International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:3, No:4, 2009

Internet Governance based on Multiple-Stakeholders: Opportunities, Issues and Developments

Martin Hans Knahl

***Abstract*—** The Internet is the global data communications infrastructure based on the interconnection of both public and private networks using protocols that implement Internetworking on a global scale. Hence the control of protocol and infrastructure development, resource allocation and network operation are crucial and interlinked aspects. Internet Governance is the hotly debated and contentious subject that refers to the global control and operation of key Internet infrastructure such as domain name servers and resources such as domain names. It is impossible to separate technical and political positions as they are interlinked. Furthermore the existence of a global market, transparency and competition impact upon Internet Governance and related topics such as network neutrality and security. Current trends and developments regarding Internet governance with a focus on the policy-making process, security and control have been observed to evaluate current and future implications on the Internet. The multi stakeholder approach to Internet Governance discussed in this paper presents a number of opportunities, issues and developments that will affect the future direction of the Internet. Internet operation, maintenance and advisory organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) or the Internet Governance Forum (IGF) are currently in the process of formulating policies for future Internet Governance. Given the controversial nature of the issues at stake and the current lack of agreement it is predicted that institutional as well as market governance will remain present for the network access and content.

***Keywords*—** Internet Governance, ICANN, Democracy, Security

I. Key issues in Internet Governance

"The Internet is the global data communications capability realized by the interconnection of public and private telecommunication networks using IP, TCP, and other protocols required to implement IP Internetworking on a global scale, such as DNS and packet routing protocols." [1]

"As we renew our schools and highways, we'll also renew our information superhighway. It is unacceptable that the United States ranks 15th in the world in broadband adoption. Here… every child should have the chance to get online, and they'll get that chance when I'm President – because that's how we'll strengthen America's competitiveness in the world." [2]

"[Internet] is the basis of a fair competitive market economy,… of democracy, by which a community should decide what to do. It is the basis of science, by which humankind should decide what is true. Let us protect the neutrality of the net." Tim Berners-Lee, Inventor of the World Wide Web [3]

Internet governance relates to the global decision making process and setting of policies with regards to the Internet. It is further concerned with the ongoing control and operation of the Internet and its core resources such as the root server system, assignment of domain names or allocation of IP addresses [4]). Today the technical operation of the Internet is relevant for the global economy and the Internet provides a global communications network. Thus economical, cultural, political and technological issues are interrelated and cannot be considered in isolation. Mathiason et al [5] distinguished 3 Internet Governance functions:

- Technical standardisation (e.g. decisions regarding the TCP/IP protocol implementation and functions)
- Resource Allocation and Assignment: Given the fact that in principle each host on the Internet requires a globally unique IP address and that 32 bits are reserved for IPv4 addresses in the protocol header, only a finite amount of IP addresses is available. The same issue applies to domain names and must be regulated on a worldwide basis.
- Public Policy: The conduct of people and organisation through policy formulation, policy enforcement and dispute resolution. This function relates to individuals and organisations involved in the design, implementation, operation or use of the systems employing the (public) Internet protocols.

The governance and control of the Internet also impact upon network neutrality, the fundamental principle to guarantee equal, transparent and universal non-discriminatory access to the Internet [3]). Furthermore Wireless Network Neutrality will determine the extent at which Internet based services will be available on mobile devices (e.g. mobile phones) and the pricing of such services. Currently wireless Internet is less prominent in the USA than other countries as carriers generally tightly control services that are available on mobile devices [6]. Ultimately the telecommunication industry's interest is to control the actual services that run over its infrastructure rather than merely providing "dumb pipes" to maximise its profits. The release of Apple's iPhone in June 2007 and Google's current work on the Android Operating System - a free and universal Operating System for mobile

Note: Martin Knahl is with the University of Applied Sciences Furtwangen, Robert-Gerwig-Platz 1, 78120 Furtwangen, Germany (phone: :+49 7723 920 2241; fax: +49-7723-920-11095; e-mail: knahl@hs-furtwangen.de).

devices - put a spotlight on the struggle that companies face when they try to create direct relationships with mobile consumers.

Whenever a system connects to the Internet it runs the risk of being compromised. Thus Internet security, the protection of a system integrity and the stored and generated data, is an Internet Governance issue that must be assess by Internet Governance policy and technical procedures. Internet Security is somewhat peripheral to normal communication, but further highlights the importance of the netizens perceived confidence and intrinsic security using systems that are part of the Internet. Hence Internet Security will remain high on the Internet Governance and technical agenda as cyber criminals can reap great benefits form the inherent insecurity and users are in danger of being compromised. Whenever decisions need to be made about how to police and enhance the security of the Internet the various stakeholders are required to work together. The differences in security and privacy legislation throughout the world and the different understanding of freedom versus control makes globally supported counteraction a challenging task. However, Mathiason suggests that *"there are the beginnings of an international agreement, however, that dealing with cybersecurity and crime is an international responsibility"* [5]. Other stakeholders such as the ITU agreed at the Plenipotentiary Conference of the International Telecommunication Union [7]) upon:

> *"a) the crucial importance of information and communication infrastructures and their applications to practically all forms of social and economic activity;*
> *b) …new threats from various sources have emerged that may have an impact on confidence and security in the use of ICTs by all Member States, Sector Members and other stakeholders… give rise to evergrowing security challenges across national borders for all countries…;*
> *c) …to protect these infrastructures… [through] international cooperation and coordination..."*

This study further identifies and outlines key Internet deployment and Internet Governance implications and distils current trends and developments with respect to Internet governance into the broader political and technical context. The study follows a transdisciplinary approach to address the socio-technical issues it describes. It considers different forms of governance to address the dynamic structure of the Internet. These can broadly be split into those that follow traditional (vertical) organisational forms and those that are collaborative and distributed in character (horizontal). The attempt to regard the Internet as a single, coherent unit that can be regarded in isolation does not reflect its infrastructure and the vested interests it serves. It can be argued that current Internet Governance lacks transparency and clear formalised procedures.

II. Internet Operation and Accessn

The network of networks that forms the Internet has grown from a small research network connecting a limited number of systems in the late 1960s to a universal communications platform based on the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite [8]). Thus the backbone system of the Internet represents a major Building Block of the global infrastructure. The current distribution of Internet capacity and geographic connections indicate a hierarchy that make certain cities (such as London or New York) *'nodal points with global control capability'* [9] resulting in information flows that are heavily concentrated in a handful of hub cities in Europe and the USA [10]. Choi further argues that *'this concentration of information ... flows reflects and influences the inequitable development of the world system'* [10]. This leads critics to regard the Internet as yet another infrastructure that serves the contemporary hierarchy of the world's regions and the prevailing economical and political systems.

Table 1: Internet Penetration Statistics from InternetworldStats, 2008

Country or Region	TOP 47 in Penetration	Rest of the World	World Total Users
Penetration (% Population)	68.7 %	13.2 %	21.9 %
Internet Users	717,788,781	745,843,580	1,463,632,361
Population (2008 Estimate)	1,044,977,592	5,631,142,696	6,676,120,288
Source and Date of latest Data	IWS - June/08	IWS - June/08	IWS - June/08

Frequent political interventions occurred to facilitate the provisioning of affordable Internet services and a fair market, e.g. in the UK where Oftel has intervened repeatedly to facilitate competitive market conditions [4]). The rapid growth of Internet services and the emergence of cheap and widely available technologies such as DSL have resulted in high Internet penetration rates in western countries. Furthermore most developing countries recognize the value of the Internet and aim to support its development. It has further been recognized as a technology to facilitate the development of the region (e.g. groups in Chile such as the Centre for Informational Rights of the University of Chile, www.cedi.uchile.cl, have recommended legislation to make access to the Internet a right alongside access to clean water and shelter). However, the regional penetration rates in the developing world remain relatively low (see statistics in **Fig. 1**). The difference becomes evident with a comparison between North and South America. The population estimate for South America in 2008 was 384,604,198 with 104,037,293 Internet users as of March 2008 (27.1 % Penetration Rate) and 12,377,823 Broadband Internet Connections as of September 2007 (~3.3% broadband penetration). On the other hand, the estimated population for Northern America in 2008 was 337,167,248 with 248,241,969 Internet users as of June 2008 (73.6% penetration rate), 72,313,133 Broadband connections as of September 2007 (~35% broadband penetration). In South America a few counries (Brazil, Argentina, and Chile) are the leaders in high-speed Internet access, accounting for 90 percent of all broadband subscribers in 2006 and forming the top markets for ADSL in the region [11]. Furthermore, despite the region's low Internet penetration, fixed line and mobile phone subscriptions continue to grow at an annual rate of 50 percent according to the World Bank Group in 2006. It can be observed that increased Internet availability have led to a surge in social networking and services such as Voice-over Internet Protocol (VoIP). Governments are further committed to invest in public Internet availability to facilitate inclusion [2] [11].

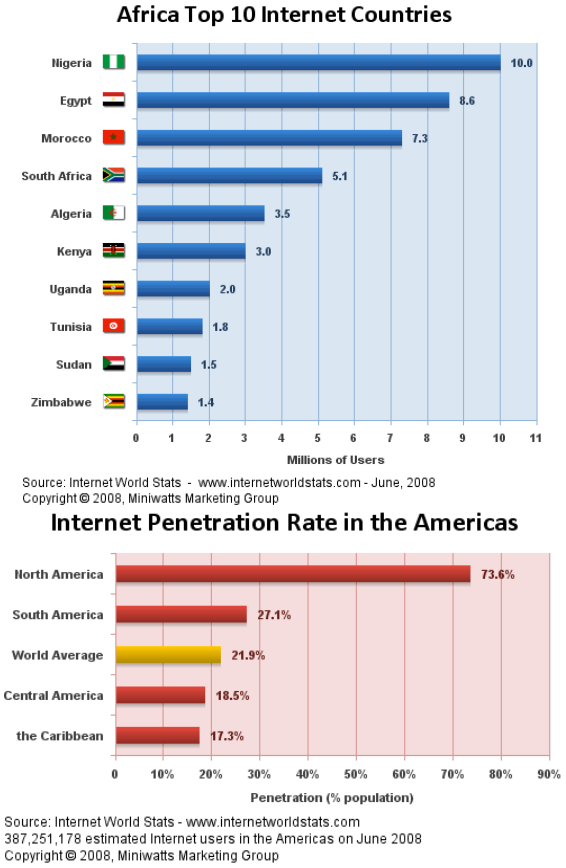

Fig. 1 Internet Penetration Rates in Developing Countries Internet Penetration Statistics from InternetworldStats, 2008

The global increase in Internet connectivity (e.g. based on "always-on" broadband connections) undoubtedly brings tremendous economic opportunity. However, software developers and *malware* authors have discovered great potential facilitated through vulnerable operating systems, Internet service and security software and inept Internet users [12]. Goth further argues that Internet violence facilitated through virus propagation, spam, click fraud, phishing, and other activities have boomed through botnets in recent year and that industry experts believe that the security threats will increase in the coming years [13]. As security threats increase typical users remain ignorant of what an expert might call "common-sense" approaches to avoid being compromised (or to keep systems "uninfected").

Botnets are commonly referred to as a collection of software robots, or bots, that run autonomously and automatically. It can refer to a network of computers using distributed computing software. However it is typically associated with malicious software. A Botnet thus constitute a collection of compromised computers (sometimes also referred to as Zombie computers) running software. The software is usually installed via worms, Trojan horses or backdoors under a common command-and-control infrastructure. The majority of these computers are running Microsoft Windows operating systems, but other operating systems can be affected. A number of botnets have been found on the Internet. Examples include a botnet discovered by the Dutch police with a reported number of 1.5 million nodes [14] and a 10,000-node botnet discovered and apparently dismantled by the Norwegian ISP Telenor [15]. To further counteract botnets international coordinated efforts to discover and remove botnets have also been initiated [16]. It is fraught with danger to estimate the size of the problem and this in itself generates insecurity. Some computer security experts believe that at least 10% of home PCs have been recruited into robot networks, or "botnets," under the control of criminals [17]. However other analysts, including Vint Cerf (one of the inventors of the Internet and now a top Google executive) was quoted at the World Economic Forum in February 2007 that botnets have become "pandemic" and that up to one quarter of all systems connected to the Internet may become part of a botnet [17] [18]. It is believed that the majority of botnets today are used to distribute spam. A spammer can use captured systems to transmit millions of messages simultaneously. As these messages are sent through the email systems of "ordinary" users may further increases resilience with regards to spam filters. The program installed by a botnet may further violate a system's hard disc and monitor its user's keystrokes to gather private data. The retrieved data is then distributed over the Internet to its master.

There are numerous examples of artists and activists through direct action by targeting or "attacking" the authority through software. An interesting example is the 'Floodnet' project. The group initially targeted Mexican and American government sites in 1998 through 'virtual sit-ins' or online civil acts of disobedience, and offered as a tool to enable protestors to effectively shut down web servers of target institutions, by flooding them with requests. The tactic follows a hacker sensibility in opening up existing security vulnerabilities in the system. As ever, power continues to produce its own vulnerability. The 'FloodNet' implementation is based on Java Applets that assists in the execution of virtual sit-ins. Targeted websites are automatically reloaded at high frequencies. It further enables users to post statements to a targeted site by transmitting them to the server's log files.

Analogue to botnets, the FloodNet program can only cause the desired effects when thousands of users are targeting the destination simultaneously [19]. In this situation, their browsers will automatically reload targeted website and to cause the desired effect (e.g. to cause an excessive amount of traffic on the server that other "genuine" users will not be able to access the website).

FloodNet is an example of conceptual net-art that further facilitates activist and artistic expression of the users [20], [21]. By the selection of phrases that are sent to non-existing URLs (e.g. using the expression "human_rights" to form the url "http://www.xxx.gb.mx/human_rights"), FloodNet effectively uploads messages to server error logs by intentionally asking for a non-existent url (i.e. causing the server to return messages like "!"# $%&'()!*+,%-*,.-"%/,-%, *! (+,server").,0! (+, (+,1-++234,$+,# $%5,!**1,+4'64'+,1'-74++, '48"4+*+,.-',web pages that do not exist. FloodNet's Java applet asks the targeted server for a directory (e.g. called "human rights"), but since that directory doesn't exist, the server will generate "error" messages and log file entries (thus

enabling users to 34$64,a message on that server). Other versions of the FloodNet have turned this notion to current events, such as during protests when the names of Zapatista farmers apparently killed by the Mexican Army in military attacks on an autonomous village (El Bosque), were used in the construction of "bad" urls. In an artistic sense, the activists regarded this as a way of acknowledging people who gave up their lives to defend their freedom [20], [21]. In a conceptual sense, the FloodNet aims to resemble a performance that illustrates a symbolic return of the dead to the servers of those regarded to be responsible for their murders.

One question is whether the Internet enables organizational change among traditional interest groups and political parties in a way that they are starting to resemble the looser network forms characteristic of social movements. It is further required to analyse the role of the Internet in new, conceptually intriguing citizen organizations such as FloodNet or MoveOn [22], [19]. ! "#$%&(proposes a concept of repertoires to argue that the Internet encourages organizational hybridity [23]. Chadwick further argues that "established interest groups and parties are experiencing processes of hybridization based on the selective transplantation and adaptation of digital network repertoires previously considered typical of social movements". Chadwick further envisages that "new organizational forms are emerging that exist only in hybrid form and that could not function in the ways that they do without the Internet and the complex spatial and temporal interactions it facilitates" [23]. These hybrid mobilization movements blend repertoires typically associated with established organizational types such as parties, interest groups, and social movements. Further, Chadwick suggest that fast repertoire switches, spatially between online and offline realms, and temporally within and between campaigns, are emerging characteristics of contemporary political mobilization.

According to different market surveys the size of the security software market is experiencing rapid growth, fuelled by 'compliance, data leakage and privacy issues, along with the need to tackle the fast evolving and sophisticated threat environment' [24]. According to latest figures from Gartner, sales of enterprise security products rose by nearly 20 per cent in 2007 and were worth $10.4bn. Symantec dominates the enterprise security market with over 26 per cent market share, followed by McAfee with over 11 percent. Latin America is the fastest growing region with over 40 percent sales growth. North America and Western Europe continued to lead the market with market shares of 47.5 per cent and 31.7 per cent respectively [24]. Post and Kagan further raise the question whether IT security controls are a burden or benefit [25]. According to the results of their study *"34% of the respondents perceived interference or delays caused by the computer security systems as a consequence of their current business environment… general employees perceive that increases (more onerous measures) in security policies and practices result in greater interference(s) with their job responsibilities."* Post and Kagan further suggest that users should be part of creating a security policy and suggest the testing of security restrictions on users to minimize task interference [25].

III. Towards a Multi-Stakeholder Approach

The theory of industrial organisation stresses the importance of strategic relationships between companies and organisations [26]. These relationships are further affected by the position they have in real or virtual space that allows them to interact. In the case of the Internet complex relationships can be identified: on the one hand it is required for network operators to be interconnected and on the other hand they typically compete on the same market. The resulting level of competition, particularly in highly regulated markets, is often favouring established organisations and disadvantaging organisations that are entering the market. This is mainly because existing and established key players (that were often state-monopolies in the past often in the case of telecommunications companies) own and control "essential facilities", enjoy "economies of scale" and are able to cross-subsidize selected services [27]. It is essential for regulation authorities to provide access-price mechanisms that allow ISPs to access another provider's infrastructure at competitive rates. A number of regulatory framework and policies have been defined (e.g. the 2002 New Interconnection Directive from the EU, ITU Recommendation D.50 or the APEC and CITEL frameworks in Latin America).

Criticism has recently been directed at Internet companies who do business in countries that violate human rights. Currently, in order to conduct business in countries such as China, companies must agree to the Chinese government's rule of self-censoring any information the government deems inappropriate. As a result it has been argued that some of these companies have violated the human rights of Chinese citizens to freely trade information based on the software systems running on the Internet. Justifications and excuses offered by these companies to absolve them of moral responsibility have been heavily scrutinized and it can be argued that both justifications and excuses offered are insufficient. Willfully abiding by unjust laws, albeit necessary to do business, should not trump moral actions that protect rights. It is an interesting case that Google's decision to do business with China was announced in the wake of its refusal to provide user information to the US Government case against child pornography [28]. The company's business priorities resulted in heavy criticism from the media and human rights organizations, accusing Google of abandoning its projected *'Don't Be Evil'* principles in pursuit of profit. However the reaction from the business community envisioned a high profit potential of the venture and the company's share price rose to record heights in the wake of the decision [28].

Another key issue, particularly for the developing world, remains high Internet access prices. According to D'Ignazio:

> *"On the one hand, asymmetric interconnection policies, and thus asymmetric fees, are very likely to be the right answer: large backbones engage in peering relationships, while they sign transit agreements with the smaller ones; thus small peripheral countries end up paying the whole interconnection cost. On the other hand, very often such high prices are caused by the endurance of local access monopolies and by the failure to liberalize the telecommunications market… Probably […] price discrimination in the upstream market and monopoly*

power in the downstream market both keep Internet access prices high, thus strengthening the digital divide". [27]

Given the relatively low level of inter-regional traffic in some regions (e.g. Latin America), it has been suggested that a particular focus should be the market for transit rates (e.g. to the U.S.) and further savings could be achieved if the countries would reach agreements to share circuit costs to connect to international network service providers [28]. Hence it is essential for developing countries to develop a competitive backbone infrastructure and to actively pursue national and international policy making of upstream and downstream markets to create competitive transit prices and peering agreements [27], [29].

Several assumptions prevail with respect to Internet governance: that Internet governance is distinct from governance of other media (e.g. television), that it is extending effectively through the whole Internet community or that it is market driven. However a number a key players and driving forces behind the evolution of the Internet put those assumptions in a different light and impact upon the current and future development. From a European perspective the European Union Framework Directive excludes key elements such as Internet addressing and naming from national bodies' responsibilities. This is opposed to other forms of international communications that are regulated by international and intra-governmental treaties [30]. Governance of the Internet is divided between different institutions. This current state of the art, the activities and authority of these, are highly contested and remain uncertain.

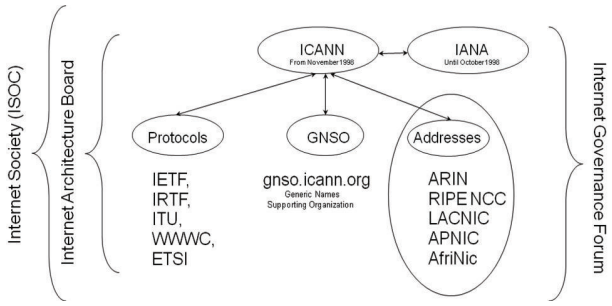

Fig. 2 IT Governance Stakeholder

The Internet Society (ISOC) is an international, non-profit organisation formed in 1992 to provide support for the Internet standards and development process. ISOC accomplishes this through maintaining and supporting other Internet administrative bodies such as Internet Architecture Board (IAB) or the Internet Engineering Task Force (IETF).

The Internet Engineering Task Force (IETF) develops and promotes Internet standards. It therefore cooperates closely with other standards setting organisations such as the W3C and ISO/IEC. It is primarily concerned with the standards of the TCP/IP and Internet protocol suite (i.e. OSI Layers 3-7), however it may further address issues that impact upon the deployment of TCP/IP protocols (e.g. Multiprotocol over ATM). It is an "open" standards organization without "formal" membership requirements. Thus the participants and leaders are volunteers. However the efforts of the contributing individuals are usually funded by their employers or sponsors. In the past the majority of contributors where academics or researchers whereas nowadays private enterprises are taking the lead in a number of core areas (e.g. the current chairperson is funded by the U.S. government's National Security Agency and VeriSign). The decision making process of the IETF is based on the notion of "rough consensus" as defined in RFC 2418 [31]:

"Working groups make decisions through a "rough consensus" process. IETF consensus does not require that all participants agree although this is, of course, preferred. In general, the dominant view of the working group shall prevail. (However, it must be noted that "dominance" is not to be determined on the basis of volume or persistence, but rather a more general sense of agreement.) Consensus can be determined by a show of hands, humming, or any other means on which the WG agrees (by rough consensus, of course). Note that 51% of the working group does not qualify as "rough consensus" and 99% is better than rough. It is up to the Chair to determine if rough consensus has been reached."

Rough consensus indicates the "sense of the group" or "dominant view" of a group concerning a matter that is under consideration as determined by its chairperson. Rough consensus is similar to other consensus models, such as Quaker-based consensus.

IV. Contemporary Issues and Propositions

ICANN controls the core Internet infrastructure (e.g. Root Server system) and resources (e.g. domain names, IP addresses) and ultimately guides the decision making process (e.g. on new top-level domain names). However it delegates the implementation and management of existing and new domains (e.g. to companies such as VeriSign). ICANN policies are hotly debated and often disputed by critics. An obvious example is the policy on new generic Top Level Domains (gTLD) to not use offensive words or ideas no words against "public policy or morality" for domain names. The problem is that this potentially results in massive Censorship and no protection for freedom of expression. However the policy is still in development, so the different stakeholders aim for to get involved to reform it. The fact that the U.S. government still exercises significant control over the core infrastructure of the Internet through the U. S. led oversight of ICANN continues to be challenged. ICANN's and the U. S. government's intention to date is to keep the existing model and to evolve rather than being replaced by a new model of communal state-led Internet governance. On the other hand the modelling and implementation of new structures for Internet governance is the clear intention of a large proportion of the international community [32], [33], [34].

Institutional cooperation is crucial for the development of the Internet, However the IETF and ICANN provide a revealing contrast of different organisational cultures. ICANN represents a move away from self-governance and is ideologically compromised given its close links to the U. S. government. To counter the implications of contemporary Internet Governance, the United Nations General Assembly sanctioned a proposal for a global summit on Information and Communication Technology in January 2002. The

International Telecommunications Union (ITU) took the lead in preparing the World Summit on the Information Society (WSIS) events, a pair of United Nations sponsored conferences about the information society that took place in Geneva (2003) and in Tunis (2005). The main aims were to bridge the global digital divide separating rich countries from poor countries by spreading access to the Internet in the developing world and to establish transparent, fair and ultimately democratic means to govern the Internet. Ultimately, the events were characterised by a lack of agreements on the key questions and no far reaching decision were made. However it established the 17 May as World Information Society Day and the Internet Governance Forum (IGF) as a multi-stakeholder forum to facilitate policy dialogue on issues of Internet governance (Marsden, 2008). The following excerpt from the IGF mandate illustrates the rather vague agenda [35].

"1. Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet;

2. Facilitate discourse… and discuss issues that do not fall within the scope of any existing body;

3. Interface with appropriate inter-governmental organizations and other institutions…

4. Facilitate the exchange of information and best practices….

5. Advise all stakeholders…

7. Identify emerging issues, bring them to the attention… where appropriate, make recommendations;

….

11. Help to find solutions to the issues arising from the use and misuse of the Internet…;

12. Publish its proceedings"

Thus the condensed mandate of the IGF is to provide a platform for discussions and recommendations to facilitate dialogue between different stakeholders. In that role, the IGF may "identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations" whilst it lacks any concrete decision-making authority [33], [36]. Hence the outcomes of the annual meetings (the last one took place in Hyderabad, India in December 2008) merely identify issues and propose suggestions to stakeholders such as ICANN. In the meantime, control of the Internet is likely to remain a highly charged political issue. US President Barack Obama recently announced an ambitious plan to build up the nation's Internet infrastructure as part of his proposed economic stimulus package and to provide universal, affordable high-speed Internet to spread knowledge, promote entrepreneurship and make the US more competitive [37]. It is interesting to note that the America, the world leader in a number of technical areas, now ranks 15th in the world in access to high-speed Internet connections.

A number of different norms and suggestions can further be isolated to isolate key proposals with respect to Internet governance [1,], [5], [34]:

- Preserve underlying technical model (to facilitate universal access, network neutrality);
- Commons (e.g. network core) must not be privatised; standards commons (e.g. IETF) must not over-regulate the market, should clarify policies and intermediaries (e.g. ISP) for security and privacy;
- Policy operators must break up and counteract monopolies and excessive market control, Deep Packet Inspection for Internet control and Mobile IP should be embedded in policies and legislation;
- Resource assignments and allocation must not be driven by policies and politics, revisit the assignment of gTLD, domain names, IP addresses etc.;
- Content of Internet communication should not be regulated through controls within the communication channel (i.e. Network Neutrality); Analogy with drug trafficking: address supply or demand rather than transportation;
- Multi-stakeholder governance should be legitimized, maintained and strengthened; establish the medium to long-term the role of IGF, ITU, ICANN etc.

The Internet is best understood as a network of networks with a multitude of loosely interconnected and layered entities as opposed to one closed medium or infrastructure. It has not (and as this research suggests cannot) have a single, unified governance organisation. It is a dynamic and evolving organism with constantly changing operational and governance requirements. Thus the necessity of different forms of governance must be acknowledged.

V. The Future of Internet Governance

The issues and challenges associated with Internet Governance reflect broader political structures in the context of globalisation which is giving rise to a new form of sovereignty that overcomes the model of the nation-state and its representational structures of government [38]. It can be argued that 'the new paradigm is both system and hierarchy' and demonstrates the structural logic of 'governance without government' [38]. Hence, the direct interference of governments can be seen to be entirely problematic. Given that the Internet is non territorial and that the Internet requires exclusive and coordinated resource assignments it can be argued that Internet standards create a global commons.

The need for new institutional reforms that reflect 'democratic' and 'rough consensus' processes that challenge the existing Internet Governance framework arises. Thus the OGF can be seen as a new model for reaching international consensus that forms the basis for international policies. Clearly there are a number of issues that require the multi-stakeholder approach such as climate change or the current financial crisis. Furthermore emergent forms of communication and social and professional networking are radically dissimilar to the ways in which relations have been organized to date. Emergent 'organized networks' are horizontal, collaborative and distributed in character offering a distinct social dynamic and transformational potential [39].

References

[1] Mueller, M. , Mathiason, M. , Klein, H. (2007).The Internet and Global Governance: Principles and Norms for a New Regime, Global Governance: A Review of Multilateralism and

International Organizations, Lynne Rienner Publishers, Volume 13, issue 2, April – June 2007: pp. 237-254.

[2] Obama, Barack (2008). President-elect Barack Obama lays out key parts of Economic Recovery Plan. Change.gov. 6 December 2008. Retrieved 27 January 2009 from http://change.gov/newsroom/entry/the_key_parts_of_the_jobs_plan/

[3] Google, 2007, A Guide to Net Neutrality for Google Users. Retrieved 13 July 2007, from http://www.google.com/help/netneutrality.html.

[4] Collins, R., 2006. Internet Governance in the UK. Media, Culture & Society. Vol. 28 (3): 337-358.

[5] Mathiason, John (2009). Internet Governance – The new frontier of global institutions. Routledge - Taylor & Francis Group. London and New York.

[6] Hernaez, Eric, 2007, Wall Street Journal on Wireless Network Neutrality, Circle ID, 15 June 2007. Retrieved 8 July 2007 from http://www.circleid.com/posts/wsj_on_wireless_network_neutrality/.

[7] ITU, Final Acts of the Plenipotentiary Conference . International Telecommunications Union (ITU) , Extracts: Resolution 130 (Rev. Antalya, 2006):Strengthening the role of ITU in building confidence and security in the use of information and communication technologies and Resoultion (Antalya, 2006): Study of definitions and terminology relating to building confidence and security in the use of information and communication technologie. Antalya, 2006.

[8] Forouzan, B., 2006. TCP/IP Protocol Suite. McGraw-Hill, International Edition.

[9] Sassen, S. , 2002, Locating cities on global circuits, Environment and Urbanization, Volume 14, No. 1 (2002): pp. 13-30.

[10] Choi, Junho H. et. al. , 2006, Comparing world city networks: a network analysis of Internet backbone and air transport intercity linkages, Global Networks, Volume 6, No. 1 (2006): pp. 81-99.

[11] Budde, Paul, 2006, Regional: Internet: The Americas – 2006, Communication Pty Ltd. , p. 27.

[12] Keizer, Gregg, 2005. Dutch Botnet Bigger Than Expected. TechWeb Technology News. Oktober 21, 2005.

[13] Leyden, John (2004). Telenor takes down 'massive' botnet. Enterprise Security. 9th September 2004.

[14] Leyden, John (2005). ISPs urged to throttle spam zombies: International clean-up campaign. The Register. 24th May 2005.

[15] Grizzard, Julian et al (2007). Peer-to-Peer Botnets: Overview and Case Study. HotBots '07 / 4th USENIX Symposium on Networked Systems Design & Implementation (NSDI '07). Cambridge (MA), 11-13 April 2007.

[16] Goth, G. (2007). Fast-Moving Zombies: Botnets Stay a Step Ahead of the Fixes. IEEE Internet Computing. Volume 11 (2): 7-9.

[17] Carr, Nicolas, 2007. Botnets - a hidden menace that threaten the future of the Internet. The Guardian. 5 April 2007.Christou, G., 2006. The Internet and Public-Private Governance in the European Union. Journal of Public Policy, Vol . 26, 1: 43-61.

[18] Weber, Tim, 2007. Criminals 'may overwhelm the web'. BBC News website. 25 January 2007.

[19] Beznosov, Konstantin and Beznosova, Olga (2007). On the imbalance of the security problem space and its expected consequences. Information Management & Computer Security. Emerald Group Publishing Limited. 2007, Volume: 15 (5):420 – 431.

[20] Lane, Jill (2003). Digital Zapatistas. TDR/The Drama Review. 2003 47:2 (T178): 129-144.

[21] Brett Stalbaum, 'The Zapatista Tactical FloodNet: A collabortive, activist and conceptual art work of the net', Retrieved 25 Jamuary 2008 from http://www.thing.net/~rdom/ecd/ZapTact.html

[22] Ford, Captain Christopher M. (2007). What Is Insurgency? Military review, US Department of Law. May / June 2007: 85-91.

[23] Chadwick, Andrew, 2007, Digital Network Repertoires and Organizational Hybridity. Political Communication, Volume 24, H. 3: 283–301.

[24] Thomson, Iain, 2008, 'Enterprise security software market booms'. Vnunet news. 18 June2008. Retrieved on 24 January 2009 from http://www.vnunet.com/vnunet/news/2219275/enterprise-software-market

[25] Post, Gerald V. , Kagan, Albert, 2007, Evaluating information security tradeoffs: Restricting access can interfere with user tasks. Elsevier / Computers & Security. No. 26, 2007: 229-237.

[26] Kranton, R. E. and Minehart, D. F. , 2001, A theory of buyer-seller networks. American Economic Review 91: 485–508.

[27] D'Ignazio, Alession and Giovanetti, Emanulele, 2006, FROM EXOGENOUS TO ENDOGENOUS ECONOMIC NETWORKS: INTERNET APPLICATIONS, Journal of Economic Surveys 20 (5), 757–796.

[28] O'Rourke, J. S. et al, 2007. Google in China: government censorship and corporate reputation. Journal of Business Strategy Emerald Group Publishing Limited. Volume 28, Number 3, 2007: 12-22.

[29] Ponce de Leon, Carlos Silva, 2005, Intra-regional Internet connectivity still an ongoing issue. Telecommunications Policy, Elsevier Ltd. , 29: 367-386.

[30] European Parliament and the Council of the European Union, 2002. Directive 2002/21/EC of 7 March 2002 on a common regulatory Framework for Electronic Communications Network and Services. OJL 108/33, 24 April.

[31] Bradner, S. (1998). IETF Working Group Guidelines and Procedures. Network Working Group / Request for Comments: 2418. September 1998

[32] Wray, R., 2005. EU says Internet could fall apart. The Guardian. 12 October 2005.

[33] Marsden, Christopher T., 2008. Beyond Europe: The Internet, Regulation, and Multistakeholder Governance - Representing the Consumer Interest? Journal of Consumer Policy. March 2008, Volume 31, Issue 1: 115-132.

[34] Mueller, Milton, 2009. Top Internet Governance Issues to Watch in 2009. Internet Governance Project Blog. 09 Jan 2009. Available under http://blog.Internetgovernance.org/blog/_archives/2009/1/9/4051237.html (27 Jamuary 2009)

[35] IGF, 2006. The Mandate of the IGF, Internet Governance Forum / Paragraph 72 of the WSIS Tunis Agenda. Available under http://www.intgovforum.org/mandate.htm (27 January 2009).

[36] Kumar, N. and Mowshowitz, A., "Increasing Internet access and freedoms with IGF participation," Technology and Society Magazine, IEEE , vol.27, no.2, pp.33-36, Summer 2008

[37] NYT, 2008. Editorial: Mr. Obama's Internet Agenda. New York Times. December 15, 2008

[38] Hardt, M. & Negri, A., 2000. Empire, Cambridge Mass.: Harvard University Press.

[39] Tapscott, Don and Williams, Anthony. 2007. Wikinomics: How Mass Collaboration Changes Everything. Atlantic Books.