen to be the outcome of a variety of choices made by many different players involved in separate but interdependent governance games. This indicates that no single set of actors actually seeks to control governance as such, but that each player pursues more focused goals in collaboration or competition with other actors, such as avoiding spam or trying to develop a market for registering names and numbers. A few such games are illustrated in Table 5.

Table 5. Selected games and players shaping Internet governance

<i>Type</i>	<i>Game</i>	<i>Main players</i>	<i>Goals and objectives</i>
I: Internet centric	Transnational jurisdictional ‘turf struggles’	Governments, regional entities (e.g. European Union), governance agencies (e.g. ICANN, ITU, UN, WIPO, WGIG), experts (e.g. Jon Postel)	National and other actors participate in governance bodies to gain or retain, limit or expand control over Internet resources, such as over the root server.
	Names and numbers	Individual experts, ICANN, Registries, Internet Service Providers (ISPs), users	Obtain, sell and allocate domain names, etc. to identify sites, servers, users.
	Standards	Standards-setting bodies, IETF, W3C	Establish and propagate Internet standards.
II: Internet- user centric	Consumer protection	Consumers, consumer groups, suppliers, regulators, spammers, telemarketers	Legislators, regulators respond to competing and complementary views and interests.
	Privacy and	Governments, citizens,	Prevent or seek disclosure

¹⁰ The term ‘game’ is used here only in this sense and should not be seen as trivializing an arena by suggesting it is like a sporting or entertainment game.

	data protection	regulators, private firms, lawyers, journalists, civil liberties activists	of personal information depending on negotiated or imposed criteria.
III: Non-Internet centric	Copyright, digital rights management	Legislators and regulators, content providers, media and telecom suppliers, services offering online access to content, ICT vendors	Consumers seek low-cost online access to content. Creators, suppliers try to capitalize on their assets. Content owners, suppliers, users, legislators negotiate access and rights terms.
	Freedom of expression	Political and religious activists, writers, artists, media rights advocates, news media, bloggers, governments, censors	Individuals, groups, organizations aim to facilitate or constrain the expression and exchange of certain viewpoints.
	Digital divides	Governments, NGOs, local activists, special-interest groups, local communities, investors	Players seek to close social, economic and other divides with the help of ICT-related infrastructure, use and human capacity building.

Source: Adapted from Table 2 in Dutton (2005: 9-10)

The impact of real-world political issues in Internet governance is illustrated by the ‘turf struggles’ relating to the root servers. The highest-level ‘A-Root’ server is the ultimate point of control on the Net, so who exercises most influence over it, and under what terms, matters as much in the real world as it does in cyberspace. From the outset, the US Government was the ultimate policy authority for the root zone servers. However, root-server administration was initially performed by one man: Jon Postel, an Internet pioneer, who was largely personally responsible for adding new top-level domain names (e.g. ‘.net’ or ‘.uk’). Many saw the creation of ICANN as an opportunity to ‘internationalize’ control over the A-Root, but this has happened only in a limited way. Other nations, such as Brazil, India, China and some European countries, have become increasingly concerned about this.¹¹ On 30 June 2005, the US government announced that it intended to ‘maintain its historic role in authorizing changes or modifications to the authoritative root zone file’.¹² The outcomes of this transnational jurisdictional turf struggle will have substantive real world impacts in terms of the bargaining power between nations, NGOs and civil society groups.

The growing popularity of peer-to-peer (p2p) networks, like Skype and music downloading services, also illustrates the complexity and rapidly-changing nature of many Internet governance ‘games’. These networks can bypass traditional hierarchically-oriented governance processes because they allow the exchange of information directly between the computers of individual users rather than being routed through a centralized service. The importance of this development is indicated by a US Supreme Court ruling on 27 June 2005 that the providers of software designed to enable such file-sharing of copyrighted works may be held liable for the copyright infringement that takes place using their software. The case

¹¹ For example, see www.icannwatch.org/articles/05/06/13/036210.shtml for more on Brazil’s Internet governance proposal.

¹² See www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm for details.

was brought by MGM and a consortium of content providers against p2p suppliers such as Grokster.¹³ The innovative culture at the edges of the Net from which p2p networks emerged could stimulate new developments that find ways around legislation, such as being harder to detect and punish. This has been the pattern in the copyright/digital-rights 'game' when previous attempts have been made to limit p2p services.¹⁴

4. PROMISING FUTURE INTERNET GOVERNANCE APPROACHES

The above analysis shows that not only is the Internet a package of many technologies across different layers, but that Internet governance is also not one process but several. It indicates that no single governance model will fit all contexts and that Internet governance should broadly remain a fluid and non-hierarchical network of many agencies and individuals using cooperating and competing governance models. Boyle argued for a pragmatic approach to dealing with wider policy issues through the adaptation of existing governance structures and better coordination between them, rather than by creating new mechanisms and rules specifically tuned to Internet dimensions: 'When unpleasant things like paedophilia that are governed by national and other laws in real life also happen in cyberspace, these laws need to be rethought to apply in this new global arena. But it would not be ideal to try to rewrite existing laws specifically for Internet governance.'

A key future aim from this perspective would be to adapt and scale-up governance approaches that have worked particularly well with Internet-centric issues to become appropriate for the ever-expanding range of wider user and social implications. This would be compatible with the introduction of new 'light touch' and agile coordination processes at a global level, but not with the establishment of new governance structures that would centralize decision making or create potentially cumbersome and innovation-stifling new arrangements.

Identifying the 'right home' for emerging Internet governance issues

A key Internet governance coordination issues was highlighted in the forum discussion on potential future governance issues, such as the social and political implications of embedded sensor networks. This indicated a need to alert existing governance agencies and affected stakeholders to developments on the horizon so that appropriate 'homes' can be found among the many organizations and stakeholders with a potential interest. The development of the UDRP to address cybersquatting shows that it is possible for an accommodation to be found for a new issue affecting many existing governance domains, although contention about the private status of ICANN illustrates the complex and politically-sensitive negotiations that need to be navigated when there are competing interests and viewpoints.

Hidden complexities can unfold even in cases where at first sight the 'right home' seems clear. For instance, WIPO has taken a lead in many Internet-related intellectual property activities in the areas for which it has clear responsibility, such as IPR, copyright and patents (Jones 2005), for which national and regional

¹³ See www.copyright.gov/docs/mgm for more on this ruling.

¹⁴ See www.theregister.co.uk/2005/06/29/after_grokster for a report on possible responses from Internet innovators.

legislation and regulation have a strong role within particular jurisdictions. However, the ease of reproduction and distribution and other special characteristic of digital content is challenging traditional approaches in these areas. This opens the door to many new potential stakeholders promoting their own governance structures and approaches, for example the open-source movement (see Table 4 and Katz 2005).

Another example is the 'whois' utility, which was designed to be a useful way of searching an Internet registry database to help get in touch with an appropriate contact if a problem arises with a domain name. Although this is clearly in ICANN's domain, David Maher (2005) of the Public Internet Registry believes this facility could violate privacy laws in some countries. Crocker is also concerned that there has been no clear home for the coordination of governance efforts to build systems with better in-built security defences, rather than just reacting to violations of security. He sees a step towards such an arrangement in recent moves by the Department of Homeland Security in the US to draw together agencies concerned with achieving this. In Europe, similar efforts are underway, for example through the European Network and Information Security Agency (www.enisa.eu.int).

At the global level, difficulties in coordinating the activities of different agencies and stakeholders can lead to long delays in achieving successful take-up, even of agreed Internet-centric regulations or standards like IPv6 or a more secure Internet naming system based on extensions to the DNS security (DNSsec) mechanism. The introduction of necessary technical upgrades to core Internet capabilities has generally slowed down as the Internet has become bigger and more diverse, with strong and growing user and supplier interests in preserving past standards to protect their substantial investments in existing ICT-based systems.

The borderless nature of cyberspace poses challenges to national sovereignty and legal jurisdiction that create particular difficulty in identifying appropriate homes for user and non-Internet centric issues having international dimensions. For instance, jurisdiction for spam offences could lie in the country in which: the spam originates; related financial transactions take place; or the victim is located. Some countries have implemented their own anti-spam laws, such as CAN-SPAM in the US, supported by inter-country agreements to assist in their implementation. Another approach to this problem is the OECD's multi-stakeholder toolkit involving codes of practice for ISPs, commercial e-mailers and other key actors (MacLean 2005: 32).

However, national jurisdictions or cross-national agreements can be bypassed in global cyberspace, for instance by an entrepreneur choosing a country with lax gambling laws in which to start a new poker or horseracing service that can be accessed by users anywhere in the world. The difficulties and slowness of agreeing and implementing global activities across cyberspace is illustrated by the Council of Europe's Cybercrime convention, which took about six years to negotiate. Yet, almost four years after the convention was signed at the end of 2001, it has been ratified by only ten countries; these exclude major Member States, like the UK, France and Germany, and non-Member signatories such as the US and Japan.¹⁵

¹⁵ As on 20 June 2005 (accessed at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>).

Compatible Internet governance routes to the future

The approach to Internet governance outlined in this paper has been formulated with an awareness of its compatibility with a number of other Internet governance proposals and ideas. For example, in his forum position paper, MacLean (2005: 31-3) develops the metaphor of the Internet as a 'network of networks' to articulate a vision of an Internet-related 'governance network of governance networks'. He sees this as involving the interaction between government, private sector and civil society networks operating at local, national, regional and global levels, each with its 'distinct ecology of goals, constituents, contents, internal structures, and underlying 'technologies' for accomplishing its purposes (i.e. laws, markets and communities respectively)'. The concept of Internet governance as a mosaic is complemented and enhanced by this view of its 'pieces' being part of network of networks where the 'big picture' itself is continuously changing through the dynamics of this ecology of governance games.

The European Internet Coregulation Network (EICN), of which the OII is a member, promotes another compatible approach. It acknowledges the limitation of state regulation alone in this field and promotes an appropriate sharing of responsibility between governments, private companies and civil society in building rules for Internet-related governance, through a process in which all stakeholders seek to achieve cooperation on rights and usage issues between them (e.g. see Falque-Pierrotin 2005; <http://network.foruminternet.org>).

The forum position paper by Thierry Vedel (2005) of the Centre for Political Research and National Center for Scientific Research in Paris identified four Internet governance modes that have been applied to Internet development and use in different parts of the mosaic: *community*, based on spontaneous solidarity and interdependence of interests between stakeholders sharing a set of values and identifying with similar norms; *market*, assuming dispersed competition between autonomous actors seeking to maximize individual advantage; *hierarchical* coordination of participants by a central authority that organizes a framework of social action to meet pre-defined end goals; and *associative*, using agreements and contracts entered into by participants who voluntarily form an association to define the rules by which relations between them and with third parties are organized. Different modes are likely to be best suited to different governance arenas.

Although it was acknowledged that analogies are rarely a perfect fit to a different context, other examples of governance mechanisms and institutions whose structure and approach could be applicable to the Internet governance mosaic were highlighted at the forum, including:

- *A framework convention on Internet governance.* Lee McKnight (2005) of Syracuse and Tufts University draws an analogy between global, multi-stakeholder Internet governance and the way climate change was dealt with in the 1980s through an international 'framework convention' that sought to provide a regime with a sound basis in international law that avoids spending too much time negotiating contentious details.
- *Subsidiarity within a global framework.* In air traffic control, the International Civil Aviation Organization coordinates the development of principles,

techniques and standards to promote safe international air navigation on a global basis. However, each air traffic control system is run by a national authority using agreed procedures for exchanging information between countries. Capacity building support is given to maintain standards in developing countries.

- *Efficient global coordination at operational levels.* Interpol facilitates international coordination of police activities in over 180 countries, prioritizing the exchange of timely, accurate, relevant and complete information.
- *Multi-agency coordination.* The World Health Organization (WHO) helped to resolve disputes over social objectives of pharmaceutical patents after negotiations in the World Trade Organization (WTO) and elsewhere had faltered. WHO helped to open up discussions by refocusing efforts towards the delivery of appropriate healthcare, while leaving detailed negotiations to take place in WTO, using a structure provided by WIPO.
- *An alternative to ICANN's private non-profit status.* The International Union for the Conservation of Nature (IUCN) is organized as an international organization based on Switzerland with a host-country agreement, but is not a Swiss corporation.

The authors' analysis showing the need for better coordination of multiple approaches to the governance of Internet-related activities indicates that these and other compatible approaches are worth further exploration in developing different solutions appropriate to different contexts.

5. CONCLUSION: CONNECTING THE PIECES OF THE INTERNET GOVERNANCE MOSAIC

The forum established much common ground in understanding and addressing governance issues relating to the Internet, such as the view that different governance models and agencies will be needed to address different governance issues. At the same time, discussions at the forum also illustrated the degree to which even common ground can be contested, as in unresolved debates about the significance of the Californian not-for-profit status of ICANN or in the lack of agreed definitions and norms to guide Internet governance efforts. This indicates that identifying and building on areas of consensus can increase the chances of success. However, there is also likely to be less risk of failure if areas of disagreement can be openly and constructively analyzed to develop realistic governance goals and the processes to achieve them.

Priority overall aims of Internet governance were agreed to be avoiding doing any harm to the Internet and preserving its openness, growth and innovative vitality. Improvements in specific areas were also identified, such as Internet security and privacy. These goals are most likely to be achieved by building on the Internet's style of fluid governance through open, adaptable and devolved bottom-up decision making by a loosely-linked network of individuals and institutions with efficient international coordination. The question then is not whether to establish a new organisation for Internet governance, but how to improve the existing structures,

networks and processes through better global arrangement that helps to identify and coordinate the 'bigger' picture by the emerging Internet governance mosaic.

This paper has emphasized the key themes of the forum as being the fragmented nature of emerging patterns of Internet governance and the pivotal importance of a coordination process that helps find appropriate governance homes for different issues. The key advantage of the way this paper has classified Internet governance issues into more detailed levels has been to illustrate that it is possible to avoid unmanageable fragmentation by decomposing issues into manageable chunks within a big picture framework that ties them together, which are helping to ensure key issues aren't neglected and a balance is maintained across the spectrum of Internet governance issues.

The authors believe an appropriate model for achieving this could be an independent advisory coordinating group or forum with knowledge of different aspects of Internet-related technologies and their wider policy implications. This would help to identify, alert and link relevant agencies to aspects of the bigger picture that may otherwise be missed or underplayed. It would focus on building linkages between different agencies and stakeholders—but leave the agencies and stakeholders closest to an issue to think through and arrange the most appropriate way of dealing with a specific issue.

Forum participants generally felt this coordination and 'finding a home' role would not be an appropriate task for any hierarchically-empowered agency that could use it as a strong political tool to reinforce its power base. However, such a forum appears to be an appropriate Internet governance role for the UN, given its work in seeking to encourage nations to work together in the interests of all. It would also take forward the UN's recognition of how the global political landscape is changing, for example as shown in the way the WSIS multi-stakeholder process demonstrates the UN's increasing emphasis on the role of the private sector and civil society in its deliberations. This should place the UN in an ideal position to facilitate the early identification of Internet governance problems and to make recommendations about who should address them. This role could also include an attempt to agree broadly-acceptable principles of good Internet governance.

REFERENCES

Cerf, V. (2004) Internet Governance.

http://global.mci.com/us/enterprise/insight/cerfs_up/issues/governance.xml

Cukier, K. (2005a) Slouching Towards Geneva: Ten Unappreciated Axioms of Internet Governance. In OII (2005), pp. 3-6.

Cukier, K. (2005b) The Oxford Consensus (Oxford: Oxford Internet Institute).

www.oii.ox.ac.uk/collaboration/?rq=specialevents/20050505

Dutton, W. H. (2004a) *Social Transformation in the Information Society* (Paris: UNESCO Publications for the WSIS).

Dutton, W. H. (2004b), Can the Internet Survive? Why Your Decisions Matter. In *Nominet.uk News*, December. www.nominetnews.org.uk/dec04/debate.php

Dutton, W. H. (2005) A New Framework for Taking Forward the Internet Governance Debate. In OII (2005), pp. 7-10.

Falque-Pierrotin, I. (2005) Policy Paper on the Internet Governance Addressed to the WGIG (Paris: Le Forum des Droits sur l'Internet), 15 June.
www.wgig.org/docs/ContributionJune-FDI.doc

González Mijares, J. (2005) Internet Governance: Perspectives from Mexico. In OII (2005), pp. 11-3.

Johnson, D. R. and Post, D. G. (1996) Law And Borders—The Rise of Law in Cyberspace. *Stanford Law Review* 48, 1367-402.
www.temple.edu/lawschool/dpost/Borders.html

Jones, L. (2005) Intellectual Property in the Information Society: The Role of WIPO. In OII (2005), pp. 15-22.

Katz, E. (2005) Accreditation for Open Standards-Setting Organizations. In OII (2005), pp. 23-4.

MacLean, D. (2005) Governing the Internet as Medium and Message, Model and Metaphor. In OII (2005), pp. 29-33.

Maher, D. (2005) How Should the WGIG Shape Policy and Practice on Internet Governance and Regulation? In OII (2005), pp. 34-7.

McKnight, L. W. (2005) Towards a Framework Convention on Internet Governance. In OII (2005), pp. 41-4.

Mueller M. L. (2002) *Ruling the Root: Internet Governance and the Taming of Cyberspace* Cambridge, MA: The MIT Press

Net Dialogue (2005) [HTTP://WWW.NETDIALOGUE.ORG](http://WWW.NETDIALOGUE.ORG): A Mechanism to Promote Transparency and Public Dialogue in International Net Governance (Cambridge, MA: Berkman Center for Internet and Society, Harvard Law School and Stanford, CA: Center for Internet and Society, Stanford Law School). www.netdialogue.org

OECD (2005), *OECD Input to the United Nations Working Group on Internet Governance (WGIG)* DSTI/ICCP(2005)4/Final (Paris: OECD Directorate for Science, Technology and Industry). www.oecd.org/dataoecd/34/9/34727842.pdf

OII (2005), *The Struggle Over Internet Governance: Searching for Common Ground. Position Papers* (Oxford: Oxford Internet Institute).
www.oii.ox.ac.uk/collaboration/?rq=specialevents/20050505

Paskin, N. (2005) Two Practical Examples of Issues in Internet Governance In OII (2005), pp. 45-8.

Reagle, J. (1999) Why the Internet is Good: Community Governance that Works Well. <http://www.cyber.law.harvard.edu/people/reagle/regulation-19990326.htm>

Shaw, R. (2005) Internet Governance in the Context of Historical and Future Perspectives of Telecommunications Technologies and Policies. In OII (2005), pp. 49-54.

Simonelis, A. (2005) A Concise Guide to the Major Internet Bodies. *Ubiquity* 6(5) 16-22 February. www.acm.org/ubiquity/issues6.html

Uhlir, P. F. (2005) Creating Global Commons for Public Information. In OII (2005), 58-62.

Vedel, T. (2005) The Struggle over Internet Governance: Searching for Common Ground. In OII (2005) pp. 63-7.

Vest, T. (2005) An Empirical Foundation for Normative Internet Policy. In OII (2005) pp. 68-70.

WSIS (2003), *Declaration of Principles*, WSIS-03/GENEVA/DOC/0004 (Paris: UNESCO and Geneva ITU). www.unesco.org/wsisis

APPENDIX I: FORUM PARTICIPANTS

Christian Ahlert, Research Officer, Oxford Internet Institute
Bernard Benhamou, Head of Mission on Internet Governance, French Government
Martin Boyle, International and European Policy, UK Department of Trade and Industry

* Scott Bradner, University Technology Security Officer, Harvard University
* David Clark, Senior Research Scientist, Massachusetts Institute of Technology
Steve Crocker, Chair, Security and Stability Advisory Committee, ICANN and Current ISOC Trustee

Kenneth Cukier, Technology Correspondent, *The Economist*

William Dee, European Commission

Nitin Desai, Chair, UN Working Group on Internet Governance

Bill Dutton, Director, Oxford Internet Institute

Urs Gasser, Research and Teaching Fellow, Berkman Center

Juan José González Mijares, Deputy Director General, Multilateral Economic Organizations, Mexican Ministry of Foreign Affairs

Pablo Hinojosa, Vice Chair, Government Advisory Committee, ICANN

Eric Johnson, Executive Director, Internews International

Lucinda Jones, Senior Legal Officer, Copyright and Related Rights Sector, WIPO

Eddan Katz, Executive Director, Yale Information Society Project

Markus Kummer, Executive Coordinator, Secretariat, WGIG

Don MacLean, Member WGIG

David Maher, Senior Vice President, Law and Policy, Public Internet Registry

Lee W. McKnight, Associate Professor, School of Information Studies, Syracuse University, Research Associate Professor of Computer Science, Tufts University and Co-founder, Internet Governance Project

Desiree Miloshevic, Policy Development Advisor, Afiliias, Board Trustee, Internet Society, Director-at-large, CPSR

John Palfrey, Executive Director, Berkman Centre

Norman Paskin, Director, International DOI Foundation

Malcolm Peltu, Editorial Consultant, Oxford Internet Institute

Karine Perset, Directorate for Science, Technology and Industry, Organization for Economic Cooperation and Development

Mary Rundle, Fellow, Harvard's Berkman Centre and Stanford's Center for Internet and Society

Robert Shaw, Internet Strategy and Policy Advisor, ITU

Sally Shipman, Telecommunications Policy Advisor, Office of International Communications and Information Policy, US Department of State

Emily Taylor, Legal Director, Nominet

Paul Uhler, Director, Office of International Scientific and Technical Information Programs, The National Academies

Thierry Vedel, Senior Research Fellow, Centre for Political Research and National Center for Scientific Research, Paris

Tom Vest, Research Program Manager, Packet Clearing House

Pindar Wong, Current ISOC Trustee, former Member of the ICANN Board

* Jonathan Zittrain, Faculty Co-Director, Berkman Center for Internet and Society

* *Participation from the Berkman Center via videoconference*

APPENDIX II: GLOSSARY

ALAC: At Large Advisory Committee (ICANN).

ARPA: Advanced Research Project Agency (US Department of Defense), sponsor of Arpanet, the precursor of the Internet; subsequently renamed DARPA.

CAN-SPAM: Controlling the Assault of Non-Solicited Pornography and Marketing, US Act of 2003 dealing with spam.

Cybersquatting: Registration of a well-known trademark as a domain name with the intention of selling it to the trademark owner.

DARPA: Defense Advanced Research Project Agency.

Denial of service: Attack on a Website or other computer or network service to disrupt the service provided by that system.

DDOS: Distributed Denial of Service.

DNS: Domain Name System, translates the commonly-used alphabetic version of a domain name into its numerical IP address.

Domain name: Unique IP address for each computer on the Internet (see DNS).

DOI: Digital Object Identifier.

EICN: European Internet Coregulation Network

ENISA: European Network and Information Security Agency

GAC: Governmental Advisory Committee (for ICANN).

IAB: Internet Architecture Board

ICANN: Internet Corporation for Assigned Names and Numbers Internet.

IDN: Internationalized Domain Name.

IETF: Internet Engineering Task Force.

IP: Internet Protocol.

Information commons: Conceptualization of the Internet as a shared public space offering equitable and often free access to information within it.

Internet Exchange Point: Allows direct p2p interconnection between independent or third-party Internet networks, such as those operated by ISPs.

ISP: Internet Service Provider.

ISOC: Internet Society, a professional society addressing Internet-related issues.

ITU: International Telecommunication Union.

Malware: Malicious content infiltrated onto computers, such as a virus sent via spam.

MDG: UN Millennium Development Goals

NGN: Next Generation Network.

P2p: Peer-to-peer.

Packet: Basic data unit sent via the Internet, headed by the receiver's address.

Phishing: A cybercrime using spam with an authentic appearance to tempt recipients into giving sensitive personal information, such as bank details.

Peer-to-peer: Sharing ICT resources through direct exchanges between computers rather than via a central system, for example in exchanging music downloads.

RFC: Request For Comments.

RIR: Regional Internet Registry.

Root server: A computer at the top of the control hierarchy for the DNS.

Root zone file: Contains pointers to the master (primary) and slave (secondary) servers for all Internet top-level domains.

Router: System used to establish the e2e path of a data packet.

Spam: Bulk unwanted e-mail that may contain malware.

TCP: Transmission Control Protocol

UDRP: Uniform Dispute Resolution Policy

URL: Uniform Resource Locator, specifying address of a Web page.

Virus: A self-propagating program that can damage the computer it infects.

W3C: World Wide Web Consortium, where Web standards are developed.

WGIG: Working Group on Internet Governance.

Whois: Internet utility for providing information from a domain name registry.

WSIS: World Summit on the Information Society.

Zombie: Software placed on a computer without the owner's knowledge, which can make it a slave to the zombie's controller.