INDIAN INSTITUTE OF MANAGEMENT
AHMEDABAD • INDIA

Research and Publications

A Model for Internet Governance and Implications for India

Rekha Jain

W.P. No. 2015-03-23
March 2015

INDIAN INSTITUTE OF MANAGEMENT
AHMEDABAD-380 015
INDIA

A Model for Internet Governance and Implications for India

Rekha Jain
Professor
Indian Institute of Management, Ahmedabad
e-mail: rekha@iimahd.ernet.in

Abstract

The rising role of Internet in economic growth and social aspects has brought the significance of Internet Governance to the forefront. New paradigms of Internet Governance recognize the contribution and role of governments, private organizations, civil society and other communities. The borderless and distributed architecture of the Internet substantially differentiates Internet Governance from traditional governance, challenging the established dominant role of nation-states in policy-making. Access, human rights, privacy and standards have become important Internet Governance issues. This has led to an increasing role of nation states.

Many developed countries recommend multi-stakeholder approach where nation-states are only one of the many stakeholders that include private sector and other communities. India's position on Internet Governance recommends a multi-lateral approach which is at variance with emerging scenario globally. This has isolated India and created a negative signal for investment in the ICT sector.

The approach to deal with emergent issues in Internet Governance requires flexibility, ability to incorporate new technologies and international developments. Studies of Internet Governance have not systematically addressed the issue of design of responsive organizations or national systems for effective governance. This paper contributes by addressing this lacuna by:

i) Developing a conceptual model for Internet Governance based on both the underlying architecture of the Internet and a proposed framework for evaluating the perceived legitimacy of the adopted processes and

ii) Combining these two frameworks, we develop the Multi-Tier Open Participation approach for its application to India. This approach not only strengthens domestic Internet Governance, but also increases India's role in regional and international processes.

The study recognizes that Internet Governance principles for India should be in consonance with its democratic ethos and openness and dovetail with the inherent characteristics of the Internet, namely, openness, dynamism, and innovation.

A Model for Internet Governance and Implications for India

Background

The role of Internet in economic growth and social aspects has increased the importance of Internet Governance. Internet Governance covers a wide gamut of resources and institutions at national, regional, and international levels. Internet resources comprise among others, Internet Protocol (IP) addresses, protocols, domain name systems (DNS) – often called Critical Internet Resources (CIR), telecommunication networks, cyber-laws. Examples of institutions are telecommunications authorities (national), Regional Internet Registries (regional), and Internet Corporation of Assigned Numbers and Names (ICANN). Owing to the distributed architecture of the Internet, wide variety of issues that span Internet Governance, and the high need for coordination and consequent adoption of universally accepted protocols, national and international, organizations play a role. Besides these, other actors include private organizations such as Internet Service Providers (ISPs), civil society organizations, academics, technical communities, and inter-governmental organisations. Therefore, paradigms of Internet Governance need to recognize the contributions and role of these actors.

Besides the aspect of managing CIR and the associated institutions, access, human rights, privacy, and standards have become important Internet Governance issues. Of late, driven by the surveillance by the US government that came to light consequent to Snowden revelations, there has been a renewed recognition in several parts of the world to review Internet Governance structures, especially the dominance of US and those aspects that deal with sovereignty, surveillance, cyber-security. Internet Governance issues are increasingly a proxy for a broader political struggle and for control of content.

Given the economic importance of Internet to the domestic economy as well as its influence on national security, privacy, and human rights, state actors and political leaders at the highest level want to influence Internet Governance. However, given that the range and scope of entities involved in Internet Governance is large, varied, and characterized by complex inter-relationships between them, governments face challenges in developing a framework for Internet Governance. Emergence of ever new forms (IGF, netMundial) and crafting responses add to the challenges. These are exacerbated in developing countries as they have weak institutional structure, lack of prior participation in existing Internet Governance bodies, dearth of technical know-how to participate in technical forums, inadequate human resource capability to design and manage new institutions and poor availability of finances to support development and sustain institutions. Often the strategic importance of participating in various Internet Governance process is absent in top level decision-makers.

The borderless and distributed architecture of the Internet has created virtual “properties” which may be located anywhere, and thus the jurisdictional framework they come under is open to interpretation. These aspects substantially differentiate Internet Governance from

the traditional governance, challenging traditional dominant role of nation-states in policy-making. Spaces for new participative forms of Internet Governance structures wherein nation-states are only one of the many stakeholders often referred to as the multi-stakeholder approach have emerged. These spaces have been largely dominated by developed countries, predominantly the USA and western countries. In contrast, the earlier "telecommunications" infrastructure deployments were largely within the governance domain of nation-states and coordinated under a UN umbrella through the International Telecommunication Union (ITU). This approach is referred to as multi-lateral and one that embeds state control in Internet Governance. Those supporting the multi-stake-holder approach consider that in relation to their view, multi-lateral approaches are not representative of stakeholder views, are dominated by governments and follow closed decision-making processes. On the other hand, those supporting the multi-lateral approach contend that only governments can and should make public policy as they are answerable to the citizens of the country. In contrast, the multi-stakeholder approaches are prone to capture by private enterprises for their own benefit and could lead to US dominance, and does not adequate represent people with lower resources such as those from developing countries. Thus, the debate on multi-lateral versus multi-stakeholder revolves around the question of what should be the roles and responsibilities of different stakeholders in various Internet Governance mechanisms. The challenge is to design appropriate mechanisms that are perceived to have the requisite legitimacy in their decision making processes. The issue of legitimacy is important in the context of Internet Governance as many of the entities involved are non-state actors, and need to establish processes by which state and other non-state actors accept the outcomes of the resultant outcomes of the process.

Internet Governance started as largely a coordination mechanism for IP based addresses and names. Later, it evolved to development of institutions and organizations for managing the Top Level Domains and Country Code Top Level Domains. With the growth of Internet and its role in the growth of economy, national security, democracy, the scope of Internet Governance today has grown to cover a wide range of institutions, both formal and informal and a multitude of stakeholders identified above.

Studies of Internet Governance have identified a lacuna in the field in that many areas such as telecommunications policy, information security economics and cyber-law that encompass aspects of Internet Governance, do not label themselves as studies of Internet Governance. On the other hand, studies of Internet Governance have largely been limited to the context of established institutions such as ICANN (Klein, 2002; Mueller, 1999; Reding, 2009), IGF (Christou and Simpson, 2011; Eeten and Meuller, 2012; Malcolm, 2008) RIR (Karrenberg, n.d.; Mueller, 2008). There are hardly any studies that have examined the role of networks and emergent forms that deal with Internet Governance. Thus, conceptualization of Internet Governance has been challenging due to the absence of formalized international regimes on one hand and the distributed nature of decision-making, cross border jurisdiction of Internet resources, low formalization in several key organizations, and a variety of organizational forms (Eeten and Meuller, 2012) that are involved in managing CIR.

Internet Governance in India

India's response to the changing Internet Governance structures, like that of many other developing countries, had been largely ad-hoc and has varied over time. India does not have a national strategic plan for including its concerns in various Internet Governance processes. Though the Indian government and members of Indian civil society have participated in various Internet Governance processes like WSIS, WCIT, Plenipot and other IGF meetings, these participations have not been a part of a national strategy. Various departments have participated independently and there has not been a coordinated approach.

Department of Electronics and Information Technology (DeitY) has been the nodal ministry responsible for interfacing with a variety of national, regional and international organizations. It has participated in various forums such as ICANN, RIR, etc., albeit in an ad-hoc way. While Internet Governance deals with a wide range of policy issues, Indian response from the Ministry of External Affairs (MEA) and Department of Telecommunications (DoT) has been limited to cyber-security and standards respectively. This was at the expense of various other important issues of access, interconnection, network neutrality etc. Both have been driven by a multi-lateral approach. Sometimes the views of different ministries have been in conflict.

Of late, segments of the Indian decision-makers have begun to realize the critical importance of strengthening India's domestic Internet Governance processes and playing a more dominant role in regional and international level, although such initiatives are sparse.

1 Introduction

1.1 Importance of Internet to India and Emerging Economies

Internet has become the vehicle of economic growth, social program delivery and governance in several countries. These aspects of Internet are of critical importance to India, as they are to many other emerging economies. Studies have shown a direct impact of Internet growth on Gross Domestic Product (GDP). For example, Internet users in India are growing at a Compound Annual Growth Rate (CAGR) of 20% with a base of nearly 239 million as of December 31, 2013. On an average 10% increase in Internet subscriber results in 1.08% of increase in output, adding nearly $17 billion in GDP incrementally[1].

In the context of poor physical infrastructure, a characteristic of many emerging economies, including India, the Internet provides a delivery platform for social services, thus overcoming some aspects of this gap. For example, mobile banking, using the Internet platform, gives access to banking services in rural areas where physical branches are scarce or unavailable. However, despite India being one of the countries with highest number of Internet users, the penetration remains low and a large number of citizens remain excluded. Further, the quality of Internet and Broadband experience is relatively poor.

Recognizing the importance of Internet in all aspects of national and international trade, economy, innovation, and security, Internet Governance is increasingly becoming centre stage both at domestic and international levels. It is expected that such issues will become centre stage as a part of global diplomacy in a similar vein as climate change (Christou and Simpson, 2011).

On the other hand, Internet Governance issues have become increasingly complex as the Internet is a fast evolving, complex, global resource. Cyber-space represents virtual properties that may be located anywhere and therefore what jurisdictional framework they come under is open to interpretation. In contrast, the telecom networks infrastructure over which it runs are governed by nation/state jurisdictions and their laws.

Internet infrastructure and its related tools, processes and organizations are now seen as critical resources. The instruments such as IP addresses used to govern the Internet are virtual and institutions governing these instruments have evolved, sometimes in a reactive mode, in a bottom up way rather than being designed top down. This is unlike other institutions/organizations managing global, virtual

[1]http://dartconsulting.co.in/DARTBlogs/growth-of-internet-users-in-india-and-impact-on-countrys-economy/, accessed on June 26, 2014

resources such as World Intellectual Property Organization (WIPO) for managing Intellectual property. Since Internet largely emerged from USA, management of Critical Internet Resources (CIR) largely remained within control of US and had representation mostly from the US.

Despite the importance of Internet to the economic growth and social development in emerging economies, they have played very little part in Internet Governance. This has been dominated by developed countries, predominantly the USA. Of late, driven by the surveillance by the US government that came to light consequent to Snowden revelations, there has been a renewed recognition in several parts of the world, including Europe, Russia, Brazil, India, China that there is a need to review Internet Governance, especially those aspects that deal with sovereignty, surveillance and cyber-security. In the case of emerging economies, issues related to greater access and better quality to and of Internet are significant issues of Internet Governance. This has led to greater international recognition of the increased role for other countries especially emerging ones in the future for Internet Governance. Therefore, institutional mechanisms for Internet Governance have become subject of international and national debates. Internet Governance regarding the technologies, the architecture, the infrastructure, services, applications and end-users is increasingly becoming a proxy for broader political struggles and for control of content

1.2 Internet Governance Framework

"Internet governance is the development and application of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet"[2]. Internet governance includes activities of a variety of stakeholders, including governments, private and civil society organizations. It is characterized by "shared global ownership without central control, innovations based on open and interoperable frameworks"[3].

We give below key organizations involved in Internet Governance:

- Internet Engineering Task Force (IETF)[4]: They work within the broad framework that the architecture should lead to smooth evolution and operation of Internet. Principles for the Internet have been developed, a group of engineers who are a part of a large, open, international community of network designers, researchers, operators, and vendors who are concerned about the smooth

[2]http://www.internetsociety.org/history-internet-governance, accessed on February 20, 2015
[3]http://www.internetsociety.org/sites/default/files/Internet%20Governance%20for%20Sustainable%20Human.pdf, accessed on June 27, 2014
[4]Excerpted from http://www.iab.org/wp-content/IAB-uploads/2011/03/081128-appel-IAB.pdf, accessed on February 14, 2015

evolution and operation of the Internet. The IETF is organized as a number of Working Groups, Area Directors, and the Internet Engineering Steering Group (IESG). The Internet Architecture Board provides oversight and adjudication against the decisions of the IESG. The Internet Society (ISOC) charters the IAB and IESG for these purposes.

- The Internet Research Task Force (IRTF)[5]: It focuses on longer term research issues related to the Internet while the IETF focuses on the shorter term issues of engineering and standards making. The IRTF is a composed of a number of focused and long-term Research Groups.

- The Internet Assigned Name Authority (IANA): It is responsible for global allocation and coordination of the DNS root, IP addressing and other IP resources such as protocol numbers, port numbers, ASN, and management information base identifiers.

- Internet Corporation for Assigned Names and Numbers (ICANN): It is a non-profit international organization, was identified as the entity for managing the IANA, and functions under agreement with the IETF. ICANN has an MOU with the US government. IANA became a department of ICANN. The ICANN carries out these functions through Regional Internet Registries (RIR) in each of the five regions: AfriNIC (*Africa*), APNIC (Asia-Pacific), ARIN (*Canada, USA, many Caribbean and North Atlantic islands*), LACNIC (*Latin America and parts of the Caribbean*), RIPE NCC *(Europe, parts of Asia and the Middle East*). ICANN's primary principles of operation have been to preserve the operational stability of the Internet. The new technologies including IPv6, Internationalized Domain names (IDN) and security enhancement of the DNS (DNSSEC) created new challenges for ICANN. For example, with the opening of the IPv6 address space, ICANN had to find mechanisms to address addition of a large number of gTLD in the DNS.

  ICANN has several Supporting Organizations and Advisory Committees[6]:

  - Address Supporting Organization (ASO)
  - At-Large Advisory Committee (ALAC)
  - Country Code Domain Name Supporting Organization (ccNSO)
  - Generic Names Supporting Organization (GNSO)
  - Governmental Advisory Committee (GAC)
  - Root Server System Advisory Committee (RSSAC)
  - Security and Stability Advisory Committee (SSAC)

[5]Excerpted from https://irtf.org/, accessed on February 17, 2015
[6]https://www.icann.org/resources/pages/welcome-2012-02-25-en, accessed on June 27, 2014

- Internet Society (ISOC): It has evolved as a legal entity to provide funding and secretarial support to the IETF and support activities that are important for the development of the Internet. It is an international, not-for-profit organization governed by its Board of Trustees. Its objective is to provide leadership in Internet related standards, education and policy. Its mission is "to promote the open development, evolution and use of the Internet for the benefit of all people throughout the world"[7]. It has more than 65,000 members, 145 chapters and more than 100 organization members.

  Its three key areas of focus are standards, public policy, and education. The IETF, IAB, IESG and the IRTF and IESG are the organizational homes for the standards activities. For fulfilling its public policy mandate, ISOC works with governments, national and international organizations, civil society, private sector and other entities. For the education component, it supports, coordinates and delivers training on topical Internet issues, and supports local and regional Internet bodies.

- World Wide Web Consortium (W3C): It is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards. W3C is not a legal entity in the traditional sense. It is administered via a joint agreement between four universities/institutions: MIT , ERCIM , Keio University, and BeiHang University, giving it an international flavour. The W3C works through Advisory Committees, Advisory Boards, chartered groups, populated by member representatives and invited experts, and which produce most of W3C's deliverables according to the steps of the W3C Process to work on standards, patents, web architecture standards.

1.3 Internet Governance – A New Governance Paradigm

"Internet Governance is the development and application of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet"[8]. It is characterised by "shared global ownership without central control, innovations based on open and interoperable frameworks"[9]. Governance covers aspects of institutions, their internal processes and their relationships with other institutions and constituencies. Such processes range from national and international laws to binding treaties and the softer aspects of informal

[7] http://www.internetsociety.org/who-we-are/mission, accessed on February 20, 2015
[8]Definition adopted from the report of the Working Group on Internet Governance. (Source: http://www.wgig.org/docs/WGIGREPORT.pdf, accessed on December 8, 2014)
[9]http://www.internetsociety.org/sites/default/files/Internet%20Governance%20for%20Sustainable%20Human.pdf, accessed on June 27, 2014

rules and uncoded practices such as moving forward based on 'rough consensus', as is practiced in IETF (Resnick, 2014).

The increasing importance of Internet to both businesses and states, has led to formal and informal discussions, and debates on the evolving nature of Internet Governance. The issues have ranged from the relative roles of the states, private sector and civil society to the extent of formalization of structures and decision-making processes for governance. This shift in orientation in Internet Governance from a largely informal mechanism that existed earlier to a demand for more well defined boundaries and specification of roles of various organizations has created space for global politics (Cooper, 2013).

Internet Governance includes activities of a variety of stakeholders, including governments, private and civil society organizations. Further, given the investments made by the private sector and their role in innovation and entrepreneurship in proliferating Internet, they have become stakeholders in the governance process. Additionally, since Internet and public policy issues of access, local language content, human rights, copyrights etc. have increasingly become integral to Internet Governance, civil society has become another important stakeholder. Debates regarding appropriate approach for Internet Governance have ranged from multi-stakeholder that aims to provide a platform for all stakeholders to participate in an open democratic way.

In contrast, several countries that are concerned by the dominant role of the USA and relatively lower role of established state institutions and organizations, call for established inter-governmental organizations set up under the UN for taking up an active role in Internet Governance. The approach has been called the multi-lateral approach. The debate in Internet Governance is at the broadest level about the multi-lateral model that "extend national sovereignty into cyber-space" and as involving "state-centric control of the Internet", while the other is multi-stakeholder that involves participation of civil society, Internet users and local internet businesses in a democratic bottom up manner.

Internet Governance now presents a mode of governance that increasingly is being characterized as "transnational and semi-privatized" (Chenou, 2011; Christou and Simpson, 2011) as states, private organizations such as Internet Service Providers (ISPs), civil society, academics, technical community, inter-governmental organization all participate in its governance. Some authors have called such governance as "embryonic transnational democracies", while others feel that "transnational elites" play a dominant role (Chenou, 2011; Christou and Simpson, 2011). The latter position finds sympathy with those in emerging economies as there is a perception that they do not play a significant role in this increasingly important emergent space.

1.4 Drivers for India to Play a More Dominant Role in Internet Governance

In the context above, it is important to analyse the developments in the field of Internet Governance and institutions and processes, both formal and informal, with a view to develop a rationale for how India should participate/create a role in this space.

There has been a growing concern about the influential roles played by the USA government and by the companies and civil society organizations based out of USA in driving the agenda for the public policy issues related to Internet Governance. Emerging economies have often felt and voiced their inability to influence substantive policy issues related to Internet Governance. At the global level, issues regarding incorporation of an emerging economy's perspective into the policy development process for Internet Governance, remain open and unresolved. For example, for the new gTLD program, there is under-representation of emerging economy applicants and there are relatively few accredited registrars. For example, in the growing Internet industry that relates to services such as domain names, IP addresses, registrars and exchanges, India's share is miniscule. A number of global companies have acquired gTLDs and built new business models around it. However, there has been little progress in India on this front.

There is a growing realization that Internet resources and processes that deal with allocation of Internet resources are often not transparent and show little understanding from an emerging economy perspective. For example, the high cost of ASN is a deterrent for many emerging economy's citizens and organizations to participate in the Internet economy.

There is little representation in policy development bodies in the Internet Governance space mentioned above. For example Stakeholders from emerging regions often struggle to be effective within ICANN. Moreover, concern about emerging economies' challenges and interests has not always been widely shared across the private sector community[10]. Mechanism to address these and similar issues such as the IGF that have emerged are not effective. IGF is a discussion forum with no decision making powers.

In order to leverage the Internet industry and Internet for its economic and social growth, India needs to have a national strategy for its future role on Internet Governance and bring visibility to its efforts. For example, Brazil has taken an initiative to bring Internet Governance and public policy issues from its perspective

[10]www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions, accessed on October 20, 2014

(including that of other emerging economies) to the global stage through highly publicized NETmundial[11]. Just prior to this event, the Brazilian Senate unanimously passed a bill guaranteeing online privacy on an equal access to the Internet for their citizens. This signalled a national eagerness to participate in Internet Governance.

With respect to the above, it is necessary that India should formulate strategies, governance principles, structures and processes that it should adopt in order to play a dominate role in Internet Governance.

In international forums, the Indian government has largely taken the position that Internet should be governed under the existing multi-lateral system under the UN, an approach that is labelled as "multi-lateral" (ML). We need to examine if this approach is appropriate given the current functions and architecture of the Internet and its future growth potential for India.

[11]http://icannwiki.com/NETmundial, accessed on October 20, 2014

2 Scope of Study and Methodology

2.1 Scope of the Study

The present study examines the issue of 'Internet Governance and Options for India'. This is done in the context of existing Internet Governance structures and processes and other ecosystems. Specific suggestions regarding the approach, strategy, organizational structures, and process at the national level are presented. Specifically, the study:

i) Develops an approach for conceptualizing Internet Governance based on both the underlying architecture of the Internet and a framework for evaluating the perceived legitimacy of the adopted approach, and

ii) Contextualizes the approach for its application to India for strengthening domestic Internet Governance while also increasing its participation and contribution to regional and international Internet Governance processes.

The Internet Governance principles that emerge for India should synergize the Indian democratic ethos and openness with the inherent characteristics of the Internet, namely, openness, dynamism, and innovation.

2.2 Methodology

The study is based on primary and secondary data. For primary research, we contacted key individuals, civil society groups and the government functionaries and government ministries and departments on relevant issues. Two key events that helped us to gather a broad perspective as well as helped us to contact key people in this area were:

1. The Asia Pacific Regional Internet Governance Forum, Delhi, India 2014
2. The Internet Governance Forum, Istanbul, Turkey 2014

3 Developments in Internet Governance

3.1 Emergence of Working Group on Internet Governance and Internet Governance Forum

Given the dominant position of US government in Internet Governance and location of critical infrastructure such as root name servers in USA, Europe and Japan, there were suggestions in the international forum, that individual governments or multi-lateral organizations such as International Telecommunication Union or the United Nations should have a significant role in Internet Governance. However, there was wide support domestically for the USA to retain control over the one centralized resource of Internet that was both "unilateral and centred in the US" (Mueller, 2010, pg 75).

The Tunis Agenda

The World Summit on Information Society (WSIS) had its first round in Geneva in 2003 and second round in Tunis in 2005. The Geneva round established principles and a plan of action with eleven action lines (C1 to C11) for achieving an information society based on shared knowledge that is accessible to all. The Tunis Agenda, released at the conclusion of WSIS, recognized the importance of multi-stakeholder dialogue in Internet Governance. The Tunis Agenda articulated[12]

> *"We reaffirm that the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect, it is recognized that policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues." (§ 35)*
>
> *"We recognize that all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the Internet. We also recognize the need for development of public policy in consultation with all stakeholders." (§ 68)*

The Tunis Agenda called for "the creation of a new forum for multi-stakeholder policy dialogue called the Internet Governance Forum". The same Agenda also recognized the need for enhanced cooperation[13] between governments in international public policy issues pertaining to the Internet. Effectively, the Tunis

[12]http://www.itu.int/wsis/docs2/tunis/off/6rev1.html, accessed on February 20, 2015
[13]Enhanced Cooperation is a term borrowed from European Union to reflect advanced integration or cooperation between a limited number of states.

Agenda created two tracks: IGF and process of Enhanced Cooperation. However, there is a view that there has been convergence in the scope of these tracks[14].

Leading up to the Tunis Agenda, the Working Group on Internet Governance (WGIG) was set up after the Geneva round of 2003 to resolve the issues regarding the relative roles of governments and international organizations in Internet Governance. Incidentally, WGIG did not have representation from ITU and other international organizations, although it did have representation from ICANN and Internet Society (ISOC). While the US and EU, among others, were in favour of private sector led ICANN, emerging economies wanted representation from governments and international organizations. The Tunis Agenda endorsed the multi-stakeholder arrangements for Internet Governance, which signified that ICANN was unlikely to come under an inter-governmental body.

The Tunis Agenda while recognizing the authority of governments to define public policy for the Internet, also endorsed the multi-stakeholder approach. It identified that public policy issues were the sovereign rights of governments, technical and economic matters were areas where private sector had an important role to play and community issues was a domain where civil society could lead. It envisaged that inter-governmental organizations should play facilitating role in the coordination of Internet-related public policy issues.

However, by separately categorizing various actors along the functional aspects of governance, and by explicitly limiting their respective roles, the Tunis outcomes failed to recognize the linkages between public policy and technical and operational issues.

In 2006, the UN Secretary-General established an Advisory Group (now known as the Multi-stakeholder Advisory Group, or MAG), and a Secretariat, as the main institutional bodies of the IGF. MAG has members from international governments, the commercial private sector, and public civil society, including academic and technical communities. While the IGF was successfully instituted in 2006, no progress has been made on any enhanced multi-lateral cooperation for public policy-making.

The IGF is often criticised for being avenue for policy dialogue where no constructive policy-making takes place. In response to these criticisms, efforts have been undertaken to improve the nature and adoption of outputs from the IGF. These improvements have emerged from the recommendations of the Working Group on Improvements to IGF headed by United Nations´ Commission on Science and

[14]http://unctad.org/meetings/en/Presentation/cstd18may2012_p04_EN.pdf, accessed on June 27, 2014

Technology for Development (UN CSTD). Efforts at constructive outputs have also emerged in the form of the Best Practices Forum in IGF 2014[15].

A Working Group on Enhanced Cooperation, constituted under the UN CSTD, was asked to prepare a report in 2013-2014 to suggest a way forward for enhanced cooperation. The WG on Enhanced Cooperation (WGEC) was driven by demands of a "multilateral, transparent, democratic" mechanism for Internet Governance[16]. The Working Group concluded its work without any agreement on the nature of enhanced cooperation. Many in this process rejected the fixing of the roles and responsibilities by the Tunis Agenda and suggest that all stakeholders should participate at an equal footing in public policy making, as they currently do in most existing Internet Governance mechanisms. These actors reject the notion that public policy is the exclusive domain of the states. This approach captures the beliefs of those in favour of an equal footing based multi-stakeholder Internet Governance mechanism.

This interpretation of enhanced cooperation wherein only governments are involved in policy-making is understood as multi-lateral. The International Telecommunications Union (ITU) is often cited as an example of a multi-lateral organization.

3.2 Changes in ICANN

Historically, IANA was managed by the Information Sciences Institute at the University of Southern California under a contract with the US Department of Defence. Network Solutions Incorporated (NSI) had signed an agreement with the Network Science Foundation (NSF) to manage the system of registering names and to maintain the .net, .com and .org domains. Effectively, NSI, in consultation with IANA, was responsible for root zone management.

Owing to the exponential growth of the Internet during and subsequent to 1990s, DNS management became more complex, and under pressure from businesses and foreign governments[17], US government decided to privatize the IANA functions. This was done with the objective of enabling competition and fostering global participation in Internet management. The US government decided that a not-for-profit organization with a global and functionally representative board would be the blueprint for achieving the above objectives.

[15]http://www.internetcollaboration.org/wp-content/uploads/sites/12/2014/08/TC-BP-MS-Mechanisms-Clean.pdf, accessed on October 23, 2014
[16]http://unctad.org/meetings/en/Presentation/cstd18may2012_p04_EN.pdf, accessed on June 27, 2014
[17]https://www.icann.org/en/system/files/files/report-20feb14-en.pdf, accessed on June 26, 2014

In 2000, ICANN and National Telecommunications and Information Administration (NTIA), an agency of the Department of Commerce (DOC), US Government, entered into a sole source contract for ICANN to perform the IANA technical functions. This contract has been renewed several times. The current contract extension runs until September 2015, with the DOC having unilateral option to extend it through September 2017 and further until September 2019[18].

Handing over of IANA functions to ICANN and the decision-making processes of ICANN have often been criticized as being non-transparent. NTIA's oversight led to it being not considered a neutral governing body[19]. This organizational structure and processes related to generic TLDs, country code domains, the proposed increase for domain registration so that ICANN could have a larger budget have also been areas of controversy.

The governing Memorandum of Understanding (MOU) was replaced with the "Affirmation of Commitments" (AOC) which gave the framework for the relationship between the US government and ICANN. DOC confirmed its commitment towards a multi-stakeholder, private sector led bottom-up policy led development model for DNS technical coordination"[20]. The AOC signed in 2009 and the IANA contract signed in 2012 co-exist. The contract between the US government and ICANN is in force, despite the stated intent of both parties that the AOC govern the technical management of the DNS[21].

Although US government had stated its intention to have private involvement in the IANA, the DOC's unilateral involvement has continued. In March 2014, the NTIA announced that it planned to end its contract with ICANN for the IANA functions and turn the oversight to a global, multi-stakeholder process by September 2015. The NTIA was also clear that new model could not replace its own role with a government-led or an inter-governmental organization. ICANN has constituted a "coordination group"[22] to steer this transition[23].

3.3 Brazilian Initiatives

The Brazilian Internet Steering Committee (CGI.br), created by an inter-ministerial ordinance in 1995, later amended by the Presidential decree in 2003 is the apex body for "coordinating and integrating all Internet service initiatives in Brazil as well as for promoting technical quality, innovation and dissemination of the available services" (www.cgi.br). CGI.br has 21 members, nine from the federal government,

[18]https://www.icann.org/en/system/files/files/report-20feb14-en.pdf, accessed on June 26, 2014
[19]http://en.wikipedia.org/wiki/Internet_governance, accessed on June 26, 2014
[20]ibid
[21]https://www.icann.org/en/system/files/files/report-20feb14-en.pdf, accessed on June 26, 2014
[22]https://www.icann.org/resources/pages/process-next-steps-2014-06-06-en, accessed on June 30, 2014
[23]https://www.icann.org/en/system/files/files/report-20feb14-en.pdf, accessed on June 26, 2014

four from the corporate sector, four from civil society, three from the technical and scientific community and an Internet expert. Its responsibilities are detailed in 'Annexure 1 – CGI.br Roles and Responsibilities'.

In a reaction to the Snowden Revelations of systematic USA surveillance of sovereign functionaries in various countries, including Brazil, the Brazilian President, put forth a proposal to the 68th UN General Assembly to tackle such practices. She also proposed a discussion on the global civil framework for Internet Governance and use and measures to ensure protection of data on the Internet. Working with the German Chancellor, Angela Markel, they submitted a draft resolution on the right to privacy in the digital age. This was passed by consensus.

In order to provide momentum for having greater involvement of different countries in Internet Governance, the Internet Steering Group in Brazil and /1 Net, a forum that gathers international entities of various stakeholders involved in Internet Governance, organized the Global Multi-stakeholder Meeting on the Future of Internet Governance, on April 23-24, 2014. The objectives of this meeting were to develop:

> *"a) Internet Governance principles, and*
> *b) Roadmap for the future evolution of the Internet Governance ecosystem*
>
> *"The meeting will aim to produce universal internet principles and an institutional framework for multi-stakeholder Internet governance. The framework will include a roadmap to evolve and globalize current institutions, and new mechanisms to address the emerging internet governance topics"*[24].

The meeting was hosted by the High Level Multi-stakeholder Committee (HLMC) composed of Ministerial representatives from 12 countries: Argentina, Brazil, France, Ghana, Germany, India, Indonesia, South Africa, South Korea, Tunisia, Turkey, and USA, and 12 non-state actors from the private sector, civil society, technical/academic community and two from inter-governmental organizations (ITU, and the UN Department of Social and Economic Affairs) (Varon, 2014).

The meeting produced a non-binding statement in favour of multi-stakeholder Internet Governance processes while endorsing the fixing of roles and responsibilities by the Tunis Agenda. The statement also called for increased priority and advancement of discussions on enhanced cooperation. The final resolution stated that the IANA transition should be completed by September 2015.

[24]http://www.internetgovernance.org/2013/11/19/booting-up-brazil/, accessed on December 11, 2014

3.4 ITU Plenipot 2010 and WCIT 2012

Given the convergence of telecommunications and the Internet, attempts have been made by ITU, a multi-lateral organization, to bring certain aspects of Internet Governance within its domain – including aspects of numbering resources, lawful interception, cyber-security amongst other public policy issues through its Plenipot in 2010 and the International Telecommunications Regulations (ITR) at the WCIT 2012.

In ITU Plenipot 2010, pursuant to WSIS 2003 and WSIS 2005, the ITU adopted resolutions 102, 130, 133 and 140. The key aspects of these were for ITU:

- (Resolution 102) to find "Means for greater collaboration and coordination between ITU and Relevant organizations involved in the development of IP-based networks and the future internet, through cooperation agreements, as appropriate, in order to increase the role of ITU in Internet Governance so as to ensure maximum benefits to the global community". For this, "the ITU Telecommunication Standardization Sector (ITU-T) would contribute its expertise, and liaise and coordinate on the management of Internet domain names and addresses and other Internet resources within the mandate of ITU, such as IPv6, ENUM and IDNs, as well as any other related technological developments and issues"[25], and collaborate on issues concerning member states ccTLDs.

- (Resolution 130 and 133): to enhance "cooperation on cyber-security and combating spam", and Internationalized Internet domain names respectively to provide support and a collaborative framework for capacity building and strengthening resource base for addressing issues such as cyber-crime, internationalized IDNs especially in response to the needs of emerging economies, invited member states "to consider joining appropriate competent international and regional initiatives for enhancing national legislative frameworks relevant to the security of information and communication network"[26] and "to take an active part in all international discussions and initiatives on the development and deployment of internationalized Internet domain names, including the initiatives of relevant languages groups, and to submit written contributions to ITU-T in order to help implement this resolution"[27].

[25]Excerpted from www.itu.int/en/action/internet/Documents/Resolution_101_pp14.pdf, accessed on February 20, 2015
[26]Excerpted from http://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20130.pdf, accessed on February 20, 2015
[27]Excerpted from http://www.itu.int/en/action/internet/Documents/Resolution_133_pp14.pdf, accessed on February 20, 2015

- (Resolution 140)[28]: to review the progress made on WSIS 2003 and 2005.

In WCIT 12, the move by ITU to bring Internet Governance mechanisms within the realm of the ITU was met with resistance from the groups espousing multi-stakeholder approach. Sustained campaigns by this group during WCIT-12 prevented the ITU from introducing such regulations. ITU was able to get only 89 signatories.

The debate on the appropriate role of different stakeholders, including the government has found greater resonance after the Snowden Revelations, which reflected how states like the US cannot be blindly trusted in governing the Internet. Some others also fear that a multi-lateral organization could mean that restrictive regimes like China, Russia and Iran can censor information and fragment the Internet.

[28]http://www.itu.int/en/council/cwg-wsis/Documents/ITUPP14_RESOLUTION_140.pdf, accessed on February 20, 2015

4 Indian Initiatives Related to Internet Governance

Besides the large and growing base of Internet users including citizens, private sector organizations and the government, who use it as a vehicle of economic growth and social development, an additional driver for India to play a greater role in Internet Governance has been the national concerns over cyber-security.

While there are some civil-society organizations working in the domain of Internet and public policy, there have been few systematic national level approaches to participation in Internet Governance. The Indian government and members of civil society have participated in key activities such as WSIS in 2003 and 2005 respectively, WCIT 2012, various IGF meetings, Plenipot2014 etc. These participations have not been a part of a national strategic plan. Various departments of the government and ministries, civil society and private sector have participated independently. Even among the government departments and ministries, there has not been a coordinated approach. Unfortunately, so far, India's approach to Internet Governance at the global level has been ad-hoc.

We briefly give below the Indian institutional structure for Internet Governance and present the outcomes of participation in international forums. This will help us to analyse the current situation and recommend future action.

4.1 Institutional Structure for Internet Governance - Role of DeitY

DeitY is the nodal ministry for policy matters relating to the Internet (except licensing) and promotion of the Internet as per the Allocation of Business Rules of the Government of India. Other areas under the DeitY include formulation of cyber laws such as the Information Technology Act and assisting various ministries and departments in designing, developing and implementing e-governance. In pursuance of its objectives, DeitY has been involved in:

- ***International Participation:*** DeitY has undertaken advisory and planning processes and represented India at various Internet Governance organizations and processes including APNIC, ICANN, IGF and ISOC, IGF

- ***Managing the Critical Internet Resources:*** DeitY deals with both the technical and policy matters related to CIR through the setting up and operations of the National Internet Exchange of India (NIXI) as an Internet Exchange Point (IXP). It also manages .IN ccTLD Registry, .bharat IDN Registry, and the National Internet Registry. It is responsible for mirror root servers.

- ***Internationalized Domain Names:*** DeitY along with NIXI is entrusted with the responsibility of setting up the registry for the IDNs .भारत (.bharat) for ccTLD in local Devanagri language and other regional Indian languages.

- ***Provision of Legal and Policy Framework:*** Deity has provided the legal framework for Internet through the Information Technology Act and its rules and a framework National Cyber Security Policy etc.

- ***Playing a Pivotal Role in e-Governance Programs:*** DeitY has developed a framework for and deployed e-governance applications, both at the central and state level.

- ***Developing Frameworks for Emerging Technologies:*** DeitY has taken the lead in and developed frameworks for emerging technologies such as the Framework for Internet of Things (IoT), Framework for Mobile Governance.

The above aspects are elaborated as follows:

- ***International Participation:***

  The objective of DeitY is to establish India as an influential body in the Internet Governance space. It has been a part of Tunis Agenda, NETmundial, and IGF. DeitY has supported Multi-stakeholder approach for Internet Governance and has played a lead role in the formation of MAG. DeitY is a member of the Internet Society (ISOC) and supports capacity building through fellowships etc.

- ***Managing the Critical Internet Resources:***

  DeitY has set up the NIXI as a Section 25 not-for-profit company for providing Internet Exchange Points (IXP), .IN ccTLD Registry, National Internet Registry (NIR) and for managing mirror root servers (I, K and F) in India. NIXI was initially established for peering of ISPs among themselves for the purpose of domestic routing of domestic traffic, instead of taking it all the way to US/abroad, thereby resulting in better quality of service (reduced latency) and reduced bandwidth charges for ISPs by saving on international bandwidth. In 2005, the ccTLD Registry (.IN) operation was additionally given to NIXI under a liberalised policy framework and implementation plan devised by DietY. Till now, .IN registry has enrolled more than 1.7 million domain names. In 2012, NIXI successfully applied to APNIC and was announced as a NIR (IRINN) for allocation of numbers (IP and AS). In 2014, NIXI successfully applied for .bharat IDNs in local Indian language scripts to become the IDN registry in India.

- ***Internationalized Domain Names:***

  DeitY and NIXI have collaborated with ICANN and APNIC Regional Internet Registry (RIR) for the rooting of the domains in the local languages. The local language content greatly helps in the proliferation of the Internet as people are more acquainted with their regional languages especially in the rural areas. NIXI had set up the registry for .भारत (.bharat) for ccTLD. On November 18, 2014, domain name booking for the IDNs have begun and the websites with localised domain names were successfully launched. Domain names in other regional languages like Marathi, Konkani, Bangla, Urdu, Punjabi, Telugu, Tamil, and Gujarati would be available soon.

- ***Playing a Pivotal Role in e-Governance Programs:***

  DietY is responsible for issuing policy guidelines on all matters pertaining National E-Governance Plan (NeGP) such as standards, security, use of new technologies, etc. It also facilitates the implementation of NeGP by various Ministries and State Governments, and provides technical and program level assistance. It is implementing the core infrastructure projects such as State Data Centre Scheme (SDC), State Wide Area Network (SWAN), State Service Delivery Gateway (SSDG), State Portal, the e-District Mission Mode Projects (MMP) and project support components such as capacity building, awareness and communication etc. DeitY assists the national e-Governance Advisory Group and the Prime Minister's Office.

- ***Provision of Legal and Policy Framework:***

  DeitY has produced various policy documents to create a framework for governance of the Internet and communications. These include policies for:

  - National Cyber Security
  - E-Mail
  - National Open Data

- ***Developing Frameworks for Emerging Technologies:***

  DeitY has developed frameworks for several emerging technologies including the following:

  - Draft Framework for Internet of Things (IoT)
  - Framework for Mobile Governance
  - GI Cloud Policy
  - National IPv6 Deployment Plan

4.2 Outcomes of Participation in International Forums

4.2.1 United Nations Committee for Internet Related Policies and Related Developments

In 2011, India proposed the setting of establishment of United Nations Committee for Internet Related Policies (CIRP) as the new institutional mechanism. The CIRP would take inputs from IGF and comprise 50 member states based on equitable geographic representation.

> *"The proposed body should include all stakeholders and relevant inter-governmental and international organizations in advisory capacity within their respective roles as identified in Tunis agenda and WGIG report. Such body should also develop globally applicable principles on public policy issues associated with the coordination and management of critical Internet resources"*[29].

The functions of CIRP were envisaged as follows:

> *"The CIRP shall be mandated to undertake the following tasks:*
>
> *i. Develop and establish international public policies with a view to ensuring coordination and coherence in cross-cutting Internet-related global issues;*
> *ii. Coordinate and oversee the bodies responsible for technical and operational functioning of the Internet, including global standards setting;*
> *iii. Facilitate negotiation of treaties, conventions and agreements on Internet-related public policies;*
> *iv. Address developmental issues related to the internet;*
> *v. Promote the promotion and protection of all human rights, namely, civil, political, social, economic and cultural rights, including the Right to Development;*
> *vi. Undertake arbitration and dispute resolution, where necessary; and,*
> *vii. Crisis management in relation to the Internet"*[30].

[29] http://cis-india.org/internet-governance/blog/india-statement-un-cirp, accessed on December 8, 2014
[30] ibid

CIRP would report directly to the General Assembly and present its recommendations to consider, adopt and disseminate among all relevant inter-governmental bodies and international organizations. Initially CIRP was envisaged to be funded by the regular budget of the United Nations. Subsequently, it was planned that a separate Fund would be set up from the domain registration fees collected by various bodies. *A Research Wing was to be established by CIRP to support its activities and the fund would be mainly used to finance the wing.*

CIRP was envisaged to have multi-stakeholder representation, and also take inputs from a more strengthened IGF. The CIRP model drew upon the WGIG models put forth as outcomes of Tunis 2005. However, this proposal did not have buy-in from the domestic stakeholder community as they felt that inadequate consultations and poor governance processed adopted to come up with the proposal reflected possibly only the views of the government. There was expectedly sharp criticism from the US government and its allies, corporate sector and civil society. The proposal specified that the CIRP would take over the technical, operational and standard setting functions of Internet Governance, but did not detail out how given the existing systems, the transition could happen. Also, the proposal did not specify how the countries in CIRP would be chosen.

However, the Indian delegation changed its stand over a period of time in October 2012. Prior to the Budapest Convention, Mr Sachin Pilot, Minister of State (MoS), reflecting the changed views of the Indian government said,

> "*The extreme views being floated by some countries on Internet governance could lead to the balkanisation of Internet and we are against any such move, including control of Internet by government or inter-governmental bodies. We seek enhanced dialogue and continuation of a working group to find ways to resolve the sharp differences that currently exist*"[31]. Further, *"We are moving ahead with new proposals. While the existing system certainly needs to be changed,* ***India's position will include multi-stakeholder involvement and not inter-governmental bodies that may have been proposed in the past"***[32].

[31] http://www.thehindu.com/news/national/on-internet-rules-india-now-more-willing-to-say-icann/article3994985.ece, accessed on September 20, 2014
[32] Ibid.

4.2.2 WGEC and NETmundial

India proposed a multi-lateral approach both in WGEC and NETmundial. India, along with Japan, Iran, and Saudi Arabia were members of the WGEC. India was also a part of the HLMC of the NETmundial. India has taken a stand at WGEC and NETmundial that the Internet Governance model should be multi-lateral. This was driven by India's concern for being able to influence public policy issues with regard to Internet Governance, specifically cyber-security and surveillance.

In NETmundial submission, India also proposed renaming Internet to Equinet, a concept put forward by its then Minister of Communications and IT, Mr Kapil Sibal. This concept aimed at reflecting that all nations should be equal stakeholders on its operations, thus bringing in greater equity in the choice of standards especially in areas such as cyber-security, data protection and privacy. This was to counteract the dominance by the US and allies in the developed world. The model of all nations becoming equal stakeholders would result in decentralization of decisions related to the Internet. This was in the wake of Snowden revelation, regarding India.

> *"The Internet governance should be multilateral, transparent, democratic, and representative, with the participation of governments, private sector, civil society, and international organizations, in their respective roles. This should be one of the foundational principles of Internet governance"*[33].

4.2.3 WCIT-12

Despite DoT's support for ITU as a multi-lateral organization to take lead in Internet Governance, India is not a signatory to the WCIT proposals.

4.2.4 Joint Working Group on Cyber Security

Recognizing the role of private sector, the government decided that under the National Security Council Secretariat (NSCS), a permanent Joint Working Group on Cyber-security (JWG) would be setup. The JWG was envisaged as an advisory body and would coordinate Public-Private Partnerships (PPP) on cyber security. The areas of focus were identified as standards, audit, testing and certification, security, and capacity building through setting up of Centres of Excellence. Joint Committee on International Cooperation and Advocacy

[33]Initial submission of the Ministry of External Affairs (MEA), http://www.bgr.in/news/india-wants-the-internet-to-become-equinet/, accessed on October 14, 2014

(JCICA) was set up as a permanent Advisory Committee (AC) to provide a platform for articulating India's perspective on various Cyber-security issues, especially in International forum.

4.2.5 India IGF

As a part of its activities to participate more actively in Internet Governance activities, India set up the India IGF in July 2013, along the lines of similar organizations in other countries. A MAG has been constituted to steer the India IGF. The MAG comprises of experts from the academia, industry consortiums, civil society and from relevant ministries of the government. The first India IGF was scheduled for November 2014.

Besides a number of active civil society organizations, India also has four ISOC chapters, with varying levels of activities.

4.2.6 ICANN

India's participation in ICANN, through its various Advisory Committees (AC), Supporting Organizations (SO) and User Constituencies (UC), is summarised in 'Annexure 2 – India's Participation in I* Organizations'. This summary reflects that India is under-represented in the decision-making bodies of ICANN.

4.2.7 Pre- Plenipot and Plenipot 2014

In the Pre-Plenipot, the DoT took the stand that ITU, must play a dominant role in Internet Governance. This is because, ITU has member states in decision-making committees and has played a coordinating role in allocation of numbering resources for the PSTN and spectrum It has also worked in developments of some telecom standards. The DoT's viewpoint is that since Internet runs on telecom infrastructure, the governance mechanisms for the same should be adopted for the Internet. Further, this will allow the governments to play a dominant role in Internet Governance. The DoT's position was contrary to the discussion and meeting outcomes on the role of Internet Governance with the Industry. Further, apparently such submissions were not as per the pre-plenipot processes. This recommendation was not accepted.

The DoT has taken a stand at the ITU Plenipot 2014 that there is a need for:

- An IP Address Allocation Plan that ensures that IP address allocations of different countries are discernible, systematic, equitable, fair, just, democratic and transparent.

- A Routing Plan or Network Architecture that
  - ensures domestic traffic remains domestic and does not traverse in foreign jurisdictions.
  - allows traceability of communications
  - ensures safety, robustness and resilience
- Standards/Protocols that are secure and tamper-proof in the wake of IoT and Machine to Machine (M2M).

Critique of the DoT Stand at the ITU Plenipot - 2014

Many of the issues raised by DoT in the ITU Plenipot are driven by cyber-security concerns. For example, need for discernible IP address allocation, local routing, traceability, secure standards etc. are driven by security needs.

Concerns arising from the cyber-security perspective: The concerns of the DoT identified above are justified and non-negotiable, but the means of achieving such objectives need to be reviewed. There are two possible ways to achieve these objectives: (i) to work with IETF to evolve existing standards; and (ii) to develop competing standards and start a new network that eventually replaces the Internet. To adopt the first option would imply strengthening existing processes in India to participate in IETF and to have greater representation on India specific policies. For the second option, the ITU or a domestic Standard Development Organization (SDO) would have to release alternate standards that are different from IETF standards, which would result in a fragmented Internet. Due to poor network effects, the alternate standard may find little acceptance in the short run. For such an initiative even to take off, significant lobbying amongst different nations would need to be done, both at the political and technical level. Politically, the idea that the new Internet may have constraints on sharing information or restrict content would have to be sold. Technically, this could require changing existing hardware and software for which the selected countries must see benefits. Evolution of standards is a slow and continuous process; and pushing for an alternate standard to emerge in the short run does not appear to be practically feasible.

Therefore, the question reduces to how, within the framework of existing (and evolving) IETF standards, can DoT achieve its stated objectives in the short run? For example, within the framework of existing standards, domestic routing can be ensured by (i) having an effective Indian IXP; and (ii) having data hosted domestically. Both (IXP and domestic data centres) are domestic issues that do not require the intervention of the ITU. Currently, India needs to revise its domestic IXP policy and to provide a conducive regulatory and economic environment for domestic data centres, as explained in detail in later sections of the paper.

Concerns regarding fair and equitable distribution of IP addresses: IP addresses are currently a limited resource given the limited bits in the Internet Protocol version 4 (IPv4) address. With evolution to IPv6, such concerns are expected to be reduced as it substantially increases the address length, and the resource pool that it creates. The speed of transition to IPv6 should therefore be a priority for India. As of now, such transition is slow: as of statistics released in 2013, only 6 of the 22 major ISPs were IPv6 compatible.

Another alternative that DoT may have considered is placing ICANN under the oversight of an organization like ITU. This would address the concern of several countries, including India that USA had disproportionate influence (Lenard and White, 2011). However, the IANA transition framework precludes such a possibility. Further, the responsiveness of a bureaucratic organization that requires agreements between different governments is likely to be low and could impede further developments.

Yet another mechanism to influence IP address allocation in the Asia Pacific region is through APNIC. Within this region, the concern of DoT is reflected in the statistics that Eastern Asia (including Japan) holds 2,712,098 of the IPv4/24 addresses while South Asia (including India) holds only 170,365 of the IPv4/24 addresses[34]. However, such statistics may also reflect that India has been a late adopter of the Internet. In addition to the skewed allocation of IP addresses, the election process of the APNIC EC is also a matter of concern as discussed later in the paper.

A National Internet Registry (NIR/IRINN) has been created in India for domestic allocation of IP addresses in 2012. The NIR has given greater autonomy to India in its allocation of IP addresses. However, this process was delayed as there were uncoordinated parallel applications for NIR sent to APNIC by DeitY and DoT[35].

APNIC policy development processes (PDP) follow a bottom-up process and provide an additional venue to have its concerns addressed. Therefore, while ITU may be one venue for addressing such concerns, India should also adopt the APNIC PDP process for ensuring fair and equitable distribution. If the DoT is suggesting that the ITU should take over the functions of the RIRs, it needs to suggest a migration path that chalks out how reallocation of existing IPv4 resources is going to take place, so that such a plan may be reviewed on its merits. On the other hand, by playing a greater decision-making and policy role in APNIC, India could influence the allocations as APNIC is a constituency for

[34]www.apnic.net/publications/research-and-insights/stats/ipv4-sub-regions, , accessed on September 28, 2014
[35]https://www.apnic.net/__data/assets/pdf_file/0020/14915/india-nir-cfc.pdf, accessed on October 16, 2014

ICANN, whose constituencies include the RIRs. This could be a pragmatic route to achieve our objectives.

4.3 Recent Developments:

In recent meetings, there has been discussion on India Internet which needs to be "examined with regard to trust relationships, peering relationships, necessity and open architecture and risk containment mechanisms" (NSCS, 6th meeting of the JWG on PPPs in cyber-security, author's records). However, we could not get details of it. The JWG has decided to focus on sector specific Information Sharing and Analysis Centres. Further, the JWG decided to set up and chair a sub-group consisting of DeitY and private sector associations on cyber-security in international forums.

4.4 Summary

Of late, there has been a growing acknowledgement within the Indian government that the multi-lateral approach is unlikely to work, as most western countries that have strong voices and resources to lead Internet Governance processes do not agree with this approach. On another dimension, the industry in India feels that by supporting multi-stakeholder approach, western countries, predominantly the USA, give support to their private sector, whereas the Indian government explicitly does not. The lack of Indian companies that have strong presence in the Internet space broadly makes it difficult for the Indian government to support the private sector. This is in contrast to USA and China that have strong Internet companies.

DoT, MEA and DeitY have taken varying and sometimes conflicting stands on Internet Governance. For example, in the pre-plenipot concluded recently, the DoT made a submission that recommended that ITU take over the CIR management[36] (even though ITU has not made any such statement of intent) that was not accepted. MEA has been recommending a UN like structure. The MEA has formulated its approach based on the framework that national security has traditionally been managed by member states alone within multi-lateral bodies under the UN. In contrast, in the recent IGF in Turkey in 2014, DeitY took the stand that a more nuanced approach is required that recognizes the different layers of Internet Governance[37]. India's stand has largely been voiced by DoT and MEA, mostly in multi-lateral forums such as ITU and UN respectively.

[36] 4th APT Preparatory Meeting for PP-14 (18th to 22nd August 2014)
[37] http://www.intgovforum.org/cms/174-igf-2014/transcripts/1977-2014-09-04-ms-evolution-of-the-ig-main-room, accessed on October 16, 2014

5 Current Debate on Multi-Lateral versus Multi-Stakeholder

5.1 Context of the Debate

The debate on multi-lateral versus multi-stakeholder revolves around the question of what should be the roles and responsibilities of different stakeholders in various Internet Governance mechanisms. This further translates into questions such as: Who are the relevant stakeholders? Is public policy-making the exclusive right of the nation states? Does the concept of nation states exist in an online borderless virtual environment? Should different stakeholders participate at an equal footing? Can governance processes followed for technical issues also be adopted for policy issues?

The Tunis Agenda attempted to answer a few of these questions. It noted that Internet Governance encompasses both technical and public policy issues; it also recognized that while management of the Internet should involve all stakeholders, different stakeholders have specific roles and responsibilities. The Tunis Agenda, emergence of the two approaches (multi-lateral and multi-stakeholder), and the creation of the two tracks (IGF and Enhanced Cooperation) are summarised in ***Section 3.1***. The importance of the debate in the context of the Snowden Revelations and WCIT 2012 is summarised in ***Section 3.4***. India has so far predominantly adopted the multi-lateral approach in international forums for Internet Governance. The DoT has recommended that the ITU (a UN organization) should take the lead, while the MEA has favoured the UN.

Characteristics of the Multi-Lateral and Multi-Stakeholder Approaches:

The multi-stakeholder approach is generally characterised by an open participation and a bottom-up policy process that is consensus driven and usually produces non-binding soft outputs. In contrast, the multi-lateral approach is generally characterised by participation limited to member states and a top-down policy process that veers towards voting for resolution and produces outputs that are more binding on its members. Often, multi-stakeholder approach is seen as favouring US dominance, since the representation from private sector is largely driven by large Internet companies such as Facebook, Google, Yahoo! etc, all of which are US based companies. On the other hand a multi-lateral approach, with member state representation is seen as diluting the US dominance.

However, the characterisations of both multi-stakeholder and multi-lateral sometimes differ from process to process. For example, there exist many variations of multi-lateral processes that initiate bottom-up agenda setting processes. Similarly, there are many multi-stakeholder processes that have resorted to voting to deal with holdouts. There may be multi-stakeholder implementations where the final decisions

and implementation may be assigned to a single stakeholder group. These decision makers are always accountable to all of the stakeholders for their decisions and implementations.

It is also recognized that there are different types of multi-stakeholder and multi-lateral processes (Mueller and Wagner, 2014). For example, Hill (2014) suggests three different types of multi-stakeholder models: (i) with different roles and responsibilities as fixed by the Tunis Agenda; (ii) with equal footing for all, including for public policy issues; and (iii) with only advisory role for governments (like the GAC of ICANN).

Similarly, different types of multi-lateral models also exist including, but not limited to: (i) a consultative policy development model wherein the viewpoints of various stakeholders feed into the decision-making by the Governments (ii) a closed non-consultative process comprising only of governments; and (iii) a process wherein only the final yes-no decision lies with the governments whereas the policy development process is bottom-up.

On another dimension, there are proponents of the multi-lateral approach that advocate "a new form of multi-lateral cooperation….which emphasizes the importance of networks between state and private actors…global partnerships, multi-stakeholder initiatives, global public policy networks and governance concepts of variable geometry" (Martens, 2007, pg 3). Few authors view that multi-lateral governance encompasses the relationship between the private and public sector with specific roles assigned to each (Christou and Simpson, 2011). Further, the increasing role of non-state actors such as civil society, academics, professional experts, advocacy networks has given rise to contemporary form of multi-lateral approaches that are now required to take them into account in their decision-making structures and processes. These transnational actors, who act beyond national borders but do not represent their governments, have created complex forms of governance[38]. On the other hand, the aspects of legitimacy, representativeness and accountability in a multi-stakeholder environment are open to debate (Bendiek and Wagner, 2012; DeNardis and Raymond, 2013).

Despite the rhetoric on both sides of the multi-lateral and multi-stakeholder approaches and the possible variations, there has been little discussion on what could be practical ways to combine or put together structures that combine the best elements of both approaches. It is in this context that we need to view India's stated position of adopting a multi-lateral approach with respect to Internet Governance.

[38]http://acuns.org/wp-content/uploads/2012/06/Transnational_turn_in_Multilateralism.pdf, accessed on September 20, 2014

Strategic Concerns Regarding India's Adopted Approach

It is important for India to articulate its views regarding the forms of Internet Governance that it will adopt. Such mechanisms signal to the investors, other governments, and citizens the likely path of Internet growth in the country. The dilemma as posed by decision-makers is that while a multi-lateral approach allows the government to have a dominant role in policy making, the little support for India's position has isolated it. Therefore, for the Indian government, the issue framed by decision-makers is how to design institutions/committees/processes that define the role of the government in a way that reflects the open ethos of and multiple stakeholders in Internet Governance while retaining its dominance in public policy making? We highlight the issues in India's stated position.

Power Balance: India's preference for adopting a multi-lateral approach is partly driven by an objective of its concern for diluting the dominance of US and western countries. However, an examination of the more recent multi-lateral organizations, which have been designed to address the concerns of emerging economies in other policy arenas, shows that they have not been entirely successful. For example, while World Trade Organization (WTO) was started with the mission of "ensuring a level playing field for all"[39], emerging economies have been side lined[40] by the economic and political interests of global powers.[41] Assessment of WTO has shown that participation in WTO and information support from WTO continues to be a challenge from an emerging economy's perspective. Empirical evidence cited in numerous reports suggests that lack of capacity within emerging economies results in persisting content-related and participation-related challenges. How is India going to address the future reality of similar multi-lateral forums for Internet Governance, were such a suggestion to be implemented?

Perception of Openness*:* Increasingly, trading partners from the developed world are likely to link the goal of facilitating free flow of information and data across national boundaries while protecting individual privacy and Intellectual Property Rights (IPRs) as a part of future trade agreements. This is because they foresee that future growth of Internet will facilitate growth of their businesses. If India's stand on Internet Governance is seen as restrictive, it is unlikely that future trade will be facilitated. India's stand in various Internet Governance forums elaborated earlier has been convergent only with a handful of countries namely Iran, Saudi Arabia, Russia, China. These countries have been advocating a national network or

[39]www.wto.org/english/thewto_e/whatis_e/wto_dg_stat_e.htm, accessed on September 20, 2014
[40]http://www.guardian.co.uk/global-development/poverty-matters/2011/jul/29/wto-doha-fails-poorest-countries, accessed on September 20, 2014
[41]http://www.twnside.org.sg/title2/twninfo339.htm, https://saylor.longsight.com/handle/1/10903, http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=7809812&fileId=S1474745610000261, accessed on September 20, 2014

"balkanization" of Internet, which would restrict the freedom of their citizens to the free flow of information, an inherent characteristic of the Internet as it is largely known now. Such "clubbing" with restrictive regimes on the issue of Internet freedom may send a wrong signal to existing and potential investors. Such an approach has already isolated India. Ironically, some of the countries that have sided with us are not our significant trading partners. While it is necessary that at the sovereign level, we should be driven by larger governance principles, it is also important that we reflect the democratic, open ethos of our country in public forums. If other countries, notably USA, Europe, UK, Japan and Korea see India's stance as restrictive, it is unlikely that companies in those countries are likely to make investments in the Information and Communication Technology (ICT) sector, as they are likely to foresee lower Internet penetration and hence evaluate India not as favourable for their investments.

Limited Action and Contribution: There has been little contribution from India in terms of the blueprint of the proposed role that India wishes to play in this domain. The submissions in the international forums (for example, in NETmundial) have been proposing primary role for the states through UN like agencies. However, the role and scope of proposed organizational structures or processes that could deal with Internet Governance within UN have not been elaborated. There has also been little action on the ground to seek alliance with other like-minded countries to develop an agenda and work together. Further, DoT and MEA have taken different views. For example, in the pre-plenipot concluded recently, a DoT submission recommended that ITU take over the CIR management[42] (even though ITU has not made any such statement of intent) while MEA has been recommending a UN like structure. The DoT's position was contrary to the discussion and meeting outcomes on the role of Internet Governance. Further, apparently such submissions were not as per the pre-plenipot process requirements.

Limited Scope of Participation: On another dimension, whatever be the content of message in the DoT's submission, there was disregard for the views of the industry, without sharing this concern with the latter. We are not sure whether Department of Information Technology (DIT) was consulted on this issue. If India wishes to play a significant role in Internet Governance, then it must establish processes of discussion, debate, involvement of all stakeholders, including businesses and civil society domestically.

Scope of Governance: Many government officials were concerned that a multi-stakeholder approach that advocates an equal footing for various stakeholders in its processes is contrary to their belief that government has a dominant role in policy making. We believe that this is a limited perspective. Citizens and various

[42] 4th APT Preparatory Meeting for PP-14 (18th to 22nd August 2014)

stakeholders now demand a greater say in how they are governed. Governance processes must provide space for this. Further, this approach does not take into account that even when governments need to take a lead in decision-making, the processes of identifying the agenda, seeking inputs could be participative and the government should consider itself first among equals.

Proposed Role by DoT for ITU in Standards Development

There is a concern that issues of relevance to emerging economies including those of India are not addressed in standards bodies. This was possibly one of the drivers for DoT to propose that the ITU should take over the standards for CIR, including IP addresses, protocols, and DNS. However, a review of standards development and adoption process shows that standards are increasingly being developed in private sector led professional groups and consortia and not through intergovernmental bodies.

Further, ITU-T (the ITU group that deals with standards) membership is limited to member states, private (vendors) and professional bodies such as Institute of Electrical and Electronics Engineers (IEEE). The ITU-T tends to follow a relatively closed process wherein standards are not open to comments and reviews from non-paying volunteers (Ryan and Glick, 2012).

Recognizing the emerging role of Internet standards, ITU now collaborates with organizations like IEEE and IETF on some standards. Given the need within ITU to organize itself around member countries, it is possible that even when ITU recommends a standard, it may be driven by the need to support a private company in that country (for example, Huawei for MPLS in China) (Bennett, 2012), rather than the developmental interests of the emerging economies. It is in this context that the debate on the role of ITU vis-à-vis existing organizations involved in standards has emerged. ITU's role and process in standard making have the following concerns:

a. *Adoption Rate in the Internet Space*: While ITU has ventured in the Internet space, the adoption rate (refer to the Perceived Legitimacy Framework in Section 5.3) of standards in this space has been poor. The X.25, OSI (Open Systems Interconnection) suite of protocols for internetworking and X.400 for email are a few examples of where visible efforts were failures. (Malcolm, 2008, pg 59). There have been few successes. There is a concern that ITU-based standards are "complex, hierarchical and over engineered" (Malcolm, 2008, pg 60). To be more visible, in recent times, ITU has attempted to be involved in the Internet space through linkages with IETF and ICANN.

   A few areas where ITU based Recommendations have been deployed on the Internet include: E.164, spectrum orbital slots, the specification for telephone

numbers and its usage by ENUM (an IETF standard that maps telephone numbers on the DNS), initial success of H.323 (for VOIP), later being overtaken by a community standard, SIP; and X.509 for digital cryptography. Even here, the strong support of Microsoft and Netscape for a hierarchical trust mechanism was credited for the success of X.509 (Malcolm, 2008).

b. Institutional Capacity:

i. Limited Participation: ITU conferences take place without substantive input from academia, civil society and representatives from the private sector. Further, USA's commitment to ITU based Internet standards have been reducing.

Only member states and sector members may participate in the various ITU activities. While the membership includes governments, private sector, and academia, the cost of membership is considered high by most entities in emerging economies (Ryan and Glick, 2012).

Having and enabling broad-based participation is not an implicit design element of ITU processes. For example, Council Working Groups preparatory processes for WCIT precluded participation from civil society. Further, participation by academic institutions in the Plenipot processes is severely limited. The rule making processes for standards development are shared only with participating members and sector members. In contrast, the IETF process is open for anyone to participate.

c. *Openness of ITU Standards:* While ITU standards are now freely downloadable, the intermediate drafts are not. In the IETF, there is a drafts directory, open to all where intermediate drafts are uploaded for review and comments. For example, in the case of the MPLS standard, despite a joint working team (JWT) of ITU and IETF working on it, the ITU developed its own version. When it came to making a choice, only the member states were allowed to vote, not the sector members such as IETF43. After several meetings it was decided that IETF would have the sole responsibility for MPLS design, while research on transport layer would be taken up by the ITU SG -15.

d. *Narrow Representation:* Companies at the application layer (such as Google, Facebook) have not been represented in the ITU, although there is no formal reason for them to not be.

[43]http://www.internetsociety.org/, accessed on October 15, 2014

Thus, not only has the ITU played a limited role in Internet standards, its structures and processes are not designed for supporting open participation. On another dimension, given that standards are increasingly being set in and by industry bodies, the role of governments is changing to selection of standards at the domestic level.

So, having a multi-lateral organization such as the ITU responsible for developing standards is not appropriate. Nor is it a guarantee against private sector capture or undue influence of some member states, reducing the perceived legitimacy. An open forum with inputs from a number of actors is a better option. Further, legitimacy for the outcomes that these standards bodies have is through their expertise and the ability to make things work and ensure that the announced standards are adopted.

DoT's support for ITU to take lead in Internet Governance must be seen in the light of the aspects mentioned above and a judicious choice needs to be made. Public statements at the national level will not only affect the trajectory for Internet growth but also the investment climate for private and foreign companies in India.

5.2 Summary of Existing Arguments

After a summary of the arguments presented by those who treat the two approaches as dichotomous, we show that each of these approaches may be characterised on the basis of a number of parameters, thus resulting in a more nuanced enunciation of an appropriate approach. This allows us to move away from rhetoric and give a more analytical basis for adopting an appropriate approach.

Table 1 summarizes the multi-stakeholder and multi-lateral approaches along the dimensions given below.

Table 1: Different parameters in multi-stakeholder and multilateral approaches

S.No	Parameters	Multi-stakeholder	Multi-lateral
1	Participation	Wide including civil society, academia, private sector and governments.	Nation states
2	Representation	• Wider constituencies • Greater role for civil society and corporate	• Narrow Constituencies • Greater role for nation states
3	Decision making/ Agenda Setting	Top down	Bottom up
4	Transparency	Claimed to be open	Closed
5	Capture	Corporate (Claimed to be US dominated)	States with restrictive regimes like China, Iran, Russia etc.,
6	Accountability	Constituencies	Nation states/citizens

S.No	Parameters	Multi-stakeholder	Multi-lateral
7	Processes	• Scope for innovation (exemplified by evolution of the Internet)	• Slow and bureaucratic • Possibility of vote trading between states.
8	Role for civil society	High	Limited
9	Outcomes	Binding	Non-binding
10	Shortcomings	• Controlling spam, malware, cyber-crime, illegitimate expressions, lack of privacy and surveillance • Linkage between funding agencies and civil society members may not be clear	Limited scope for creative solutions and restrictive participant scenario, fear of capture by states with opposing ideologies

Source: Author's Analysis

Based on India's stand so far, we analysed the characteristics of the two approaches and consequently, arguments for and against them. We use this analysis to develop a framework based on the perceived legitimacy of the proposed model.

5.3 Need for Establishing Legitimacy

Institutions and organizations in the Internet Governance space have a strong need to establish the legitimacy of their processes as these are new kinds of governance mechanisms outside of existing forms of organizations such as governments, multi-lateral or civil society organizations. To establish their legitimacy or the acceptance of the governance relationships, they also need to articulate explicitly the driving underlying logic of the same. Since such organizations do not derive their authority from being sovereign states or have legitimate authority as given to international governance organizations that have been created with the consent of sovereign states (Bernstein and Cashore, 2007), they need to establish legitimacy to be effective (Skogstad, 2011B; Underhill and Zhang, 2008).

Legitimacy of global governance came into focus with the emergence of global governance institutions such as the World Bank, IMF, WTO etc. The focus emerged despite the fact that these institutions were created within the ambit of and concurrence of nation states. Emergence of the network mode of governance of global resources in which a variety of actors including governments, civil society, technical experts, private organizations are involved in policy decisions and governance, creates a need for establishing legitimacy (DeNardis, 2010). This is because a variety of non-state actors are involved in this process (Bogason and Musso, 2006; Juhola and Westerhoff, 2011). Institutions in other global governance spaces that have similar ambit to influence domestic, regional and international

processes are Kyoto Protocol, judges and regulators networks, international environmental law (Bernstein, 2004-05) and Financial Action Task Force[44], amongst others (Bernstein and Cashore, 2007). The power of such organizations to frame rules and the authority to link them to consequences of non-compliance, much like nation states has heightened the need for assessment of their legitimacy to do so (Buchanan and Keohane, 2006; Zurn, 2004).

As in the Internet Governance space, organizations such as FATF, Kyoto Protocol are network organizations that develop policy but do not derive their policy making authority from the power of being a sovereign (DeNardis, 2010). While states may play a significant role in their processes, such organizations are not accountable to them. They are more often accountable to the communities that they represent.

Past work on legitimacy highlights both factors such as "normative environment", and the processes such as interactions of actors within communities (Bernstein and Cashore, 2007). Further, (Kummer, 2012; Scharpf, 1999; Skogstad, 2011A; Underhill and Zhang, 2011) argues that both input including procedural and output legitimacy are necessary in such contexts. Skogstad (2011B) suggest that "all strategies to render policies acceptable by virtue of democratizing the procedures by which they can be arrived at can be viewed as input legitimation". The ability to make binding decisions and willingness of communities to obey such decisions is influenced by the input quality of representation, representativeness, accountability and transparency on the input side (Skogstad, 2011B). On the output side, while input legitimacy is necessary, the extent of participation, democratization of processes and consensus facilitates acceptability of outcomes (Scharpf, 1999: pg 7; Vallejo and Hauselmann, 2004). While on one hand participation enhances legitimacy (Undehill and Zhang, 2008; Vallejo and Hauselmann, 2004), in the context of EU genetic engineering policy formulation, it was found that it could also lead to weaken it as resolution of conflicts could become more problematic in a more diverse group (Skogstad, 2011B). Similar results regarding the relationship between efficiency and legitimacy have been reported in (Vallejo and Hauselmann, 2004) in their analysis of multi-stakeholder processes.

Another dimension that contributes to enhanced legitimacy is accountability of outcomes (Buchanan and Keohane, 2006; Underhill and Zhang, 2008) to the relevant stakeholder groups. The issue then is how these may be identified. For example, are civil society organizations accountable to their funders or the citizen groups or causes they represent? A related construct is that of transparency in the processes of the organization. This relates to the easy availability of accurate information, both within and outside the organization regarding its operations.

[44] http://www.fatf-gafi.org/, accessed on February 20, 2015

The relationship between outcomes and perceptions of legitimacy is not necessarily commutative. For example, legitimate processes could lead to poor outcomes and good outcomes may not necessarily be the result of legitimate processes.

The challenge in developing an analytical framework for Perceived Legitimacy is that the "perception of legitimacy differs across time, place and organizational context, making it impossible to determine a set of criteria for legality that is generally applicable to all governance institutions" (Bernstein and Cashore, 2007).

> *"There are some currently recognized and accepted norms for global governance that have been established in the context of democratic western world scenario organizations (Koppell, 2008). These include (Koppell, 2008):*
>
> *Representation: Those governed need to have a voice in decision-making and the right to be represented.*
>
> *Participation: Those governed need to have the opportunity to observe and comment on the activities of the governance initiative.*
> *Neutrality: All stakeholders involved need to be treated equally and consistently.*
>
> *Procedural regularity: Decision-making processes need to take place according to a set of general procedures: Decisions need to be transparent, open for public scrutiny, and there needs to be a right of appeal (Bernstein and Cashore, 2007)".*

Significant work on Perceived Legitimacy has been done in the context of global governance organizations in the areas of climate change (Bernstein, 2004-05; Vallejo and Hauselmann, 2004; Virgoe, 2009), and the financial sector. However, there is little work that integrates the various aspects related to legitimacy in the arena of Internet Governance.

In the following, we attempt to develop such a framework based on the literature survey above and interviews conducted with different stakeholders. The proposed Perceived Legitimacy Framework (PLF) is the first step developing a strategic approach towards India playing a greater role in Internet Governance. This framework could also be used as a basis for evaluating the quality of any chosen approach.

5.4 Our Approach – Perceived Legitimacy Framework

In this framework, we identify parameters on the basis of which stakeholders assess the legitimacy of a process. Next, we break down the governance processes into its structural and procedural components and then identify how each component affects

the perceived legitimacy of the process in the minds of the stakeholders. We also show that when broken down to their structural and procedural components, it results in more nuanced discussion on the perceived legitimacy of the approaches.

We categorise the identified parameters into three aspects covering the life cycle of processes namely (i) participation; (ii) agenda-setting and decision-making processes; and (iii) outcomes.

Each aspect comprises of parameters that we use to develop a framework of perceived legitimacy parameters as follows:

(i) Participation

- *Openness to Participation:* Any policy process that is open to participation by all relevant stakeholders is perceived to be more legitimate in comparison to one that excludes participation by an important stakeholder category

- *Diversity and Representativeness of Participation:* A process that is representative and has a wider diversity of participation is viewed as more legitimate than a process with lower diversity.

- *Barriers to Participation:* Even if participation is formally open, the extent of barriers (language, location, funding and capacity) to the participation in any process contributes to its perceived legitimacy.

(ii) Agenda-Setting and Decision-Making Processes

- *Agenda-Setting:* The agenda-setting process may either be bottom-up or top-down. A bottom-up process is viewed with higher legitimacy as it provides participants at all levels to contribute.

- *Resolution:* In the final decision-making process, an outcome will have more legitimacy if all stakeholders agree or compromise on an outcome, in comparison to a process wherein the decisions of dominant stakeholders prevail.

- *Preparedness and Level of Discussions:* A process wherein participants are well prepared for discussion is viewed with greater legitimacy than a process wherein participants come unprepared. Additionally, the legitimacy of a process is viewed to be greater if the level of discussions is more detailed and advanced.

- *Accountability:* We examine the following dimensions:

- *Transparency:* A process in which there is higher transparency is viewed to be more legitimate than a process in which there is little or no flow of information regarding the process. Flow of information allows stakeholders to observe the process and empowers them to critique it.

- *Capture:* A process that is prone to capture, or has been captured in the past is viewed with low legitimacy while a process that can avoid capture or has not been captured is viewed with higher legitimacy. Processes that do not build in sufficient checks and balances to prevent capture are not perceived to be legitimate.

- *Influence:* A process in which the entity to be regulated could play an influencing role in decision-making process is viewed with low legitimacy.

(iii) Outcomes

- *"Bindingness" or Adoption Rate*: A process in which the outcome is either binding on the participants or if non-binding, has a high voluntary adoption rate is seen to have higher legitimacy.

- *Constructiveness:* A process which produces tangible outputs is viewed with greater legitimacy than a process that does not produce results.

Informed choices about the appropriate approach to adopt should take into account the framework that we have outlined above. Labelling an approach purely as multi-stakeholder or multi-lateral is not appropriate as either approach could have varying extent of these parameters.

By breaking down the process into its various structural and procedural components using the Perceived Legitimacy Framework (PLF), it is apparent that the two approaches are clearly not dichotomous. There are numerous variations of the two approaches that are ignored if the two approaches are treated as dichotomous. We shall use the PLF in subsequent chapters to arrive at the recommended policy approach.

Summary: India's rationale for seeking a multi-lateral body for Internet Governance is not clear. While with the Snowden revelation, USA's dominance and role of multi-stakeholder in Internet Governance has been questioned, but it is not clear how a multi-lateral approach alone would solve these issues. Further, these issues are ***those that several other countries also espouse. However, they are not all suggesting a multi-lateral approach.*** There is a need to focus on Internet Governance space on dimensions other than cyber-security and adopt a wider perspective.

There is scope for India to consider and move towards governance mechanisms that are more open and participative and aim to see how it could influence Internet Governance domestically, regionally and internationally to take into account concerns of emerging economies.

Based on this analysis of India's adopted approach, we use our PLF as a basis to arrive at the recommended policy approach. In the next chapter, we apply this framework to the underlying architecture of the Internet to recommend the policy approach for India.

6 Multi-Tiered Framework for Internet Governance

6.1 Introduction to the Tiered Approach

To recommend the scope of Internet Governance for India, we take the underlying layered architecture of the Internet as a basis and incorporate the specifics of the relevant public policy issues. In this approach, five tiers of Internet architecture have been identified. The tiered approach demonstrates that since the functions, actors, processes and institutions at each of these layers are different, the public policy issues are likely to be different. The tiered approach highlights the need for different governance mechanisms at each of the tiers. Given the difference between the tiers, a single institutional approach towards Internet Governance may not be the most efficient.

Based on the following tiers of Internet architecture and functions, the corresponding policy issues are highlighted:

- *Infrastructure Tier:* This tier comprises of the physical infrastructure that is required for access to the Internet. The dominant policy issues in this layer are licensing and spectrum management, interconnection, access, and standards.

- *Critical Internet Resources (CIR) Tier:* In this tier, relevant policy issues are around allocation of IP/AS numbers, management of the domain name system including root name servers, and development of protocols and standards.

- *Service Tier:* This tier comprises of policy issues such as security, spam and malware.

- *Content and Application Tier:* This tier comprises of policy issues arising from content and applications such as privacy, intermediary liability, copyright etc.

- *End User Layer:* This tier comprises of policy issues dealing with the end user including capacity building, awareness programs, affirmative action and regulating end user behaviour on the internet.

The following diagram summarises the Multi-Tiered Framework for Internet Governance. The framework identifies the various organizations, institutions, network elements, services, processes and issues that are relevant at each tier. For example, at the Infrastructure Tier, the framework recognizes Telecom Service Providers, Internet Service Providers, Infrastructure Providers (IP-I), Internet Exchanges, Equipment Manufacturers and Software Developers as important actors. It also shows the nature of policy interventions by the Government in that tier. At the Infrastructure Tier, licensing and spectrum management, interconnection, access and

standards are important public policy issues. Similarly, at the CIR Tier, public policy issues such as new ccTLD and gTLD applications; and allocation of IP/AS numbers etc. are important. The framework also shows how actors in one tier interface with actors in another tier. For example, the framework shows how NIXI from the Infrastructure Tier interfaces with the IETF, Country Code Names Supporting Organization (CCNSO) and RIRs in the Critical Internet Resource Tier.

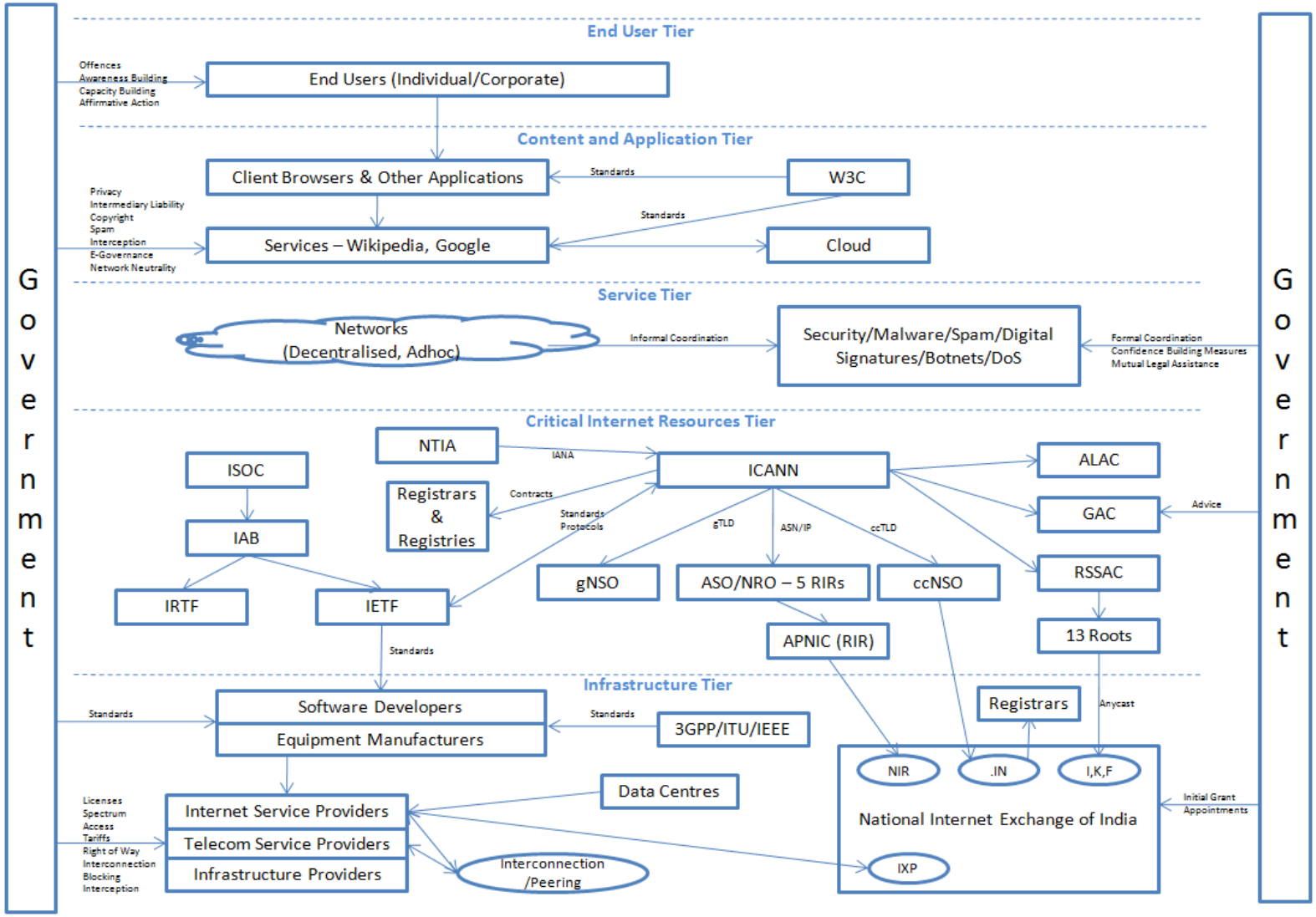

Fig 2: Tiered Architecture of Internet

6.2 Infrastructure Tier

The Infrastructure Tier comprises of the physical infrastructure that is required for access to the Internet. The governance mechanisms of this layer determine who and what regions have access to the Internet and what is the dominant technology for accessing the Internet. While most debates largely focus on the international dimensions of Internet Governance, critical aspects of the Infrastructure Tier are largely governed by governance mechanisms evolved domestically.

The dominant actors of the Infrastructure Tier are the Telecom Service Providers, Internet Service Providers, Infrastructure Providers (IP-I), Internet Exchanges, Equipment Manufacturers and Software Developers besides the state actors and institutions such as the Ministry of Communications and Information Technology (MCIT) and the Telecommunications Regulatory Authority of India (TRAI). The actors in this layer are primarily domestic players; and the processes are largely top-down.

The dominant policy issues in this layer are licensing and spectrum management, interconnection, access (including tariff regulation, right of way and quality of service) and standards. These need to be seen in the light of the poor Internet penetration in India at 19.3% as of March 31, 2014. (Note: This refers to those with a data pack subscription, not necessarily Internet users). Not only is Internet access very low, the quality of Internet access is also poor. As per Akamai Report[45], India's rank was 115 among 137 countries surveyed in terms of Average Connection Speed of 2.0 Mbps, after Indonesia (rank 101) and Philippines (rank 103) with an average of 2.5 Mbps. The highest speed was for South Korea at 24.6 Mbps. In comparison, China was ranked 73rd with an average of 3.7 Mbps. There is a similar picture for the Average Peak Connection Speed. Hong Kong stood in the global first place with peak speed of 73.9 Mbps. The countries with very low speed in Asia Pacific region were China ranked at 97th with 17.4 Mbps and India ranked at 110th with 14.4 Mbps. On the dimension of high broadband connectivity, i.e., percentage connections having speeds above 10 Mbps, South Korea was ranked first globally with 78% high broadband connectivity. For India, this number was 1.2%. When we consider the percentage of those connections above 4 Mbps, South Korea had 95% rate, while for India it was 7.2%. 'Appendix 1 - Internet Statistics for Different Countries' gives the data excerpted from the report.

[45] http://www.akamai.com/dl/whitepapers/akamai-soti-q214.pdf?campaign_id=F-MC-22494&curl=/dl/whitepapers/akamai-soti-q214.pdf&solcheck=1&WT.mc_id=soti_Q214&, accessed on October 20, 2014

Nearly 80% of Internet users in India use a mobile device for accessing Internet. Therefore, it is important that adequate spectrum and enabling policies for mobile services is put in place.

In the following paragraphs, each of these policy issues is briefly discussed to highlight the institutions, actors and processes involved in the Infrastructure Tier. Since the targeted audience of this paper is presumed to be aware of existing governance mechanisms, the institutions and instruments have been summarised in 'Annexure 3 – Institutions and Instruments' and excluded from the main text. For each of these policy issues, recommendations and a critique of the governance mechanisms is presented.

1. Licensing and Spectrum Management:

   The instruments and institutions involved in the tier are reviewed in 'Annexure 3 – Institutions and Instruments' (10.3.1).

   Recommendations:

   - *It is recommended that the government create a National Spectrum Committee under the PMO or as an autonomous agency for spectrum management to facilitate coordination between different ministries and address the issues identified above. The current structure of Wireless Planning and Coordination Commission (WPC) under DoT has created problems for coordination across ministries. Further, there is lack of perceived legitimacy both across government and private operators. For the private sector, the concerns have been inability of DoT to make more commercial spectrum available, restrictive guidelines regarding unlicensed bands and creating an enabling environment for trading and sharing of spectrum.*

2. Interconnection:

   The instruments and institutions involved in the tier are reviewed in 'Annexure 3 – Institutions and Instruments' (10.3.2).

   Recommendations:

   - *It is recommended that NIXI's mandate be revised to allow interconnection with CDNs and foreign ISPs.*
   - *It is recommended that NIXI's tariff and routing policy be revised to incorporate industry concerns.*
   - *It is recommended that NIXI undertake organizational restructuring of NIXI and become independent of DeitY (Jain, 2012).*

3. Standards:

The instruments and institutions involved in the tier are reviewed in 'Annexure 3 – Institutions and Instruments' (10.3.3).

Recommendations:

- *The government/DoT should actively support participation and contribution by the Indian technical community in SDOs like Telecommunications Standards Development Society, India (TSDSI), 3GPP and IEEE.*
- *TSDSI should be actively supported to develop standards and specifications for India specific environment and needs.*
- *Standards and specifications created by TSDSI should be kept open for redistribution and reproduction to increase proliferation of these standards in the Indian academic and technical communities.*
- *The multi-lateral approach suggested largely by the DoT towards standardisation be reviewed with the TSDSI, DeitY and other stakeholders in the context of the issues discussed and a coherent Indian position on this should be articulated.*

4. Access

The instruments and institutions involved in the tier are reviewed in 'Annexure 3 – Institutions and Instruments' (10.3.4).

Recommendations:

- *The definition of broadband needs to be increased to 2 Mbps by 2015 in line with international norms and as envisioned by NTP 2012.*
- *Private participation should be increased in the National Optical Fibre Network (NOFN) by way of auctions to the most competitive bidder. There is a need to coordinate with a variety of infrastructure ministries departments, such as highways, roads, water, bridges to coordinate Right of Way (RoW) and laying of fibre optic cables.*
- *The Cyber Café Rules of the Information Technology Act be liberalized for reducing regulatory compliance costs for provision of WiFi Hotspots.*
- *A plan for the wireless access network needs to be simultaneously finalised to ensure access feasibility and allow rural citizens to use their mobile phones. Indian government should explore working with companies such as Facebook and Google for innovative technologies such as drones for last mile access.*

Summary: Analysis of the Infrastructure Tier demonstrates that functions, processes, actors, and institutions involved in the policy process in this layer are primarily domestic. Therefore, international governance mechanisms should not be the sole focus of all debates on Internet Governance; ***the debate should also simultaneously focus on domestic governance mechanisms.*** The analysis of this layer raised significant issues related to spectrum management, strengthening of NIXI, facilitating web hosting domestically, accelerating broadband deployment in rural areas. An appropriate handling of these will allow greater proliferation of Internet in India. This will give it the legitimacy to influence global Internet Governance and provide a firmer basis to participate in the other layers of Internet Governance identified in the framework.

6.3 Critical Internet Resources Tier

Policy issues in the Critical Internet Resources Tier relate to allocation of IP/AS numbers, management of the domain name system, including root name servers, and development of protocols and standards. The governance mechanisms in this tier are largely international or transnational. There are well established processes, primarily bottom-up, for governance in this tier. ***The institutions and instruments involved in the tier are summarised in 'Annexure 3 – Institutions and Instruments' (10.3.5).***

The Infrastructure Tier in India interfaces with the Critical Internet Resources Tier primarily through the NIXI. NIXI, at the time of incorporation in 2003, was only supposed to be an Internet Exchange (IX) for interconnecting private ISPs to save international bandwidth. In 2005, the Registry (.IN) function for India's ccTLDs was additionally given to NIXI. In 2012, the NIXI was made a NIR (IRINN) under the APNIC RIR for allocation of numbers (IP and AS). NIXI also manages the F, I and K root servers in India. In 2014, NIXI also became the registry for additional IDN ccTLDs using the bharat IDN strings. Despite the increased responsibility of NIXI and its control over CIR relating to India, NIXI's organizational restructuring has got little attention so far (Jain, 2012).

At the regional level, India participates in the numbering community of the CIR Tier through the APNIC RIR. The APNIC RIR has an Executive Council (EC) that serves as the governing board of APNIC. The APNIC EC is selected by way of voting. The votes allotted to members are in proportion of the IP addresses held by them. For example, if the IP holding is up to /22, the member has 2 votes; and if the IP holding is between /13 and /10, then the member has 32 votes[46]. This system creates a bias in favour of incumbent members who have grandfathered large IP holdings and penalises those members who are using IP addresses efficiently (for example by using

[46]www.apnic.net/publications/media-library/documents/membership/tiers-and-voting-rights, accessed on October 20, 2014

Network Address Translation) and also penalises the community that is yet to connect to the Internet. This bias is reflected in the statistics that Eastern Asia (including Japan) holds 2,712,098 of the IPv4/24 addresses while South Asia (including India) holds only 170,365 of the IPv4/24 addresses[47]. In stark comparison, in the NRO EC voting, every member who has attended an APNIC Conference has only 1 vote. While India has had a representative on the NRO EC for the past several years, India has managed to gain representation on the APNIC EC only once till date. Notably, the APNIC EC has remained almost unchanged for almost a decade[48].

At the international level, India's participation in ICANN, through its various Advisory Committees, Supporting Organizations (SO) and User Constituencies (UC), is summarised in 'Annexure 2 – India's Participation in I* Organizations'. This summary reflects that India is under-represented in the decision-making bodies of ICANN.

India's participation in the other operational communities like IETF is also poor. For example, out of around 6700 RFCs created by IETF till now, only 72 RFCs (around 1.07%) have come from India; out of the 15700 authors in IETF, only 67 authors have come from India; and there has never been anybody from India who has been a Working Group Chair or Area Director in IETF[49].

Currently, pertinent issues in this layer are the new gTLD applications, standards, IPv6 and IANA transition. In the following paragraphs, a few of these policy issues are briefly discussed to highlight the institutions, actors and processes involved in this layer.

- New gTLD Applications: The new gTLD program is an on-going process for adding new gTLDs to the root zone. There is no proposed cap or limit to the number of new gTLDs. The new gTLDs applications are categorised into four types: generic TLDs, community TLDs, geographical TLDs and brand TLDs. The first round of applications for new gTLDs was opened for a duration of approximately three months in 2012 and these applications are currently being processed by ICANN. Out of the total 1930 applications received, only about 20 have come from India. As a result, India is currently able to capitalise only a limited amount of the economic potential of this new resource.

  The new gTLD applications have raised numerous policy related issues. For example, registration of the .amazon by the e-commerce company Amazon has

[47] www.apnic.net/publications/research-and-insights/stats/ipv4-sub-regions, accessed on October 20, 2014
[48] www.apnic.net/about-APNIC/organization/structure/apnic-executive-council/ec-members/past-ec-members; http://www.apnic.net/about-APNIC/organization/structure/apnic-executive-council/ec-members, accessed on October 20, 2014
[49] www.arkko.com/tools/docstats.html,accessed on October 20, 2014

been issued an early warning by the GAC as it would prevent the use of the gTLD for building awareness about the Amazon biome and rainforest, situated mostly in Brazil and Peru. The GAC warning is not binding on the ICANN board and only requires it to manually review the application. Similarly, India has issued early warnings through the GAC for the use of .bible, .islam, .halal and .ram, which have possible religious implications. Surprisingly, India has not raised an early warning for the use of .shriram. Whereas .ram could possibly refer to random access memory in computers, .shriram is definitely a reference to the god Ram. India has also issued a warning for .shiksha and .indians. Interestingly, India has not issued a warning for .yoga, which has now been auctioned to private company. While most generic TLDs will be open to registration by any person for a second level domain, there are many closed generic TLDs that have also emerged. In these closed generic TLDs, the applicant for the TLD will be the sole registrant for second level domains. For example, Amazon has applied for .book as a closed gTLD.

- IPv6 Transition: IPv4 addresses are nearing a point of exhaustion and transition to IPv6 is an essential need of the hour. IPv6 extends the addresses bits to 128 bits from the present 32 bits in IPv4, thus creating a larger pool of addresses. The growth of M2M devices and increased Internet penetration in emerging economies has further accelerated the depletion of IP addresses. The Government in India, in with guidance from APNIC, has been planning for a seamless transition to IPv6. In 2010, India released the National IPv6 Deployment Roadmap in which it chalked out a strategy to deal with the transition[50]. In line with this roadmap, an IPv6 Task Force was constituted to oversee the transition. As per the roadmap, all major ISPs and all government services were to become IPv6 compatible by 2011 and 2012 respectively. As of 2013, only 6 of the 22 major ISPs have become fully ready[51]. Only 4% of Autonomous System Numbers (ASNs) belonging to Indian networks are sending and receiving IPv6 traffic. Further, only 15% of Central Government websites are IPv6 complaint. These indicators imply that India needs to hasten the process to deal with IPv6 transition. Managing a faster or a time bound deployment is purely a domestic governance issue.

- Standards: Standards for the Internet usually refers to the standards for the CIRs. Important considerations in this dimension are the ability to create specifications of high quality, need to consider interests of stakeholders, developing wide spread consensus, and evaluating the efficacy of the proposed standard for the Internet community. These aspects are best handled through representation of a variety of stakeholders (governments, civil society, academia, private sector), seeking inputs

[50]www.apan.net/meetings/India2011/Session/Slides/IPv6/1-1.pdf,accessed on October 20, 2014
[51]https://www.apnic.net/__data/assets/pdf_file/0004/58981/2013-India-DOT-IPv6.pdf, accessed on October 20, 2014

at different stages of the standards process, open dissemination and evaluation of the standards.

Adoption of technical standards in this space has several public policy issues, sometimes referred to as techno-policy standards[52]. For example, the Society and Technical group in World Wide Web Consortium (W3C) has been constituted with people from diverse background such as lawyers, academicians etc. It's Platform for Internet Content Selection (PICS) initiative enables third party labelling of content for age-appropriateness. An example of technical standards addressing public policy issues is Digital Rights Management for copyright.

Internet standards have been developed largely at IETF, an all-volunteer body. This is an open membership body, with a number of working groups such as Global Routing Options, Energy Management, IPv6 Maintenance[53]. Members contribute as individuals and not as representatives of governments or enterprises. A diversity of representation and openness in process ensures that any one particular company's preferred standards do not prevail.

As highlighted in the earlier part of the paper, India's participation in IETF and other standards organizations is weak. There is little awareness regarding the functioning and participation mechanisms of several SDO in research and technical institutes. Several private companies in Europe and USA second technical talent to such R&D efforts. In India, there has been little visibility as R&D is a very small part of the very few Indian manufacturing companies. Given their small size and relatively lower revenues, Indian equipment manufacturing companies do not have the capacity to participate in such activities.

- IANA Transition: On 14th March 2014, the United States Commerce Department's National Telecommunications and Information Administration (NTIA) announced that it would be transitioning out of the stewardship role that it currently plays in the coordination of the Internet's DNS[54]. Specifically, NTIA announced its intent to transition its role to the global multi-stakeholder community. Currently, NTIA acts as the steward of the DNS due to its position as the *contractee* of the IANA functions and the Root Zone Manager (RZM) functions. It requested the ICANN, the current contractor of the IANA functions, to convene global multi-stakeholders to develop a proposal to transition the role played by NTIA.

[52]http://www.jthtl.org/content/articles/V11I1/JTHTLv11i1_MulliganDoty.PDF, accessed on October 20, 2014
[53]https://datatracker.ietf.org/wg/, accessed on October 20, 2014
[54]www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions, accessed on October 20, 2014

NTIA put forth certain preconditions for the transition proposal. It stated that the proposal must:

- "Support and enhance the multi-stakeholder model;
- Maintain the security, stability, and resiliency of the Internet DNS;
- Meet the needs and expectation of the global customers and partners of the IANA services; and,
- Maintain the openness of the Internet"[55].

NTIA very clearly stated that the proposed new organization would not be intergovernmental or government led. It set the forthcoming ICANN's IANA contract expiry date (30th September 2015) as the deadline of for the consideration and implementation of the proposal.

The transition announcement was possibly triggered by the Snowden revelations and the subsequent announcement of NETmundial conference by the Brazilian Government[56]. As per the NTIA, it was always the intent of the US Government to transition its role to the global multi-stakeholder community as the final phase of the privatisation of the DNS that it announced in 1997[57].

In the current debates over Internet Governance, there is a scope for India to get involved at the highest level. Currently India doesn't have any significance or well laid out plan for participating in the transition

***Recommendations**:*

- *At the international level, actively participate in the bottom-up policy development processes of Generic Names Supporting Organization (GNSO) and CCNSO of ICANN, and the IETF through Working Groups.*
- *At the regional level, India should strengthen participation in APNIC through executive positions in the APNIC EC and the NRO EC. This may require initiating bottom-up policy development processes for revising the APNIC EC election framework.*
- *At the domestic level, India should enhance the accountability of NIXI (which manages India's Critical Internet Resources) towards India's strategic goals by introducing an oversight mechanism and undertaking an organizational restructuring.*

[55] ibid
[56] http://www.circleid.com/posts/20140723_ntia_foia_disclosures_limited_light_on_iana_transition_decision/, accessed on October 20, 2014
[57] www.ntia.doc.gov/other-publication/2014/myths-and-facts-ntia-announcement-intent-transition-key-internet-domain-name-, accessed on October 20, 2014

- *DeitY should awareness building and information sessions around the implications of new gTLDs for business and economy on the Internet.*
- *There should be a systematic process and a dedicated group within DeitY that examines issues regarding gTLDs from a legal and business perspective.*
- *TRAI should monitor transition to IPv6 within a specified time frame. This should be arrived at in consultation with the industry.*
- *India needs to play a more significant role in the Regional Internet Registry managed by APNIC. There should be a concerted effort from the DoT and DeitY to have a coherent approach to play a significant role in the APNIC and to support Indian ISPs to have a greater role in such bodies.*
- *Indian government needs to create programs for awareness building in engineering and technical institutes regarding the functioning, process and benefits of participation in standard setting.*
- *Indian government needs to create programs and strategies for formally participating in the IANA transition.*

6.4 Service Tier

This tier primarily deals with formal and informal institutions that have developed for dealing with cyber-security, surveillance, spam, malware, botnets, denial of service, etc. It is important to have a framework for addressing cyber-crime (spam, botnets, and exploiting security vulnerabilities) as it provides an enabling environment for business on the Internet. The growing economy around Internet highlights the imperatives for such an approach.

In the Internet domain, it is not sufficient to have a domestic law on cyber-crime as the crime may involve entities (people, servers) in other national jurisdictions. Therefore, it is important to have treaties so that there is involvement of a number of countries in the development of a domestic framework for cyber-crime. In general, private sector investments move towards those environments that provide stability and a sound legal framework. This creates a virtuous cycle of innovation and a growing economy. Further, cyber-crimes are increasingly seen as undermining of human rights. Countries that uphold the value of human rights would need to address issues in cyber-crime.

Vulnerabilities in cyber-security could lead to attack on national assets and hence managing them is integral to national security. Due to the global nature of the Internet, national cyber-security issues are not limited to domestic boundaries but have important international implications. Currently, in the context of international cyber-security there are no formally agreed upon definitions or treaties and there is little chance of applying traditional arms control regimes to cyber-space. Retaliation is often difficult in cyber-space, due to the inherent problems in attribution. Such concerns are compounded by the perspective that malicious cyber-activities could result in a conventional or a nuclear military attack.

On the other hand, challenges in implementing a cyber-security framework is the extreme difficulty of integrating any verification software into a treaty. This is because recognizing such software is extremely tough without a detailed and through analysis of affected computer systems for which no state is likely to agree. No government is likely to agree to an analysis of its domestic, including government computing resources from an external source. Further, non-state actors, who are outside the purview of state control and regulation, could play a role in violation of cyber-security. On another dimension, states may support developments of applications/software for cyber-security driven by the need to have mechanisms for disruption of opposition forces.

There has been little consensus at the international level on treaties and agreements regarding cyber-security. One of the strands of differences among countries has been the perspective and balance between security and civil liberties. While several western states explicitly espouse the aspect of openness of Internet for the free flow of information, promotion of human rights and close international cooperation and information sharing for law enforcement, other states, notably Russia, China, Iran etc., emphasize states sovereignty and territorial integrity as the framework for cyber-security.

Nations have used both formal and informal institutions to address cyber-security concerns.

Formal Institutions

There are few states that have established or announced publicly available cyber-security strategies. A European Defence Agency study of 2013[58] indicated that most countries do not have a mature cyber-security or defence strategies. The key initiatives are elaborated below:

Council of Europe Convention on Cybercrime

As of the present date, ***Council of Europe Convention on Cybercrime*** or the Budapest Convention on cyber-crime is the most widely available and accepted multi-lateral[59] treaty which has 44 members who have ratified/acceded to date. Besides European countries, these include Japan, Australia and USA. Nine countries have signed but not ratified. Several others, like India have used it as guideline for

[58]http://www.eda.europa.eu/info-hub/news/2013/05/24/eda-study-identifies-cooperation-prospects-in-cyber-defence, accessed on December 6, 2014

[59]Multi-lateral here refers to the fact that multiple countries were involved. This needs to be differentiated from the concept of multi-lateralism as understood in the UN system, where all countries are members.

domestic regulation. The Annexure in Section 10.4 gives the correspondence between the IT Act, 2008 in India and the Budapest Convention.

The Budapest Convention is the first international treaty covering cyber-crime prevention and criminal justice seeking to harmonize national substantive and procedural laws related to cyber-crimes. The Convention also seeks to improve investigative techniques and increase cooperation among participating nations. It provides uniform definitions for infringements of copyright, computer-related fraud, child pornography, hate crimes, and violations of network security. It also provides a series of powers and procedures for lawful interception both through formal and informal mechanisms.

It has increased its scope over the years. For example, in 2003, a protocol on xenophobia and racism committed through computer systems and in 2012, work began on solutions to trans-border access to data in a cloud computing platform. It also has the scope to increase its membership. While it was prepared by the member states of the Council of Europe, Canada, USA, South Africa participated in its negotiations. Additionally, Council of Europe provides support for tools on "enforcement/service provider cooperation, judicial training, cyber-crime strategies" (Seger, 2011). As the convention is technology neutral, there is scope to incorporate features that emerge from new technologies. The that there could be different positions on aspects related to freedom of speech, it was put in a separate protocol, so that depending on their national priorities, countries could join the protocol separately.

It appears that the process of building on the treaty and its gradual roll-out has been more effective than attempting to draft a comprehensive agreement covering all aspects. The Convention has led to harmonization across the countries that have acceded to it. The UNGA has supported the Convention as a benchmark for member countries to evaluate their domestic legal frameworks for covering cyber-crimes. Several countries have reported increased cooperation and support for prosecution from other signatory members. Since any new and meaningful treaty would take significant period of time (nearly 15-20 years, 3-5 years for countries to agree that negotiations should start, 3-5 years to negotiate, and 5-10 years for sufficient number of parties to sign to make it operationally effective), in the current scenario, the Budapest Convention appears as the relevant platform for harmonization of cyber-crime related aspects of Internet Governance.

Other Initiatives

- While there have been other attempts to address the issue of cyber-security at an international level, (as for example, arms control treaty as an agreement to limit the risk of cyber-conflict in 1998 by the Russian Federation), these have been mostly sporadic. The more recent interventions, in 2011 have been the proposals

by China, Russia, Tajikistan and Uzbekistan as a part of the Shanghai Cooperation Group 'in the form of a potential [UN] General Assembly resolution', an *International Code of Conduct for Information Security*. The draft refers to the non-proliferation of 'information-weapons', and the role and responsibilities of state actors in usage of ICT for peaceful purposes. These have been based on *The Shanghai Cooperation Organization*'s documents and resolutions (SCO Member Countries Action Plan to Safeguard International Information Security, 2007[60]) and revised in subsequent years.

- In September 2011, the Ministry of Foreign Affairs of the Russian Federation introduced a proposal for an international agreement called The *Convention on International Information Security (Concept).* This document articulated the concept of information security, warfare, weapons and terrorism in cyber-space in the context of international security. India has opted for observer status in this forum.

- In 2007, the ITU had launched the Global Cyber-crime Agenda where the international response to cyber-security could be coordinated. Subsequently, UN Office on Drugs and Crime signed an MoU with ITU for developing capacity, especially in the area of crime prevention and Cyber-security. The UN established Working Groups to recommend inter-alia, *"best practices, technical assistance and international cooperation with a view to examining options to strengthen existing and to propose new international responses to cyber-crime"*[61]. These recommendations were reviewed and adopted by various UN institutions dealing with crime prevention with criminal justice (UN Resolution 65/230).

- Various working groups have been recommended and set up to examine the aspect of cyber-crime such as Cyber-crime Legal Working Group of the EastWest Institute[62]. Among the recommendations has been the setting up of an International Criminal Court or Tribunal for Cyberspace, Creation of a treaty on cyber-security, establishing a law on international cybercrimes that provides for prosecution in the proposed International Criminal Court on Cyberspace, under the UN system. The existing International Criminal Court could be extended to cover the cyber-crime aspects.

- Existing international organizations such as the INTERPOL are strengthening their existing operational platforms to deal with cyber-crimes. For example the INTERPOL Global Complex, Singapore will develop state-of-the-art tools for combating cyber-crime.

[60]http://www.cybercrimelaw.net/SCO.html, accessed on December 11, 2014
[61]http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, , accessed on January 15, 2015
[62]http://www.cybercrimelaw.net/Cybercrimelaw.html, accessed on December 6, 2014

- Commonwealth Cybercrime Initiative (CCI) is an initiative created under the Commonwealth Connects program to bridge the digital divide. The Commonwealth Model Law on Cyber-crime and Harare Scheme for Mutual Assistance may be considered as a viable alternative to the Budapest Convention. The Model Law is largely compatible with the Budapest Convention. The Harare Scheme is a non-binding, constructive approach to mutual cooperation within Commonwealth countries. While the Commonwealth Expert Report[63] stated that "Commonwealth countries should be encouraged to accede, where practicable, to the Budapest Convention", they have the freedom to not work with the Budapest Convention and yet have an internationally accepted cyber-crime framework.

Informal Institutions

Under informal institutions/processes we examine loosely governed informal processes, confidence building measures and political declarations.

Informal Processes: When examining the international institutional design and processes for cyber-security, it is important to take into account the role of the informal operational networks and interpersonal relationships. The loose but effective networking between a variety of actors such as CERTs, ISPs, governments, hosting companies, experts have addressed significant security challenges (Mueller, et al. 2013). Such incidents require quick response, as threats could magnify if action is delayed. Addressing such threats may require knowledge embedded in variety of groups or computing resources under their control. While government organizations may be a part of such networks, there is no hierarchy and such functionaries operate and receive collaboration based on their legitimacy of their expertise or know-how. However, if such issues were to be treated within the framework of treaties, then the formal processes may take long and may not always provide access to the requisite resources.

Confidence Building Measures (CBMs): These are instruments that are used in traditional international politics for prevention of outbreak of war and de-escalation of crisis but are difficult to implement in a cyber-framework[64]. Currently, only a few

[63]"The Commonwealth and the Budapest Convention" by Jarvis Matiya, presented at the International Conference on #Cyberlaw, #Cybercrime &#Cyber Security, November 20, 2014, New Delhi

[64]http://www.ccdcoe.org/publications/CBMs.pdf) CBMs for cyber-space will display the nature of political commitments. Political declarations of States are a powerful tool of international relations. Importantly, they are significant for the progressive development of international law, especially within the realm of 'general principles of international law', which establish (in an abstract and general manner) several obligations of States, which are partly addressed by the existing sets of (draft) CBMs for cyber-space. A political commitment to CBMs for cyber-space concluded at a regional, or broader, international level, will support the concretisation of the respective general principles of international law, and thus establish their obligatory nature in terms of applicable 'hard law'.

international treaties can be deemed as reflecting measures as enclosed in the sets of (draft) CBMs for cyber-space.

As an example of a concerted approach to development and implementation of CBMs, the Organization for Security and Co-operation in Europe (OSCE) has developed a set of CBMs, through its Informal Working Group in a multi-stakeholder process.

Political Declarations: These are powerful tools of international relations, which can have de facto binding character (good faith, estoppel). Furthermore, the political discourse within the international community can support the development of international customary law by facilitating the evolvement of opinion juris, which is (beside State practice) a constitutive aspect of international custom.

"For the politico-military dimension of cyber-security a different solution may need to be negotiated in the coming years, possibly in the form of principles of state behaviour in cyber-space as discussed for example by the OSCE38 or in forums such as the London Conference on Cyber-space"[65]. Recognizing the role of military dimensions of cyber-security, there is a need to train large numbers of armed forces to address this aspect. For example, the USA military has created Cyber Mission Forces of 6,200 soldiers and civilians. Similarly, the Air Force has also stepped up its cyber training capacity, both in numbers and the level[66].

India needs to take initiatives in participating in these conventions and formally examine the role of cyber-security in its armed forces, evaluate the quantitative and qualitative resources required to address its security needs and develop a strategic plan for addressing its cyber-security concerns.

India's View

The erstwhile Minister for MOCIT, Mr Kapil Sibal had stated in October 2013:

> *"India will neither go with the inter-government committee of the UN, which is advocating government control over the internet, nor with the Internet Governance Forum, which favours private sector control over the net"*[67].

[65]"The Budapest Convention on Cyber-crime 10 years on: Lessons learnt or the web is a web", by Alexander Seger, Head of Data Protection and Cyber-crime Division, Council of Europe. (Based on the presentation made in Session IV (New national and international legal responses to cyber-crime) at the International Conference on Cyber-crime: Global Phenomenon and its Challenges organized by ISPAC/CNPDS/Courmayeur Foundation/UNODC/KIC in Courmayeur Mont Blanc, Italy, 2-4 December 2011

[66]http://www.politico.com/morningcybersecurity/1114/morningcybersecurity16254.html, accessed on December 6, 2014

[67]http://www.governancenow.com/news/regular-story/india-wont-sign-budapest-pact-cyber-security#sthash.HgHxvqv6.dpuf, accessed on October 15, 2014

However, he did not specify what India would do. Given the international dimension of cyber-security on the Internet, it is important for countries to collaborate. The fact that the Budapest convention had only a few countries initially architecting it, and India was not a part of it has been one of the factors in India not viewing this as a possible approach to handling the issue of transnational cyber-crime.

India's concern is that the Committee of Ministers has a formal role in adopting protocols or amendments. The rationale for participation despite this aspect is that all protocols and amendments would need to be adopted by all parties. Thus, the Council of Ministers cannot decide something that would be binding on India without its consent. From the Indian government's perspective, an inter-governmental body with significant inputs from India may have been an ideal place to start with, the pragmatic approach may be to start with the existing convention and get involved in making changes where required. As the Budapest Convention offers an existing and functioning framework, India (or any other country) could contribute to future processes, protocols and technologies (cloud, M2M)[68]. Further, this treaty does have support from a large number of countries that cover significant percentage of Internet users. With more countries adopting it, the treaty regime could become stronger.

An advantage of joining an established Convention on cyber-crime is that it spurs FDI as it gives comfort to investing companies that there is an enabling legislation. Further, becoming a part of the Budapest Convention will ensure that our domestic framework for cyber-crime is informed by the best practices that have evolved as a part of the Budapest Convention. This is so for two reasons: first, the Budapest Convention has evolved with the inputs received from the member countries and second, it requires that signatory countries have an adequate framework domestically that is compatible with it. The Budapest Convention requires that at the time of accession or ratification of the signatory country, it must have the appropriate laws in place. When a country makes a request to ratify the treaty, an assessment of the current situation vis-à-vis the legal framework for cyber-crime is made. Assistance is provided to draft a law and ratification is considered when at least a draft law is in the parliament. The Convention provides for both formal and informal cooperation, thus giving flexibility for implementation.

An example relevant to India is the process used by Sri Lanka to leverage the Budapest convention. As a country that wished to promote itself as the preferred destination for services in the sector, it decided to seek accession to the Budapest Convention. There was active involvement of all stakeholders, including the private sector. It helped them to access the best practices on data privacy and data protection.

[68]In January 2012, the Cyber-crime Convention Committee started its work on transborder access and jurisdiction.

For India, working with a more contemporary definition of multi-lateralism (elaborated in Section 5) with a view to participate in new forums that have been created for addressing international cyber-security issues would be justified. For such participation to be effective, it should include private sector expertise in its representation. India's concerns can be met by taking initiative, investing time resources and efforts, participation, agenda setting, developing best practices domestically and creating platforms for discussion and debate to feed into the policy making. India's approach to advocating a multi-lateral approach should deliberate on the contours of different aspects of processes and decision making within the framework outlined above. Adoption of such an approach could be based on India's prior experience in a related field such as the Financial Action Task Force (FATF) and experience of other emerging economies in joining the Budapest Convention.

India's experience of joining the Council of Europe/ Organization for Economic Co-operation and Development (OECD) treaty on cooperation in tax matters[69] and the FATF, a relatively new inter-governmental, policy making body shows how a more proactive approach from the Indian state led to it participating in a cutting edge international organization and the consequent up gradation of capabilities and adoption of best practices domestically. The FATF objective is to combat money laundering, terrorist financing and maintain integrity of the international financial system. It was established in 1989 by the Ministers of its Member jurisdictions.

The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures to achieve its objectives. The FATF Recommendations are treated as a set of harmonized measures across states that support co-ordinated response. "The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In collaboration with other international stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse"[70].

Starting as an initiative of G7, FATF today has 36 members. Its charter and objectives are analogous to those in the Budapest Convention, as are its processes. India took the decision to join the FATF and made adequate preparations to qualify to be a member. Until India was able to adopt internationally accepted regulatory processes, it could only be an observer. A subsequent review of progress made by it, and India's satisfactory compliance with the benchmarks of FATF, allowed it to join as a member. A similar approach to adopting the Budapest Convention and seeking

[69]http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=208&CM=8&DF=27/11/2014&CL=ENG, accessed on October 27, 2014
[70]http://www.fatf-gafi.org/, accessed on October 27, 2014

ratification would help India to not only be a part of a global team in addressing cyber security but also help it to achieve best practices domestically. The Plenary of FATF, the decision-making body of FATF, provides space for private sector participation through consultative meetings.

Another driver for India (or any other country) to joining an existing organization is that any mechanism that is designed afresh will take a few years to get established and until then India (or any other country) would have a platform to address its security concerns within the existing organizations.

Summary: Participation in the international forums and influencing specific treaties and developing CBMs is important for India. This is specially so for the security and national sovereignty aspects. Since cyber-security has ramifications beyond countries that may be involved on specific issues with another country/countries. It is important that India's participation should be wide. By participating in established treaties, India will become a part of a process where established cyber-security frameworks could be leveraged to strengthen our own cyber-security as well as help us to influence future directions in line with our national priorities. Prior experience of other countries such as Sri Lanka and in other sectors such as FATF could be a basis for working on a cyber-security framework for India. Further, by taking initiatives in areas such as CBMs will help to establish robust infrastructure and processes for strengthening cyber-security.

Recommendations:

a. *Strengthen the JWG to ensure that its outcomes are implemented.*

b. *Develop human capacity for understanding the legal and technological issues related to cyber-security. This should be done for executives in the government departments listed above. These should be joint sessions so that the participants get a holistic perspective. At another level, government could support launch of relevant courses in technological, management and law schools.*

6.5 Content and Application Tier

This tier comprises of policy issues arising from content and applications such as privacy and data localisation, intermediary liability, e-governance, local language content etc. The actors involved in this layer range from large internet mammoths like Google and Facebook to individuals developing apps and content on their own in their free time. The government also plays an important role in provision of e-governance services.

Harmonisation in this tier may emerge in a bottom-up manner as *best practices* which are incorporated into national legislations; or in a top-down manner in which the UN recommends a model law, which is voluntarily adopted into national legislations.

A few of the policy issues are briefly discussed to highlight the institutions, processes and actors involved in this layer:

- *Privacy and Data Localisation*: India should harmonise the procedures as substantive policy issues vary from country to country and therefore harmonisation is difficult and contentious. Online privacy in India is presently dealt with under Section 43A of the Information Technology Act (ITA). The Section requires corporate bodies that possess, deal or handle any kind of sensitive personal data to implement reasonable security measures. The Justice AP Shah Report outlines the important principles required for new privacy legislation in India[71]. The Department of Personnel and Training has released a draft legislative bill in 2014[72], which is presently under consideration and consultation.

  Since India does significant outsourcing work for EU and US, any data privacy legislation must take their frameworks into account. The EU introduced major reform in 2012 to the legal framework for protection of personal data. This standard is unfortunately significantly different from that in the United States. India would need to take cognizance of the same.

  Many countries such as Brazil have introduced data localisation requirements to deal with security and surveillance threats. India had made ad-hoc executive decisions in this regard. Notably, Blackberry was singled out in 2012 to install servers in India and to enable data decryption. Further, despite a policy directive for use of NIC emails for official purposes, many government officials send/receive formal emails from their Google, Yahoo or similar email applications.

  - *It is recommended that since most of the data centres reside in the United States and Europe, efforts need to be taken to harmonise privacy regulations with these two jurisdictions.*
  - *It is recommended that DeitY and DoT actively monitor and enforce the use of NIC emails for official government communications.*

[71]http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf, accessed on October 27, 2014
[72]http://articles.economictimes.indiatimes.com/2014-02-18/news/47451233_1_personal-data-privacy-bill-draft-bill, accessed on October 27, 2014

- *Intermediary Liability*: Intermediary liability is presently governed by Section 79 of the Information Technology Act[73]. A notice-and-takedown regime has been created for limitation of intermediary liability. The Section and its Rules thereunder have been under considerable challenge, including writ petitions before the Supreme Court of India, for having a chilling effect on free expression.

    - *It is recommended that the Intermediary Guideline Rules 2011 be reviewed and revised by way of in-depth open stakeholder consultations. The Intermediary Liability regime should be liberal such that it encourages service providers to host data domestically in India.*

- *E-Governance*: E-Governance is presently planned under the National E-Governance Plan (NeGP). The NeGP creates various central, state and integrated Mission Mode Projects while creating state-wide networks and data centres. While a few projects have been successful, their proliferation at citizen level requires changes in government process, laws and modes of delivery.

    - *It is recommended that all government sites be mobile enabled.*
    - *It is recommended that regular audit and monitoring of all existing e-governance services be carried out to ensure minimum service levels.*

- *Local Language Content*: Presently, very little content is available in the local vernacular languages of India. As a result, citizens not fluent in English have little incentive to use the Internet. For example, the number of Wikipedia pages in English is nearly 4.7 million (mn), number of page views per hour is 10.61 mn and content editors is 21 per mn speakers on a speaker base of 1500 mn. The corresponding numbers for Hindi are 0.10 mn (content articles), 0.02 mn (page views per hour) and 0.10 per mn with a speaker base of 550 mn. An examination of Table 1shows that in comparison to other languages, such as Portuguese with a lower speaker base (290 mn) the data for above dimensions shows far lower values for Hindi. Normalizing these values with respect to English language (columns 8, 9, 10, 11 in the Table below) we see that the ratio of English contributors per mn speakers in relation to China is 21.0 while that for Hindi is 264.0. This shows that although China has 21 times less contributors per mn speakers in relation to English, for Hindi it is 264 times lower contributors. The analysis in the table shows similar statistics for Usage views per hour and content article count. Although this data is for Wikipedia pages, it highlights the need to focus on local language development. It also shows that India is far behind countries like China and other developed countries. The data for China needs to be seen in the light of the extremely large market share of indigenous Chinese

[73]http://cis-india.org/internet-governance/resources/section-79-information-technology-act, accessed on October 20, 2014

language search engine and “Wikipedia” Baidu, due to which these statistics are likely to be lower for the Chinese language.

Table 2: Wikipedia Statistics (August 31, 2014)

	1	2	3	4	5	6	7	8	9	10	11
Languages	**Prim.+Sec. Speakers** *(mn)*	**Editors** *(per mn speakers)*	**Usage Views per hour** *(mn)*	**Content Article count** *(mn)*	**Contributors** *(mn)*	**Usage Views per hour** *(per mn speakers)*	**Ratio of English Usage Views per hour per mn speakers in relation to other languages**	**Content Article count** *(per mn speakers)*	**Ratio of English Content Article count per mn speakers in relation to other languages**	**Contributors** *(per mn speakers)*	**Ratio of English contributors per mn speakers in relation to other languages**
English	1500	21.0	10.61	4.68	0.921	0.007071	-	0.003120	-	0.000614	-
Chinese	1300	2.0	0.87	0.78	0.038	0.000668	10.6	0.000597	5.2	0.000029	21.0
Hindi	550	0.1	0.02	0.10	0.001	0.000036	195.4	0.000188	16.6	0.000002	264.0
Arabic	530	1.0	0.14	0.32	0.013	0.000270	26.2	0.000595	5.2	0.000025	24.3
Spanish	500	8.0	1.45	1.12	0.097	0.002895	2.4	0.002247	1.4	0.000195	3.2
Malay	300	0.2	0.02	0.27	0.002	0.000068	103.3	0.000897	3.5	0.000006	100.8
Portuguese	290	5.0	0.54	0.84	0.039	0.001871	3.8	0.002894	1.1	0.000135	4.6
Russian	278	12.0	1.51	1.15	0.068	0.005446	1.3	0.004130	0.8	0.000244	2.5
Indonesian	250	2.0	0.15	0.35	0.007	0.000588	12.0	0.001390	2.2	0.000029	21.1
Bengali	230	0.4	0.01	0.03	0.001	0.000044	161.6	0.000139	22.5	0.000004	136.9
French	200	22.0	1.03	1.54	0.099	0.005174	1.4	0.007715	0.4	0.000497	1.2
German	185	32.0	1.23	1.73	0.151	0.006639	1.1	0.009339	0.3	0.000819	0.8
Japanese	132	29.0	1.39	0.93	0.082	0.010504	0.7	0.007049	0.4	0.000622	1.0
Persian	107	7.0	0.10	0.42	0.013	0.000939	7.5	0.003925	0.8	0.000121	5.1

Source: http://stats.wikimedia.org/EN/Sitemap.htm, accessed on October 17, 2014 and Author's Analysis

- *Local content generation needs to be actively supported. Chinese language search engine and "Wikipedia" developed by Baidu that became the first Chinese company to be included in the Nasdaq 100 index, has helped Chinese population to have access to local content. It handles more than 80% of online queries in China.*

- *The government should encourage provision of all e-governance services in vernacular languages wherever possible.*

- *Books in vernacular languages kept in national libraries should be digitised and made accessible online. Collaborations may be initiated with service providers like Google Books and Amazon Kindle to leverage their existing infrastructure. A plan for royalty sharing with authors of such books be introduced in line with established practices.*

- *Regulation of OTTs and Network Neutrality*: Network Neutrality refers to the absence of discrimination of Internet data on the basis of content or application by the Internet Service Provider and the Government. Currently, India does not have any Network Neutrality regulations. India has not put in place a clear roadmap and regime for over the top (OTT) providers like Skype and Whatsapp creating uncertainty in the market. There have been calls from a section of the stakeholders asking for the regulation of this sector and the Government is yet to take a clear stand on this issue. Proliferation of OTT services has raised the fear that non-neutral measures may be adopted by TSP/ISPs to deal with the rising threat of OTT services. Further, India is a mass market and should encourage app developers and content providers to develop localised content. On another dimension, a massive project to convert Wikipedia into regional languages could be started. This should be supported by the government, as it is a public good. This would make those involved (translators, reviewers), aware of the value of web content.

  - *It is recommended that the government bring certainty in the regime by taking a clear stand on the issue of OTT licensing and Network Neutrality.*

6.6 End User Tier

This tier deals with issues regarding capacity and awareness building, and regulating end user behaviour on the Internet. Issues in this layer are largely domestic. A few of the policy issues are briefly discussed to highlight the institutions, processes and actors involved in this tier:

- *Awareness and Capacity Building*: Awareness and capacity building deals with interventions aimed at removing barriers to knowledge that impede the proliferation of the Internet and its benefits. There is also a need to generate trust in the Internet and the services provided over it.

    - Awareness and capacity building can be achieved using training sessions in schools, colleges and through various other commercial training centres. Incentive structures should be created that encourage people to learn using the Internet. For this, funding for public schools and colleges to connect to the Internet should be provided.

- *Regulating End User Behaviour*: This deals with creating legislative provisions that regulate the behaviour of the end user over the Internet. For example, the end user needs to be discouraged from hacking, spamming, impersonating, squatting etc. Most of the issues about misuse of the Internet would be largely domestic due to local network effects despite the international interconnectivity of the Internet. (Additionally, the legislative framework will rarely find applicability or enforceability in foreign jurisdictions.)

  Issues in this layer are largely domestic and little international coordination is required. The Department of IT and Department of Telecom need to coordinate with the Ministry of Human Resources to encourage capacity and awareness building.

6.7 Summary

Based on the analysis of different tiers, we present Table 2 which shows the different tiers, the key issues, lead and other actors, and geographic scope of decision making. This helps in designing the appropriate models and actors for dealing with special issues regarding the Internet Governance.

Table 3: Key Issues, Actors and Scope for Internet Tiers

S. No	Tier	Issue	Leading Actors	Other Actors	Geographical Scope
1	Infrastructure Tier	• Licensing and spectrum management • Access	DoT, DeitY, TRAI, TSP/ISPs	Civil Society	National
		• Interconnection (IXP)	NIXI, DeitY, DoT, CDNs, TSP/ISP	Civil Society	National/International
		• Access Standards (Development)	Technical community (including equipment manufacturers and academia), TSDSI	Civil Society, DoT, DeitY	National/International
		• Access	DoT, DeitY, TSP/ISP	Civil Society	National

S. No	Tier	Issue	Leading Actors	Other Actors	Geographical Scope
		Standards (Adoption)			
2	Critical Internet Resources Tier	• IP/AS numbers	NIXI (DeitY), TSP/ISP	Civil Society, DoT	Regional/National
		• Names (DNS/TLDs)	Civil Society, MCI, Business community	DoT, DeitY	
		• Standards and Protocols	Technical community, DoT, DietY	Civil society	
3	Service Tier	• Security	DoT, DeitY, NSA, MHA and Technical community	Civil Society	National/International
		• Spam/Malware	Technical community and Informal networks	DoT, DeitY	National/International
4	Content and Application Tier	• Privacy • Intermediary Liabilities	Intermediaries (ISP/TSP/CSP etc.), civil society		National
		• Copyright	Copyright Office (MHRD), DIPP (MCI), Civil Society		
		• Network Neutrality	ISP/TSP, OTT, TRAI, Civil society	DoT, DeitY	
		• Interception • Blocking	DoT, DeitY, NSA, ISP/TSP, state police, civil society		
		• Data Localisation	NSA, civil society		National
		• E-governance • Local language content	state, district and village administrations, DeitY, Civil society, CSPs	TSP/ISP	Regional
5	End user Tier	• Capacity building • Awareness building	Civil society, MHRD, DeitY, State administration		Regional/National
		• Regulating end user behaviour (hacking, spamming, squatting etc)	Civil society		National/International

Source: Author's Analysis

7 The Recommended Approach – MTOP

Based on the analysis of the Multi-Tiered Framework, and taking into account the Perceived Legitimacy Framework (PLF) developed in the previous chapter, we recommend a Multi-Tier Open Participation (M-TOP) approach.

The Multi-Tiered Framework argues that there are different actors, institutions and processes at different tiers of Internet Governance; and therefore a different approach to Internet Governance is required at each tier (Refer Diagram in Section6.1). The PLF identifies the various parameters that contribute to the legitimacy of an Internet Governance process (Refer Section 5.3).

The M-TOP approach combines the Multi-Tiered Framework and the PLF developed by us. The M-TOP approach recognizes that there is no single approach to governance that is applicable across all tiers of Internet architecture, and the relevant public policy issues. Accordingly, the paper recommends that since models of governance at different tiers are likely to have diverse drivers, participants, processes and outcomes, India should adopt the M-TOP approach for all levels of Internet Governance: domestic, regional and international.

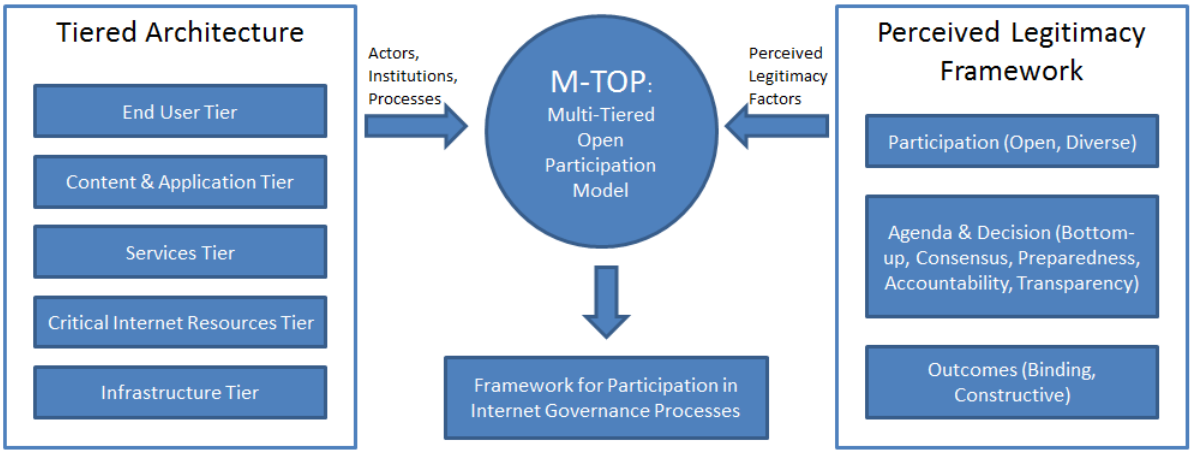

Fig 3: Framework for Internet Governance

The M-TOP approach recognizes that even when nation states need to be involved in decision-making, they need to adopt a multi-stakeholder approach for participation, agenda setting and decision-making and have outcomes that are likely to high adoption rates and be constructive. Any Internet Governance process should satisfy the legitimacy parameters enumerated below:

- *Open Participation*: All policy development processes should aim to be open in terms of including all relevant stakeholder groups, have wide representation including focus on emerging economies and gender, and overcome barriers emerging as a result of language, location, capacity and funding. We believe that different categories of

stakeholders will contribute to various issues and policy stages depending on their expertise. For example, while the technical community needs to take the lead on and represent India on issues of technical standardisation, the governments need to take the lead on and represent issues of cyber-security and cross-border capacity building for say, cyber-security and lawful interception. In this model, specific group of stakeholders may be assigned the role for implementation; the selected group would have to be accountable to all of the stakeholders for their decisions and implementations.

- *Agenda Setting and Decision-making Processes*: The agenda setting process should be bottom-up and include inputs from as many stakeholders as possible. There should be a mechanism to streamline the agenda to be as inclusive as possible. A consensus driven approach is recommended. The decision-making process should give adequate time and information to concerned participants to ensure higher level of preparedness. This can be facilitated by making such resources easily accessible.

  The decision-making processes need to ensure transparency of information. The process design should ensure that there is no capture by any dominant group and that the entity to be regulated has no role in influencing the decision-making process.

- *Outcomes*: Decision-making processes should produce tangible outputs with high adoption rates. Processes design elements or performance measures for outcome should include adoption rate.

  In areas such as cyber-security, both formal and informal institutions play a significant role. The recommended M-TOP approach embeds this aspect. For example, in the area where national sovereignty is critical, the government should take a driving role and ensure that its views are represented in international forums. However, domestically, it must seek support from the private sector and civil society for developing its view. Other area of governance space, where the government needs to take a lead role but with support from all stakeholders is in capacity building and awareness creation. Government needs to take a facilitating role in creating the suggested working groups, not necessarily be the driving member or heading each group.

  Thus, India needs to adopt a more nuanced approach as highlighted by adopting the M-TOP approach in the overall Internet Governance space at all levels: domestic, regional and international.

8 Summary and Recommendations

8.1 Summary

The WSIS process was instrumental in changing the dimensions of debate on the institutional framework on Internet Governance. While various stakeholders had dealt with issues related to Internet Governance in an opportunistic manner, the WSIS process created a common platform where these issues could be addressed. On another dimension, the WSIS deliberations created space for the governments to recognize the role of non-state actors in Internet Governance. Internet has given rise to a governance space that goes beyond traditional nation-state frameworks that existing frameworks deal with. The ability to deal with emergent issues in this domain requires flexibility of approach, keeping track of new technologies and international developments and how these may influence Internet Governance.

The analysis in the paper reveals that India's position on Internet Governance that recommends a multi-lateral approach has been ad hoc, inconsistent and at variance with emerging scenario globally. This approach has isolated India and as created a negative signal for investment in ICT. The rationale for the position has not been articulated. The focus of the position has been limited only to the international aspects of Internet Governance dealing largely with cyber-security, albeit a critical aspect, at the expense of economic and social goals domestically. Even in the domain of cyber-security, India has not articulated its position clearly. When it has recommended a multi-lateral approach, it has been isolated and grouped with countries that do not recommend a free and open Internet. This has led to concerns from the industry regarding future growth and investments in the country. While *India needs to leverage its growing Internet user base to influence the policies of private sector investment and trade on the Internet, it must do so through developing a strategic approach at the highest level, investing in R&D, and developing both end-user and institutional capacity.*

If India wants to play a dominant role in Internet Governance and leverage it to influence public policy issues to its advantage, then it needs to have a strategic perspective. For this, there needs to be *deliberation at the highest political and executive level*. Further, its position needs to be articulated through a due process characterized by consultation, openness, enhanced scope from its current limited focus, largely on cyber-security. It needs to focus more on participation in standardization, management of Critical Internet Resources, and IANA transition as an instrument to leverage a significant role for itself and other developing countries.

This paper develops a (i) Multi-Tiered Framework to identify the governance mechanisms in different tiers of Internet Governance; and (ii) Perceived Legitimacy Framework for assessing the legitimacy of any Internet Governance processes.

Combining these two frameworks, the paper proposes the M-TOP approach to Internet Governance that India should adopt at the domestic, regional, and international levels. We presented a strategy to systematically include India's concerns in various Internet Governance processes and to enhance India's participation in various Internet Governance organizations.

At another level, this study delineates the implications of India's multi-lateral approach to Internet Governance in international forums and shows that it has isolated India in various forums such as the Plenipot – 2014. Not only is it necessary to review our multi-lateral approach, it is equally important to review the processes by which such an approach was formulated.

Further, India's approach to Internet Governance so far has linked a multi-stakeholder approach with US dominance in Internet Governance. This needs to be separately examined. India needs to develop a strategic approach to influence and participate in various related processes such as the IANA transition, so that going forward there is a more equitable balance of power in Internet Governance.

8.2 Recommendations

Given the far reaching implications of the Internet and quality of Internet Governance on the Indian economy as highlighted in the paper, we give our recommendations under the following two heads: Overall Policy and Detailed Policy.

Overall Policy:

1. ***Role of DeitY***: Given its assigned scope and continued prior participation in various Internet Governance decision-making bodies, committees, forums, ***DeitY should continue to be the lead ministry/department for Internet Governance***. Its representation in ICANN, efforts in managing Critical Internet Resources including the ccTLD/IDN Registry and National Internet Registry, , establishment of India Internet Governance Forum (India-IGF), the Multi-stakeholder Advisory Group (MAG) and the Inter-Ministerial Group (IMG), eminently qualify it for this position. DeitY has built institutional capacity for dealing with Internet Governance processes, both at the technical and policy level.

2. ***Need for a Timely Strategic Response*:** The global environment under which Internet Governance issues are being deliberated is under rapid flux. Going forward, if India is to play a significant role in Internet Governance, it must review and strengthen existing institutional mechanisms to respond in a time bound manner. The issues are becoming more complex and span across functional and territorial jurisdictions and laws. The IANA transition and the NETmundial Initiative are two examples where a rapid response at the organizational/policy

level is critical. India needs to draw inspiration from Brazil's CGI.br, which has taken a leadership position in this aspect.

Given the criticality of the Internet to the Indian economy and its role in maintaining our cyber-security and sovereignty, India needs to take a strategic perspective on its role in Internet Governance.

3. ***Model for Internet Governance:*** We recommend that since models of governance at different tiers of the Internet as articulated in the study are likely to have diverse drivers, participants, processes and outcomes, India should adopt the M-TOP approach for all levels of Internet Governance: domestic, regional and international. ***The M-TOP approach recognizes that even when nation states need to be involved in decision-making, they need to adopt a multi-stakeholder approach for participation, agenda setting and decision-making.*** Further, any Internet Governance process should satisfy the legitimacy parameters enumerated below:

   - *Open Participation*: At all tiers of Internet Governance, policy development processes should aim to be open in terms of participation of all relevant stakeholder groups; have wide representation including focus on emerging economies and gender; and overcome barriers emerging as a result of language, location, capacity and funding. At different tiers of Internet Governance, different categories of stakeholders are expected to contribute to various issues and policy stages depending on their expertise and the nature of public policy issues in that tier. For example, while the technical community needs to take the lead on and represent India on issues of technical standardisation, the governments need to take the lead on and represent issues of cyber-security and cross-border capacity building for say, cyber-security and lawful interception.

   - *Agenda Setting and Decision-making Processes*: The agenda setting process should be bottom-up and include inputs from as many stakeholders as possible. A consensus driven approach is recommended. The decision-making processes need to ensure transparency of information. The process design should ensure that there is no capture by any dominant group.

   - *Outcomes*: Decision-making processes should produce tangible outputs with high adoption rates.

   The figure below gives the schematic representation of the proposed Internet Governance model.

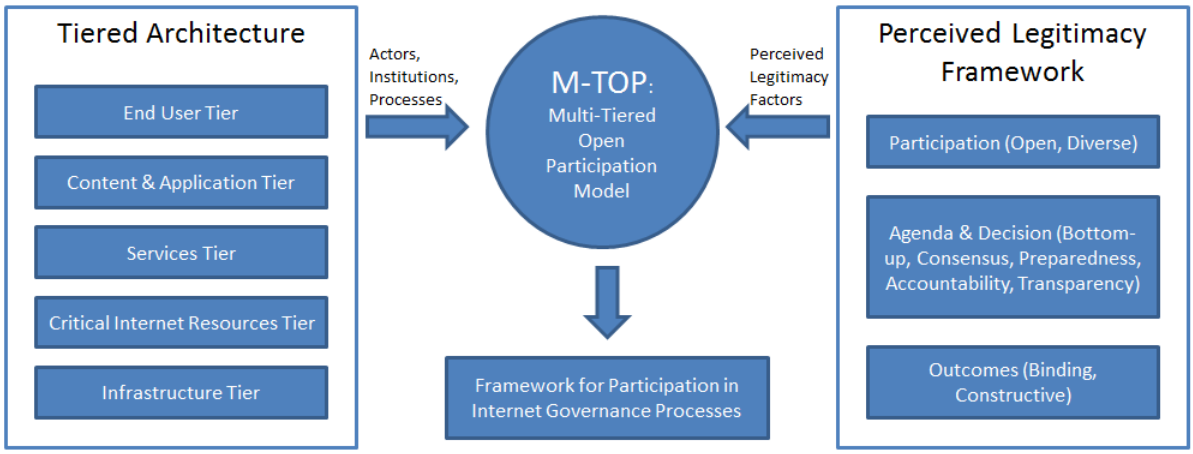

Fig 4: Model of Internet Governance

Table-2, Section 6.7 which presents the tiered approach should be used as a basis for identifying the issues, lead and other actors, and geographical scope across different tiers.

4. ***Participation in Internet Governance Organizations at Domestic, Regional and International Levels:*** India needs to focus at all levels of Internet Governance namely domestic, regional and international levels. Further, India must play a more significant role both at the regional and international levels. For this, not only greater participation in the organizations and processes related to Internet Governance is required, but a strategic long term plan to influence and shape these organizations must be undertaken.

5. ***Legitimacy to Influence Internet Governance at the Regional and International Levels:*** To gain legitimacy to influence governance, especially at the regional and international levels, India needs to accelerate Internet and Broadband adoption and drastically improve the quality of the Internet experience. For this a much greater focus on domestic Internet Governance issues is crucial.

6. ***Capacity Building:*** Senior government officials across different ministries need to be made aware of the various aspects of Internet Governance and how these governance mechanisms influence public policy such as access, access to information, human rights and development and international trade.

Detailed Policy Recommendations

1. Infrastructure Tier:

- Licensing and Spectrum Management:

  - It is recommended that the government create a National Spectrum Committee under the PMO or as an autonomous agency for spectrum management to facilitate coordination between different ministries and address the issues identified above. The current structure of WPC under DoT has created problems for coordination across ministries. Further, there is lack of perceived legitimacy both across government and private operators. For the private sector, the concerns have been inability of DoT to make more commercial spectrum available, restrictive guidelines regarding unlicensed bands and creating an enabling environment for trading and sharing of spectrum.

- Interconnection:

  - It is recommended that NIXI's mandate be revised to allow interconnection with CDNs and foreign ISPs.
  - It is recommended that NIXI's tariff and routing policy be revised to incorporate industry concerns.
  - It is recommended that NIXI undertake organizational restructuring of NIXI and become independent of DeitY (Jain, 2012).

- Standards:

  - The government/DoT should actively support participation and contribution by the Indian technical community in SDOs like TSDSI, 3GPP and IEEE.
  - TSDSI should be actively supported to develop standards and specifications for India specific environment and needs.
  - Standards and specifications created by TSDSI should be kept open for redistribution and reproduction to increase proliferation of these standards in the Indian academic and technical communities.
  - The multi-lateral approach suggested largely by the DoT towards standardisation be reviewed with the TSDSI, DeitY and other stakeholders in the context of the issues discussed and a coherent Indian position on this should be articulated.

- Access

    - The definition of broadband needs to be increased to 2 Mbps by 2015 in line with international norms and as envisioned by NTP 2012.
    - Private participation in the NOFN should be increased by way of auctions to the most competitive bidder. There is a need to coordinate with a variety of infrastructure ministries departments, such as highways, roads, water, bridges to coordinate RoW and laying of fibre optic cables.
    - The Cyber Café Rules of the Information Technology Act be liberalized for reducing regulatory compliance costs for provision of WiFi Hotspots.
    - A plan for the wireless access network needs to be simultaneously finalised to ensure access feasibility and allow rural citizens to use their mobile phones. Indian government should explore working with companies such as Facebook and Google for innovative technologies such as drones for last mile access.

2. Critical Internet Resources Tier

- *At the domestic level*, India should enhance the accountability of NIXI (which manages India's Critical Internet Resources) towards India's strategic goals by introducing an oversight mechanism and undertaking an organizational restructuring.
- *At the regional level*, India should strengthen participation in APNIC through executive positions in the APNIC EC and the NRO EC. This may require initiating bottom-up policy development processes for revising the APNIC EC election framework.
- *At the international level*, actively participate in the bottom-up policy development processes of GNSO and CCNSO of ICANN, and the IETF through Working Groups.
- DeitY should organize awareness building and information sessions around the implications of new gTLDs for business and economy on the Internet.
- There should be a systematic process and a dedicated group within DeitY that examines issues regarding gTLDs from a legal and business perspective.
- TRAI should monitor transition to IPv6 within a specified time frame. This should be arrived at in consultation with the industry.
- India needs to play a more significant role in the Regional Internet Registry managed by APNIC. There should be a concerted effort from the DoT and DeitY to have a coherent approach to play a significant role in the APNIC and to support Indian ISPs to have a greater role in such bodies
- Indian government needs to create programs for awareness building in engineering and technical institutes regarding the functioning, process and benefits of participation in standard setting.

3. Service Tier

- Strengthen JWG on cyber-security.
- Develop human capacity for understanding the legal and technological issues related to cyber-security. This should be done for executives in the government departments listed above. These should be joint sessions so that the participants get a holistic perspective. At another level, government could support launch of relevant courses in technological, management and law schools.

4. Content and Application Tier

- Privacy and Data Localisation:
    - It is recommended that since most of the data centres reside in the United States and Europe, efforts need to be taken to harmonise privacy regulations with these two jurisdictions.
    - It is recommended that DeitY and DoT actively monitor and enforce the use of NIC emails for official government communications.
    - It is recommended that books in vernacular languages kept in national libraries be digitised and made accessible online. Collaborations may be initiated with service providers like Google Books and Amazon Kindle to leverage their existing infrastructure. A plan for royalty sharing with authors of such books be introduced in line with established practices.

- Intermediary Liability:
    - It is recommended that the Intermediary Guideline Rules 2011 be reviewed and revised by way of in-depth open stakeholder consultations. The Intermediary Liability regime should be liberal such that it encourages service providers to host data domestically in India.

- E-Governance:
    - It is recommended that all government sites be mobile enabled.
    - It is recommended that regular audit and monitoring of all existing e-governance services be carried out to ensure minimum service levels.

- Regulation of OTTs and Network Neutrality:
    - It is recommended that the government bring certainty in the regime by taking a clear stand on the issue of OTT licensing and Network Neutrality.

5. End-User Tier

- Awareness and capacity building can be achieved using training sessions in schools, colleges and through various other commercial training centres. Incentive structures should be created that encourage people to learn using the Internet. For this, funding for public schools and colleges to connect to the Internet should be provided.

9 References

1. Bendiek, A., and Wagner, B. (2012). The Constitution of the Internet the EU needs to develop a common Strategy for Cyber Security, *Internationale Politik*, 67(6), 85-92.
2. Bennett, R. (2012). The Gathering Storm: WCIT and the Global Regulation of the Internet, Information Technology and Innovation Foundation, November 21, 2012. Available at http://www.itif.org/publications/gathering-storm-wcit-and-global-regulation-internet, accessed on February 21, 2015.
3. Bernstein, S. (2004-05). Legitimacy in Global Environmental Governance, *Journal of International Law and International Relations*, 1(1-2), 139-166.
4. Bernstein, S. F., and Cashore, B. W. (2007). Can Non-State Global Governance be Legitimate? A Theoretical Framework, *paper presented at the annual meeting of the International Studies Association 48th Annual Convention*, Chicago, February 28-March 3, 2007.
5. Bogason, P., and Musso, J. A. (2006). The Democratic Prospects of Network Governance, *The American Review of Public Administration*, 36(1), 3-18, March 2006.
6. Buchanan, A., and Keohane, R. O. (2006). The Legitimacy of Global Governance Institutions, *Ethics & International Affairs*, 20(4), 405-437.
7. Chenou, J. (2011). Is Internet governance a democratic process? Multistakeholderism and transnational elites, *paper presented at the ECPR General Conference 2011*, University of Iceland, August 25-27, 2011. Available at http://ecpr.eu/filestore/paperproposal/1526f449-d7a7-4bed-b09a-31957971ef6b.pdf, accessed on February 10, 2015.
8. Christou, G., and Simpson, S. (2011). The European Union, multilateralism and the global governance of the Internet, *Journal of European Public Policy*, 18(2), 241-257, DOI: 10.1080/13501763.2011.544505.
9. Cooper, M. (2013). Why Growing Up is Hard to Do: Institutional Challenges for Internet Governance in the "Quarter-Life Crisis" of the Digital Revolution, *Journal on Telecommunications and High Technology Law*, 11, 45-134.
10. DeNardis, L. (2010). The Emerging Field of Internet Governance, *Yale Information Society Project Working Paper Series*, Available at SSRN: http://ssrn.com/abstract=1678343, accessed on February 10, 2015.

11. DeNardis, L., and Raymond, M. (2013). Thinking Clearly about Multi stakeholder Internet Governance, *paper presented at Eighth Annual GigaNet Symposium*, Bali, Indonesia, October 21, 2013.
12. Eeten, M., and Mueller, M. (2012). Where is the governance in Internet governance?, *New Media & Society*, 15(5), 720-736, August 2013.
13. Hill, R. (2014). The internet, its Governance, and the Multi-stakeholder Model, *Info*, 16(2), 16-46.
14. Jain, R. (2012). Unshackling the NIXI Legacy: Imperatives for Future Growth, *a report submitted to NIXI*, February 2012.
15. Juhola, S., and Westerhoff, L. (2011). Challenges of adaptation to climate change across multiple scales: a case study of network governance in two European countries, *Environmental Science & Policy*, 14, 239–247.
16. Karrenberg, D., Ross, G., Wilson, P., and Nobile, L. (n.d.). Regional Internet Registry. Available at http://cis.mhcc.edu/pm/CIS151/Chap%2006%20Part%201/RIR-Cisco.pdf, accessed on March 1, 2015.
17. Klein, H. (2002). ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy, *The Information Society: An International Journal*, 18(3), 193-207, 2002.
18. Koppell, J. G. S. (2008). Global Governance Organizations: Legitimacy and Authority in Conflict, *Journal of Public Administration Research and Theory*, 18(2), 177-203.
19. Kummer, M. (2012). CSTD meeting on enhanced cooperation on public policy issues pertaining to the Internet, *The United Nations Commission on Science and Technology for Development Meeting on Enhanced Cooperation on Public Policy Issues Pertaining to the Internet*, May 18, 2012. Available at http://unctad.org/meetings/en/Presentation/cstd18may2012_p04_EN.pdf, accessed on March 20, 2015.
20. Lenard, T. M., and White, L. J. (2011). Improving ICANN's governance and accountability: A policy proposal, *Information Economics and Policy*, 23, 189–199.
21. Malcolm, J. (2008). *Multi-stakeholder Governance and the Internet Governance Forum*, Published by Terminus Press, ISBN: 9780980508406.
22. Martens, J. (2007). Multi-stakeholder Partnerships – Future Models of Multilateralism?, *Occasional Papers, Dialogue on Globalization*, January 2007.

Available at http://library.fes.de/pdf-files/iez/04244.pdf, accessed on January 10, 2015.

23. Mueller, M. (1999). ICANN and Internet governance: sorting through the debris of "selfregulation", I*nfo*, 1(6), 497-520.
24. Mueller, M. (2008). Scarcity in IP addresses: IPv4 Address Transfer Markets and the Regional Internet Address Registries, *Internet Governance Project*. Available at http://www.internetgovernance.org/wordpress/wp-content/uploads/IPAddress_TransferMarkets.pdf, accessed on February 22, 2015.
25. Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*, MIT Press, Cambridge, MA.
26. Mueller, M., and Wagner, B. (2014). Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance, *Internet Governance Forum*, 9–10 (2014). Available at http://www.internetgovernance.org/wordpress/wp-content/uploads/MiltonBenWPdraft_Final.pdf, accessed on January 10, 2015.
27. Mueller, M., Schmidt, A., and Kuerbis, B. (2013). Internet Security and Networked Governance in International Relations, *International Studies Review, Special Issue: International Relationships in the Information Age*, 15(1), 86–104, March 2013.
28. Reding, V. (2009). Commissioner Reding's Weekly Videomessage Theme: "The Future of Internet Governance: Towards an Accountable ICANN", May 4, 2009. Available at http://www.isi-initiative.org/index.php?option=com_docman&task=doc_download&gid=212&Itemid=3, accessed on February 27, 2015.
29. Resnick, P. (2014). On Consensus and Humming in the IETF, June 2014. Available at http://tools.ietf.org/pdf/rfc7282.pdf, accessed on January 10, 2015.
30. Ryan, P. S., and Glick, J. (2012). The ITU Treaty Negotiations: A Call for Openness and Participation, *North American Network Operators' Group 55th (NANOG 55) Meeting*, June 2012. Available at SSRN: http://ssrn.com/abstract=2077095, accessed on February 10, 2015.
31. Scharpf, F. W. (1999). *Governing in Europe: Effective and Democratic?*, Oxford: Oxford University Press.
32. Seger, A. (2011). The Budapest Convention on Cyber-crime 10 years on: Lessons learnt or the web is a web, *paper presented at the International Conference on Cyber-crime: Global Phenomenon and its Challenges organized by ISPAC/CNPDS/Courmayeur Foundation/UNODC/KIC* in Courmayeur Mont Blanc,

Italy, 2-4 December 2011. Available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/AS_UNISPAweb_V6_16feb12.pdf, accessed on January 17, 2015.

33. Skogstad, G. (2011A). Contested Accountability Claims and GMO Regulation in the European Union, *Journal of Common Market Studies*, 49(4), 895–915, July 2011.
34. Skogstad, G. (2011B). Legitimacy and/or policy effectiveness?: network governance and GMO regulation in the European Union, *Journal of European Public Policy*, 10(3), 321-338.
35. Underhill, G. R. D., and Zhang, X. (2008). Setting the rules: private power, political underpinnings, and legitimacy in global monetary and financial governance, *International Affairs*, 84(3), 535–554, May 2008.
36. Vallejo, N., and Hauselmann, P. (2004). Governance and Multi- stakeholder Processes, *published by the International Institute for Sustainable Development*, May 2004. Available at http://www.iisd.org/pdf/2004/sci_governance.pdf, accessed on January 25, 2015.
37. Varon, J. (2014). The NETmundial: An Innovative First Step on a Long Road, *Beyond NETmundial: The Roadmap for Institutional Improvements to the Global Internet Governance*, 16-24. Available at http://www.global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial_FINAL.pdf, accessed on March 20, 2015.
38. Virgoe, J. (2009). International governance of a possible geoengineering intervention to combat climate change, *Climatic Change*, 95, 103–119, 2009.
39. Zurn, M. (2004). Global Governance and Legitimacy Problems, *Government and Opposition*, 39(2), 260–287, Spring 2004.

10 Annexure

10.1 Annexure 1 – CGI.br Roles and Responsibilities

The roles and responsibilities of CGI.br are given below[74].

"The Brazilian Internet Steering Committee (CGI.br) was created by Interministerial Ordinance 147, of May 31st, 1995, which was amended by Presidential Decree 4,829 of September 3rd, 2003, with the purpose of coordinating and integrating all Internet service initiatives in Brazil, as well as promoting technical quality, innovation and the dissemination of the services available.

The CGI.br is comprised of members from the government, the corporate sector, the third sector and the academic community, and as such constitutes a unique Internet governance model for the effective participation of society in decisions involving network implementation, management and use. Based on the principles of multilateralism, transparency and democracy, since July 2004 the CGI.br has been democratically electing representatives from the civil society to participate in discussions and to debate priorities for the Internet together with the government".

Mission

"The mission of the CGI.br involves certain rights and responsibilities, which include:

- proposing policies and procedures regarding the regulation of Internet activities;
- recommending standards for technical and operational procedures for the Internet in Brazil;
- establishing strategic directives related to the use and development of the Internet in Brazil;
- promoting studies and technical standards for network and service security in the country;
- coordinating the allocation of Internet addresses (IPs) and registration in the <.br> domain;
- collecting, organizing and disseminating information on Internet services, including indicators and statistics".

[74]Excerpted from http://cgi.br/about/, accessed on December 8, 2014

10.2 Annexure 2 – India's Participation in I Organizations*

India and ICANN: The presence of Indians/Persons of Indian origin (PIOs) on the ICANN Board and its affiliated committees and the technical bodies associated with Internet governance is as follows[75]:

1. **ICANN Board of Directors:** The Board of Directors comprises of 15 members. These are appointed by various constituencies. Eight members on the Board are nominated by the Nominating Committee of the ICANN Board and these nominated members are expected to reflect diversity in geography, culture, skills, experience and perspective. Five regions have been defined for this purpose. India is covered as part of Asia Australia Pacific region. Presently, there is no Indian nominated by the Nominating Committee. Mr. Rammohan, Vice President and CTO Afilias is nominated to the Board by Security and Stability Advisory Committee (SSAC) of ICANN. He is a PIO with American citizenship but still has roots in India.

2. **Committees of ICANN:** There are several Committees provided under the ICANN. Byelaws and each forms an important constituency of the Internet governance ecosystem. The roles and responsibilities of each of these Committees are laid down in the byelaws. The lack of adequate representation of India on these bodies is reflected from details below.

   a. **Governmental Advisory Committee (GAC):** India is one of the 132 countries/regional formations which are represented on the GAC. India is represented through the Department of Electronics and IT.
   b. **Root Server System Advisory Committee (RSSAC):** There is no Indian representation in the Executive Committee of the RSSAC. Verisign is the Root server operator.
   c. **Security and Stability Advisory Committee:** Neither the Chairman nor any of the 50 Members of SSAC are Indians. Mr Ram Mohan is a member of SSAC and also SSAC nominee to the ICANN Board.
   d. **At-Large Advisory Committee (ALAC):** No Indian in the 15 Members of ALAC or in the four member leadership team of ALAC.
   e. **Address Supporting Organizations (ASO/Number Resource Organization (NRO):** There are 15 members in the NRO Number Council representing different regions. Mr. Naresh Ajwani is one of the members representing Asia Pacific region. He is also Vice Chair of the Council.
   f. **Country Code Names Supporting Organization (ccNSO):** Neither the Chairman nor any of the 18 Members of ccNSO Council are Indians. All three representatives from Asia Pacific are non-Indians.

[75]Compiled by DeitY

g. **Generic Names Supporting Organization (GNSO):** Neither the Chairman nor any of the 23 Members of GNSO Council are Indians. Mr. Pranesh Prakash is an Executive Committee Member Non-Commercial Users' Constituency which is in turn part of the Generic Names Supporting Organization
h. **Nominating Committee:** Neither the Chairman nor any of the 21 Members of Nominating Committee of ICANN Board are Indians.
i. **Technical Liaison Group (TLG):** None of the four liaisons of the TLG are Indians.

3. **Regional Internet Registries (RIRs):** There are five RIRs in the ICANN ecosystem responsible for registration and allocation of Internet numbers. The RIR relevant to India is Asia Pacific Network Information Centre (APNIC) with headquarters at Melbourne. Australia. APNIC has 8 EC members. None of them are Indians. After prolonged negotiation APNIC has agreed to set up a National Internet Registry (NIR) for India in March 2012. The NIR is managed by NIXI and was formally inaugurated in March 2013. India is one of the few countries to have a NIR which is managed by its own agency.

4. **Technical Bodies associated with ICANN**

a. Internet Engineering Task Force (IETF): IETF works through Working groups. Currently there are 16 active Working Groups. None of the Working Groups has an Indian chair.
b. Internet Society (ISOC): None of the 13 Trustees on the Board are Indians.
c. Internet Architecture Board (IAB): None of the 15 members are Indians.
d. World Wide Web Consortium (W3C): None of the 9 Advisors on the board are Indians.

10.3 Annexure 3 – Institutions and Instruments

10.3.1 Licensing and Spectrum Management

In India, all TSPs and ISPs are licensed by the Central Government under the Telegraph Act 1885. Historically, India has offered separate licenses for TSPs and ISPs. India has recently migrated to the Unified Licensing (UL) regime from the Unified Access Services Licensing (UASL) regime. In the UL regime, a single license is offered for all services, which is delinked from spectrum. In contrast, in the legacy UASL regime, spectrum was linked to licenses. In that, even though a single license was offered for all access services, separate licenses were required for non-access and non-telecommunications services like international and domestic long distance carriage, broadcasting etc.

Since 90% of the Indian users access the Internet using a mobile device, spectrum is an essential component of the Infrastructure Tier in India. India has a policy document called the National Frequency Allocation Plan (NFAP), according to which it allocates spectrum for different purposes based on the Radio Regulations emerging from the World Radio communications Conference of the ITU. In this, the ITU has divided the world is divided into three regions and India falls in region 3, which is the Asia Pacific region. In line with regional coordination, the NFAP provides the national allocation an utilisation of frequency spectrum for primary and secondary purposes. Spectrum is either administratively allocated or auctioned for the purpose specified in the plan. For the purpose of commercial mobile communications, India currently auctions access spectrum; while it administratively allocates backhaul spectrum.

The Central Government has recently also liberalised access spectrum, this making it technology neutral, and is also in the process of allowing spectrum trading and sharing in the secondary market. Spectrum in India is extremely fragmented and operators only have access to a limited amount of spectrum due to excessive competition.

The TRAI plays an important role in the policy development process in this area. It usually follows a process wherein it invites comments by stakeholders on a consultation paper and then provides recommendations on the basis of the comments received. The Central Government deliberates over these recommendations by TRAI and either accepts or rejects them. The WPC, which prepares the NFAP and allocates spectrum, is a body under the Ministry of Communications and Information Technology. The following figure attempts to summarise the relationships in this process.

The following governance issues were identified in our review of the instruments and institutions:

1. Lack of coordination between ministries: Currently, there is lack of coordination between different ministries with respect to spectrum requirement and allocation. For example, the DoT has been unable to allocate additional spectrum in the 2100 MHz band for 3G services because spectrum in that band is currently being held by the Defence Ministry. The DoT has been unable to refarm that spectrum due to its inability to provide an alternate media for the use by Defence.

2. No clear roadmap for future spectrum usage: The DoT has not been able to provide a clear roadmap for future spectrum auctions. In the absence of a clear roadmap, Telecom Service Providers are unable to take informed decisions during spectrum auctions as a result of which they may either over bid, under bid or abstain from participating. This information asymmetry may also be a barrier for investors looking for low risk investments.

3. Need to increase unlicensed bands: Unlicensed bands like the ISM band in 2.4GHz are essential for promoting innovation of new network technologies that allow for multiple devices to operate without interference, especially for personal area networks. There is a growing call for allowing the use of such unlicensed spectrum for purposes such as broadcasting radio and television stations, operating the local loop by telecom service providers etc. De-licensing bands may drastically bring down costs for access to the Internet; and promote efficient use of spectrum.

4. Shared use and trading of spectrum: If allocation of spectrum in the primary market is inefficient, a secondary market with low transaction costs provides TSPs the opportunity to reorganize spectrum according to the most efficient use. Allocation in the primary market in India has been inefficient due to the fragmented non-contiguous spectrum in small quantum spread across multiple bands, for technologies that are now obsolete. For all future spectrum allocations, India has liberalised spectrum and finalised a spectrum trading and sharing regime in the secondary market. However, all previous allocations are not part of this new regime creating inefficiencies that may be difficult to remove in the long run.

5. Auction as means of allocation: Auction is a well-established mechanism for allocation of access spectrum. However, administrative allocation is still followed for backhaul broadcasting, captive spectrum.

10.3.2 Interconnection

This refers to policy issues arising from network interconnection between various Telecommunications and Internet Service Providers with the objective of capturing the positive externalities arising from network effects. The TRAI has specified a Reference Interconnect Order with a standard interconnection agreement to prevent an incumbent from denying interconnection to a new TSP. Interconnection between ISPs is generally referred to as peering. The ISPs either privately peer with each other or use the facilities of the National Internet Exchange of India for interconnection. Notably, the TRAI is presently undergoing a consultation on the issue of interconnection in the context of migration to IP networks by TSPs. NIXI was incorporated in 2003 for promoting domestic routing and to save international bandwidth.

The following governance issues were identified in our review of the instruments and institutions:

1. Limited mandate of NIXI: NIXI's mandatory requirement that currently only allows Indian licensed ISPs to interconnect has prevented NIXI from emerging as a regional hub for neighbouring countries and has also proved as a barrier for CDNs not licensed as ISPs to interconnect with the exchange.

2. Due to NIXI's adverse tariff and routing policy, numerous licensed ISPs currently do not interconnect at NIXI as a result of which domestic traffic first goes out of India and then comes back into India.

3. Most of the data centres are situated outside India as a result of which India is largely dependent on International interconnection. Cost of access and services are therefore dependent on cost of international transit costs. Efforts need to be undertaken to promote data centres in India by way of economic incentives and a stable regulatory regime with minimal liability.

4. Cost of domestic leased lines vis-à-vis international lines is high, causing impediments for ISs and content providers to seek domestic lines.

10.3.3 Standards

Standard development in the access layer of telecommunications happens in standard development organizations (SDO) like 3GPP, 3GPP2 and IEEE. This layer only deals with standard development at the physical or access

layer. Standards above the wire and below the applications fall in the domain of the Critical Internet Resources layer standardisation process of IETF.

The ITU specifies minimal International Mobile Telecommunications (IMT) requirements for recognition as 3G (IMT) and 4G (IMT-Advanced); and any SDO may propose a standard that meets these minimal requirements. For example, currently, LTE-Advanced from 3GPP and WiMAX-Advanced from IEEE qualify as 4G standards. Similarly, Universal Mobile Telecommunications System (UMTS)/High Speed Packet Access (HSPA) by 3GPP and EVDO by 3GPP2 qualify as 3G standards. These standards developed these SDOs do not generally compete with the standards developed IETF. IETF generally works on layers above the access layer while SDOs like 3GPP work on the access layer only.

Standards are primarily developed by international SDOs. These standards are not binding under international law and may be voluntarily adopted by any country. The license agreement between the Central Government and the TSP mandates the use of such internationally recognized standards in the provision of telecommunications services. In addition to the standards developed by SDOs, the national governments may also specify nationally developed standards that deviate from international norms. For example, India specifies a standard for maximum EMF (Electromotive force) radiations that differs significantly from those of other countries.

10.3.4 Access

Currently, a majority of India's population does not have access to the Internet. Of those with access, the majority of them consume Internet services on their mobile device. Most internet access in India is based on two part pricing wherein a fixed price is charged in addition to variable per quantum of data consumption charge. Recognizing the lowering of tariffs due to competition, the TRAI has adopted the stance of forbearance with respect to tariff regulation. Stream-IV of the Universal Service Obligation Fund (USOF) focuses on provision of broadband connectivity to remote and rural areas through Wire Line Broadband and Rural Public Service Terminals. In order to strengthen the backbone for delivery of broadband services, the Government of India has launched the National Optical Fibre Plan to increase fibre connectivity to Gram Panchayats. This project has currently been delayed considerably due to Right of Way issues.

The government has adopted the National Broadband Plan and National Telecom Policy 2012 to outline its strategy for increasing broadband proliferation. Prior to NTP 2012, the New Telecom Policy 1999 also sought to achieve provision low speed data service to all uncovered villages 2002 to

all district headquarters by year 2000. The funds for the National Optical Fibre Network are disbursed through the Universal Service Obligation Fund.

The following governance issues were identified in our review of the instruments and institutions:

1. In providing access, obtaining Right of Way (RoW) has been a major impediment for laying cables and constructing towers. While projects such as NOFN are central initiatives, granting RoW has been the prerogative of state and municipal governments.

2. The Government has not involved any private company in the implementation of the NOFN, which is a departure from the standard practice of USOF to auction to the lowest competitive private bidder.

3. The NOFN focuses primarily on the backbone and does not formally suggest a complementary access network.

4. The definition of broadband in India is not coherent with international norms.

10.3.5 Critical Internet Resources

The dominant actors in this layer include IETF, IAB, ISOC, IRTF and ICANN. These actors are collectively referred to as the I* organizations. Owing to historical reasons, NTIA of the US Government (USG) currently presides as the steward of the DNS. Presently NTIA contracts ICANN for the IANA functions. ICANN is a not-for-profit company incorporated in the United States. The unilateral role of the USG as the steward of the DNS system is presently under transition. A transition coordination group (ICG) has been constituted to coordinate this transition.

The community of stakeholders working on names, numbers and protocols are referred to as ICANN's three operational communities (alternatively clients or customers). The numbers function is presently performed by the five Regional Internet Registries (RIRs). India falls under the APNIC RIR. In 2012, NIXI was made the National Internet Registry (NIR) for allocation of AS numbers and IP addresses in India. The five RIRs collectively form the Numbers Resource Organization (NRO). The NRO represents the numbers community in the ICANN through the ASO.

The protocols and standard development function is performed by the IETF. Standards developed by the IETF are generally above the wire (physical layer) and below the application layer. The IAB oversees IETF and its sister

task force IRTF, which focuses on long term research on the Internet. ISOC provides a legal structure to the task forces. ISOC has three main functions – standard development, education and public policy. The task forces fall under the standard development function.

ICANN functions through numerous Advisory Committees (AC), Supporting Organizations (SO) and Stakeholder Groups (SG). For example, the governments are represented in ICANN through the GAC and the general internet users are represented in ICANN through the At-Large Advisory Committee (ALAC). Similarly, the gTLD registries are represented in ICANN through the GNSO; the ccTLD registries are represented through the ccNSO; and the RIRs are represented through the ASO/NRO.

The IETF, RIRs and ICANN's GNSO follow a bottom-up policy development process (PDP). For example, IETF is open to participation by all; anybody can recommend an internet draft, which if accepted by rough consensus gets the status of a RFC. The Critical Internet Resources layer sees minimal participation by state actors in its processes. States play only an advisory role through the GAC of the ICANN. The GAC's advice is not binding on the ICANN board. In all other respects, governments are treated at an equal footing with other stakeholders. In this context, the composition of stakeholders comprising the GNSO in ICANN is largely dominated by the registry operators. Similarly, the IETF is largely dominated by the software development and equipment manufacturing industry; and RIRs are dominated by the ISPs.

Given the multi-stakeholder approach of this layer, the civil society is an active participant in policy issues. The civil society plays a part either through the bottoms up policy development processes or by voicing concerns through advocacy papers or at various conferences. The civil society operates in this space in the form of individuals and organizations demonstrating collective action through coalitions or networks. Notable coalitions include the Just Net Coalition, Best Bits, Internet Governance Caucus, Diplo and Association for Progressive Communications.

10.4 Annexure 4 – Correspondence between the IT Act, 2008 in India and the Budapest Convention

POLITIET
KRIPOS

NCIS Norway
National Criminal Investigation Service

The Budapest Convention and the legal framework in India

Several provisions of the Budapest Convention seem to have corresponding provisions in the domestic law of India.

POLITIET
KRIPOS

NCIS Norway
National Criminal Investigation Service

Provisions of the Budapest Convention: Substantive criminal law

Article	Budapest Convention	Corresponding provision in Indian law
Art. 1	Definitions	Section 2 ITA (as amended 2008)
Art. 2	Illegal access	Section 43 a and b, and 66F ITA
Art. 3	Illegal interception	
Art. 4	Data interference	Section 43 c, d, i, j and 66F (A) ITA
Art. 5	System interference	Section 43 d, e, f and 66F (A) ITA
Art. 6	Misuse of devices	Section 43 g, 84B ITA, Section 3 (2)h Intermediary Guidelines 2011
Art. 7	Computer-related forgery	Sections 66-66D ITA and Penal Code
Art. 8	Computer-related fraud	Sections 66-66D ITA and Penal Code
Art. 9	Child pornography	Section 67B
Art. 10	IPR offences	
Art. 11	Attempt, aiding, abetting	Sections 84B and C ITA
Art. 12	Corporate liability	Section 85 ITA

POLITIET
KRIPOS

NCIS Norway
National Criminal Investigation Service

Provisions of the Budapest Convention: Procedural law

Article	Budapest Convention	Corresponding provision in Indian law
Art. 15	Conditions and safeguards	General criminal law safeguards [Specific ITA (amended 2008) safeguards?]
Art. 16	Expedited preservation	Section 69 B and 67 C ITA
Art. 17	Exped preserv and partial disclosure of traffic data	Section 69 B and 67 C ITA
Art. 18	Production order	Section 69 B ITA, Evidence Act and Code of Criminal Procedure
Art. 19	Search and seizure	Sections 69 B, 80, 69 A, 76 ITA, Evidence Act and Code of Criminal Procedure
Art. 20	Real-time collection traffic data	Section 69 B ITA
Art. 21	Interception of content data	Section 69 ITA
Art. 22	Jurisdiction	Section 75

POLITIET
KRIPOS

NCIS Norway
National Criminal Investigation Service

Provisions of the Budapest Convention: International cooperation

Article	Budapest Convention	Corresponding provision in Indian law
Art. 23	General princip. (subsidiarity)	Use of existing treaties and provisions
Art. 24	Extradition	on international cooperation
Art. 25	General rules	
Art. 26	Spontaneous information	
Art. 27	MLA in absence of treaty	
Art. 28	Confidentiality	
Art. 29	Expedited preservation	Section 69 and 67 C ITA
Art. 30	Partial disclosure traffic data	Section 69 and 67 C ITA
Art. 31	MLA accessing data	Section 69 ITA
Art. 32	Transborder access	
Art. 33	MLA collection traffic data	Section 69 ITA
Art. 34	MLA interception content	Section 69 ITA
Art. 35	24/7 point of contact	In India: CBI

(Source: "The Budapest Convention on Cybercrime: Contribution in combating cybercrimes", by Eirik Trønnes Hansen, presented at the International Conference on #Cyberlaw, #Cybercrime &#Cyber Security, November 20, 2014, New Delhi)

10.5 Annexure 5 - List of people met

We would like to thank the below listed people (in alphabetical order of their last name) for providing their valuable insights.

S.no	Title	Last Name	First Name	Designation and Affiliation
1	Dr		Govind	CEO, NIXI
2	Mr	Abraham	Sunil	Executive Director, Centre for Internet and Society
3	Mr	Ajwani	Naresh	President, CCAOI
4	Dr	Bajaj	Kamlesh	CEO, Data Security Council of India
5	Mr	Bhatia	Virat	President (external affairs), AT&T for South Asia
6	Mr	Darlong	Thanglura	Joint Secretary, Counter Terrorism – Global Cyber Issues and Policy, Planning and Research
7	Ms	Das	Ankhi	Director of Public Policy, Facebook in India and South Asia
8	Mr	Hansen	Eirik Trønnes	Police Prosecutor, NCIS Norway
9	Mr	Jain	Rahul	Principal Consultant, Data Security Council of India
10	Mr	Karnik	Kiran	Director in Central board of directors, Reserve Bank of India
11	Dr	Kovacs	Anja	Director, Internet Democracy Project
12	Dr	Kumar	Ajay	Joint Secretary, Department of Electronics and Information Technology (DeitY) and Director General, NIC
13	Mr	Mathews	Rajan S	Director General, COAI
14	Mr	Matiya	Jarvis	Legal Adviser and Head of Justice Section, Rule of Law Division
15	Mr	Narain	Ram	Deputy Director General, DoT
16	Dr	Rai	Gulshan	Director General, GC and CERT-In
17	Mr	Seger	Alexander	Head of Cybercrime Programme Office, Council of Europe
18	Mr	Singh	Parminder Jeet	Executive Director, IT for Change
19	Ms	Teaotia	Rita	Special Secretary, DoT

11 Appendix

11.1 Appendix 1 - Internet Statistics for Different Countries

S.no	Country/Region	Avg. Mbps	Peak Mbps	% Above 10 Mbps	% Above 4 Mbps
1	South Korea	24.6	72.1	78.0	95.0
2	Hong Kong	15.7	73.9	52.0	89.0
3	Japan	14.9	61.5	54.0	86.0
4	Singapore	10.4	64.9	33.0	80.0
5	Taiwan	9.5	58.2	26.0	80.0
6	Australia	7.1	36.8	15.0	65.0
7	New Zealand	6.8	31.8	13.0	72.0
8	Thailand	6.3	41.3	8.2	79.0
9	Malaysia	4.3	30.5	5.5	40.0
10	China	3.7	17.4	1.8	33.0
11	Vietnam	2.9	18.2	0.6	20.0
12	Indonesia	2.5	23.5	0.5	10.0
13	Philippines	2.5	21.6	0.7	8.3
14	India	2.0	14.4	1.2	7.2

(Source: http://www.akamai.com/html/awe/login.html?campaign_id=F-MC-22494&curl=/dl/whitepapers/akamai-soti-q214.pdf&solcheck=1&WT.mc_id=soti_Q214&, accessed on December 9, 2014)

11.2 Appendix 2 - Glossary of Acronyms

S.no	Abbreviation	Full Form
1	AC	Advisory Committee
2	ALAC	At Large Advisory Committee
3	AoC	Affirmation of Commitments
4	APNIC	Asia Pacific Network Information Centre
5	AS	Autonomous System
6	ASNs	Autonomous System Numbers
7	ASO	Address Supporting Organizations
8	CAGR	Compound Annual Growth Rate
9	CBMs	Confidence Building Measures
10	CCNSO	Country Code Names Supporting Organization
11	ccTLD	country code Top-Level Domain
12	CIRP	Committee for Internet Related Policies
13	DeitY	Department of Electronics and Information Technology
14	DIT	Department of Information Technology
15	DNS	Domain Name System
16	DoC	Department of Commerce
17	DoT	Department of Telecommunications
18	EC	Executive Council
19	EMF	Electromotive force
20	EVDO	Evolution Voice-Data Optimized
21	FATF	Financial Action Task Force
22	GA	General Assembly
23	GAC	Governmental Advisory Committee
24	GATS	General Agreement on Trade in Services
25	GDP	Gross Domestic Product
26	GNSO	Generic Names Supporting Organization
27	gTLD	generic Top Level Domain
28	HLE	High Level Event
29	HLMC	High Level Multi-stakeholder Committee
30	HSPA	High Speed Packet Access
31	IAB	Internet Architecture Board
32	IANA	Internet Assigned Numbers Authority
33	ICANN	Internet Corporation for Assigned Names and Numbers
34	ICG	International Coordination Group
35	ICT	Information and Communications Technology
36	IDN	Internationalized Domain Name
37	IEEE	Institute of Electrical and Electronics Engineers
38	IETF	Internet Engineering Task Force
39	IGF	Internet Governance Forum
40	IMG	Inter-Ministerial Group
41	IMT	International Mobile Telecommunications
42	IP	Internet Protocol
43	IPRs	Intellectual Property Rights
44	IPv4	Internet Protocol version 4
45	IPv6	Internet Protocol version 6
46	IRINN	Indian Registry for Internet Names and Numbers

S.no	Abbreviation	Full Form
47	ISM	Industrial, Scientific and Medical (ISM) radio bands
48	ISOC	Internet Society
49	ISP	Internet Service Provider
50	ITR	International Telecom Regulations
51	ITU	International Telecommunication Union
52	ITA	Information Technology Act
53	ITU-T	ITU Telecommunication Standardization Sector
54	IX	Internet Exchange
55	IXP	Internet Exchange Point
56	JWG	Joint Working Group
57	JWT	Joint Working Team
58	LTE	Long-Term Evolution
59	M2M	Machine to Machine
60	MAG	Multi-stakeholder Advisory Group
61	MEA	Ministry of External Affairs
62	MHA	Ministry of Home Affairs
63	ML	multi-lateral
64	MMP	Mission Mode Projects
65	MoS	Minister of State
66	MoU	Memorandum of Understanding
67	MPP	Multi-stakeholder Preparatory Platform
68	M-TOP	Multi-Tier Open Participation
69	NAT-CIG	National Council on Internet Governance
70	NFAP	National Frequency Allocation Plan
71	NIR	National Internet Registry
72	NIXI	National Internet Exchange of India
73	NOFN	National Optical Fibre Network
74	NRO	Number Resource Organization
75	NSA	National Security Advisor
76	NSCS	National Security Council Secretariat
77	NSF	Network Science Foundation
78	NSI	Networks Solutions Incorporated
79	NTIA	National Telecommunications and Information Administration
80	OECD	Organization for Economic Co-operation and Development
81	OSCE	Organization for Security and Co-operation in Europe
82	OTT	Over the top
83	PDP	Policy Development Processes
84	PICS	Platform for Internet Content Selection
85	PLF	Perceived Legitimacy Framework
86	PMO	Prime Minister’s Office
87	PPP	Public- Private Partnerships
88	R&D	Research and Development
89	RFP	Request for Proposals
90	RIR	Regional Internet Registry
91	RoW	Right of Way
92	RSSAC	Root Server System Advisory Committee

S.no	Abbreviation	Full Form
93	RZM	Root Zone Manager
94	SDC	State Data Centre Scheme
95	SDO	Standard Development Organizations
96	SG	Stakeholder Groups
97	SO	Supporting Organizations
98	SSAC	Security and Stability Advisory Committee
99	SSDG	State Service Delivery Gateway
100	SWAN	State Wide Area Network
101	TLD	Top Level Domain
102	TLG	Technical Liaison Group
103	TRAI	Telecom Regulatory Authority of India
104	TSDSI	Telecommunications Standards Development Society, India
105	TSP	Telecommunication Service Provider
106	UASL	Unified Access Services Licensing
107	UC	User Constituencies
108	UL	Unified License
109	UMTS	Universal Mobile Telecommunications System
110	UN	United Nations
111	UN CSTD	United Nations´ Commission on Science and Technology for Development
112	USA	United States of America
113	USOF	United Service Obligation Fund
114	W3C	World Wide Web Consortium
115	WCIT	World Conference on International Telecommunications
116	WEF	World Economic Forum
117	WG	Working Groups
118	WG-App	Working Group Applications and Content Tier
119	WG-CIR	Working Group Critical Internet Resource Tier
120	WGEC	Working Group on Enhanced Corporation
121	WG-EU	Working Group End User Tier
122	WGIG	Working Group on Internet Governance
123	WG-Infra	Working Group Infrastructure Tier
124	WG-IPv6	Working Group on IPv6 Transition
125	WG- ITI	Working Group on IANA Transition Issues
126	WG-ITUP	Working Group ITU Plenipot
127	WG-NGA	Working Group on New gTLD Applications
128	WG-Ser	Working Group Service Tier
129	WG-WSIS2015	Working Group on WSIS 2015
130	WIPO	World Intellectual Property Organization
131	WPC	Wireless Planning & Coordination Commission
132	WSIS	World Summit on the Information Society
133	WTO	World Trade Organization

12 Acknowledgements

I wish to thank Mr Rishabh Dara, Doctoral Scholar at IIMA and Ms Radha Ravattu, Research Associate at IITCOE for their research assistance and contributions to the paper. Ms Sneha Jhala, Research Associate at IITCOE has helped in preparation of the paper.

I would like to express my sincere thanks to Dr Ajay Kumar (Joint Secretary, DIT) and Dr Govind (CEO, NIXI) for sharing their views and experiences with me.