Using Complex Adaptive Systems Theory for Developing an Internet Governance Model for India

Prof. Rekha Jain
Executive Chair, IIMA IDEA Telecom Centre of Excellence
Professor, IIM Ahmedabad
rekha@iima.ac.in

Introduction

- Internet Governance (IG) characterized by:
  - Intertwined technical, political, economic, and legal issues.
  - institutions that range from domestic (such as telecom service providers), regional (such as Regional Internet Registries) to international (such as International Corporation for Assigned Names and Numbers (ICANN).
  - Structurally from formally established to informal (DeNardis, 2012).
  - Instruments of governance vary from “rough consensus” to legally binding treaties.
  - Therefore, national and international governments, private sector, civil society organizations, academics, technical communities, and inter-governmental organisations play an important role. This has given rise to the development of multistakeholder approach.

IG Characteristics

- Network mode of governance in which a variety of actors involved in policy decisions and governance.
- Traditionally largely within the scope of the state.
- Thus the challenge is to design appropriate mechanisms that are perceived to have the requisite legitimacy in their decision making processes for acceptance of resultant outcomes of the process.

Modelling Internet Governance

- Need to be able to capture the complexity of structures, processes and interactions embodied in the plethora of organizations, across different countries, dealing with technical, legal, security issues involving both state and non-state actors.
- Responsive to fast technological change.
- Complex interactions between entities and between the entities and the external domain and hence unpredictable.
- Influence of events outside the country may often create a trigger for response at the domestic level.
- Past experiences may not be able to guide.
- Need to develop ever new types of organizations.

Modelling Internet Governance (contd..)

- One mechanism to address this need is to design for self-organization
  - the ability to govern without a central control.
- Emergence of ever new forms of organizations such as the Internet Governance Forum (IGF), netMundial and new technologies requires Internet Governance processes mechanisms to be adaptive. Thus Internet Governance has both characteristics of complexity and adaptiveness. Many other global governance spaces such as health care (Plsek, 2001; Begun et al, 2003; Rouse, 2008; Paina and Peters, 2012) environment (Levin, 1998; Kallis et al, 2009), supply networks (Choi et al, 2001), web (Rupert et al, 2008), that have similar characteristics as Internet Governance have been viewed as CAS. However, there have been limited instances where it has been applied to Internet Governance.

Objectives

- To develop a set of design principles emanating from our conceptualization of Internet Governance as CAS for creating a model for Internet Governance for India.

Methodology

- The study is based on primary and secondary data.
  - Primary research: semi-structured interviews with 29 key individuals, civil society groups and government functionaries at different levels covering relevant issues. These covered their perspectives on the current role of their organization in Internet Governance, the challenges and constraints they faced and the changes they would suggest to improve the situation. These interviews lasted 40 minutes to an hour.

- Two key events that helped us to gather a broad perspective as well as helped us to contact key people in this area were:
  - The Asia Pacific Regional Internet Governance Forum, Delhi, India 2014 August 3-6, 2014).
  - The Internet Governance Forum, Istanbul, Turkey 2014 (September 2-5, 2014).
  - Post the preliminary development of proposed framework, feedback was collected from key decision-makers through roundtables and workshops of various stakeholders to check the consistency of the framework and feasibility of its adoption.

Internet Governance as a Complex Adaptive System

CAS is characterized by:

- Several interacting constituents that adapt and learn from the interactions
- Emergence of order through self-organizing. (Self-organization refers to the ability to bring about change of scope, structure, and/or processes within the constituent modules to respond to changes in the environment without central control).
- Modifications in system behaviour in response to its learning from its interactions with other components and the environment.
- CAS are self-organizing, the process design of the constituents and the system should have:
  - autonomy,
  - flexibility and
  - responsiveness to changes in other constituents and/or environment.
- Co-evolve with changes in other constituents and/or environment
- Internet Governance structures need to be loosely structured even though these may operate within rigid national, regional or international boundaries.

Decision-Making for IG

- Simultaneous management of national and global resources (political, legal and sovereignty)
- Decision-structures involve multiplicity of stakeholders in a collaborative way.
- Such structures need to be flexible. The involvement of various organizations for dm is not fixed apriori. This could also happen across organizations having different scope, as for example, involving human rights organization in drafting a cyber-security treaty.

Design Principles

- Dealing with large scale, size and high levels of interdependence between constituent elements and the consequent complexity by modularization.
- Each of the modules communicates with standardized rules or interfaces. The constituent elements of a module have strong relationship with one another, while their relationships with elements in other modules is weak (Simon, 1962; Parnas, 1972).

Design Principles (contd..)

- Flexibility: extent to which the constituent modules have strict formal laid out processes. While some parts of Internet Governance would necessarily involve adherence to formal structures and processes (such as allocation of IP addresses), there is scope for voluntary coordination (as in the removal of malware, spam) across different groups spanning organizations and geographic boundaries.

- Therefore, Internet Governance when modelled as a CAS may be conceptualized as a nested system with self-organizing distributed constituents. These constituents operate at multiple levels and at different scales.

Internet Governance in India

- India's response: ad-hoc and has varied over time.
- No national strategic plan for including its concerns in various Internet Governance processes.
- Participated in various Internet Governance processes like WSIS, WCIT, Plenipot and other IGF meetings, from the government have not been a part of a national strategy

Source: http://www.thehindu.com/opinion/op-ed/on-multistakeholder-governance-of-the-internet/article7440857.ece, accessed on April 19, 2016

Internet Governance in India (contd..)

- The Department of Telecom (DoT) and Department of Electronics and Information Technology (DeitY) have participated independently. Further, responses from individual ministries have been ad-hoc.

- Indian response from the Ministry of External Affairs (MEA) and DoT has been limited to cyber-security and standards respectively.

- Move to Multi-stakeholder from multi-lateral. On the ground, an active approach to change composition of committees such as Cyber Regulatory Advisory Committee that has little representation from civil society or academia has been slow.

Internet Governance in India (contd..)

- 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. In 2015, India announced its support for a multistakeholder approach to Internet Governance. This was also considered as a signal that India would adopt more inclusive policy processes domestically. On the ground, an active approach to change composition of committees such as Cyber Regulatory Advisory Committee that has little representation from civil society or academia has been slow.

Institutional Structure of Internet Governance

- *DeitY:*
  - Nodal department for policy matters relating to the Internet (except licensing) and promotion, formulation of cyber laws such as the Information Technology Act, implementing e-governance. It has represented India at various Internet Governance organizations and participates in the advisory and planning processes including APNIC, ICANN, IGF and ISOC, IGF.
  - Deals with both the technical and policy matters related to CIR through the management of National Internet Exchange of India (NIXI) that operates as an Internet Exchange Point (IXP).
  - NIXI manages .IN ccTLD Registry, .भारत (.bharat) for ccTLD in local Devanagri language and other regional Indian languages, and the National Internet Registry.
  - It is responsible for mirror root servers.

Institutional Structure of Internet Governance (contd..)

- *DoT:*
  - Nodal department for the policy regarding telecommunication infrastructure. licensing, spectrum, broadband deployments, standards, interconnections and equipment. On the international side, it interfaces with ITU for spectrum regulation and other international aspects.

- *National Information Board:*
  - Apex level information security organization headed by the national security advisor. The National Cyber Coordination Centre is an e-surveillance and meta data screening agency that reports to the NIB.

Underlying Theory for Designing an Internet Governance Model for India

- Use the design principles and draw on the existing institutional structure to develop a model for Internet Governance for India.
- ***Structural Model:*** This is based on tiered architecture of the Internet. Since there are a wide variety of organizations and functions that constitute Internet Governance, with often overlapping scope, one mechanism to reduce this complexity is to break the scope across tiers.
  - Different tiers based on their core functionality required for Internet service provision in an open, equitable manner.
- ***Process Model:*** This gives a framework for interactions between the different constituents.

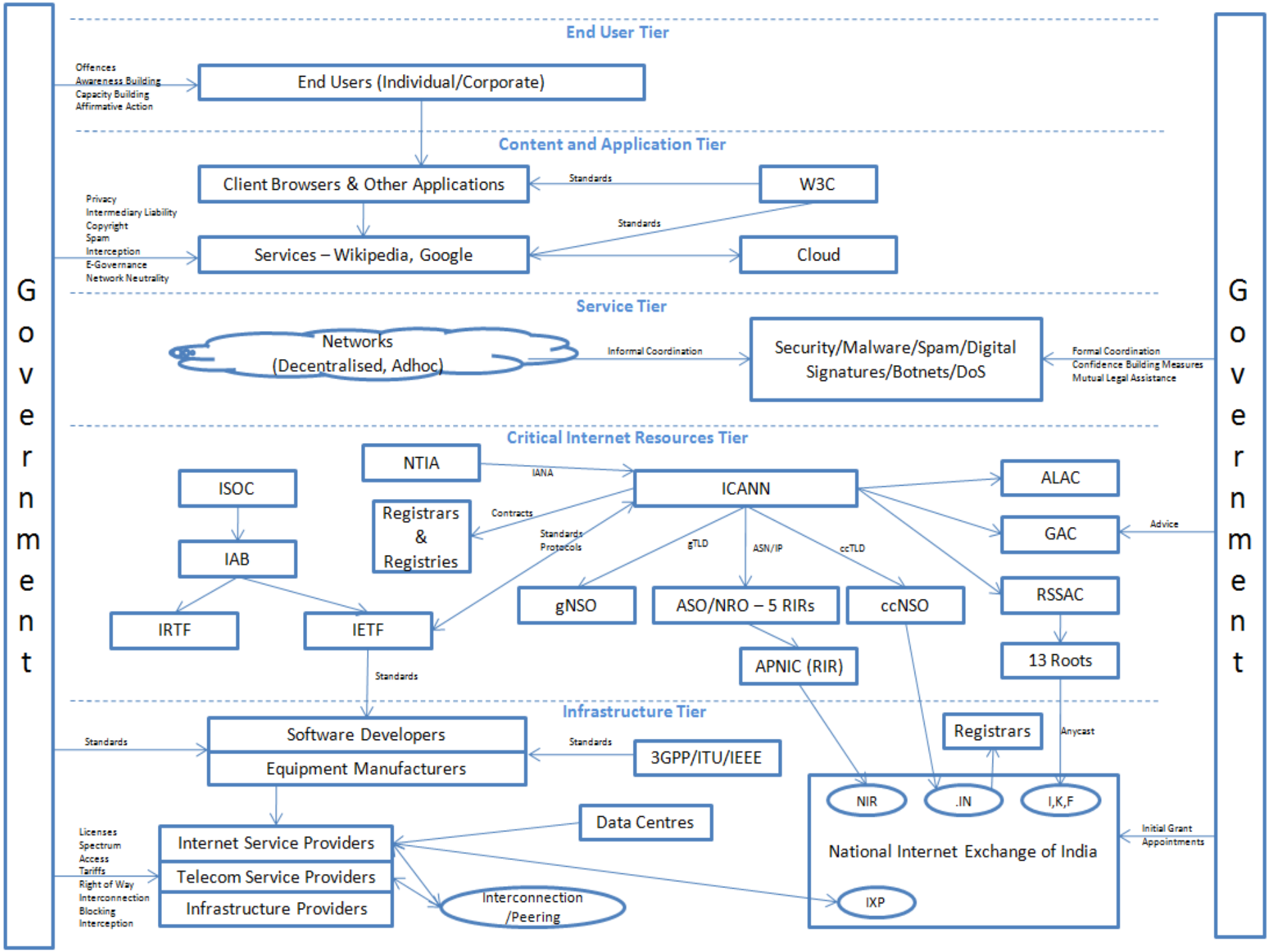
Structural Model: Multi-Tiered Approach

- The tiered approach is based on the premise that viewing Internet Governance as a sequence of tiers helps to deal with the inherent complexity associated with the multiplicity of actors, functions, interfaces in this domain. It is envisaged that the functionality of each tier provides a building block for the next one, in a way that the end-to-end functionality provided by this architecture leads to the end user having open and safe access to the Internet. Since the functions, actors, processes and institutions at each of these tiers are different, the public policy and the governance mechanisms at each of the tiers would vary, (Cerf et al, 2014; Jain, 2014). Solum and Chung (2003) and Cerf, Ryan and Senges (2014) use the tiered model of the Internet to frame the role of different multistakeholder in Internet Governance ecosystem, and highlight the scope of Internet Governance organizations such as ITU, ICANN, IETF and IGF within this model. They contend that each of these organizations must focus on their areas of expertise otherwise instruments such as treaties that span across different tiers could go awry.

Structural Model: Multi-Tiered Approach (contd..)

- Internet penetration in India:25.73% as of September 30, 2015 (Note: This refers to those with a data pack subscription, not necessarily Internet users),
- Poor quality of Internet access: Average Connection Speed (114/148 countries), and Peak Connection Speed (115/148 countries) (Akamai report)*, This data reflects that governance structure and processes at this tier have not been effective. Higher Internet penetration will give India legitimacy to influence global Internet Governance and provide a firmer basis to participate in the other tiers of Internet Governance identified in the framework.

*Source: https://www.akamai.com/us/en/multimedia/documents/content/state-of-the-internet/q4-2015-state-of-the-internet-connectivity-report-us.pdf, accessed on April 20, 2016


Government
End User Tier
Offences
Awareness Building
Capacity Building
Affirmative Action
End Users (Individual/Corporate)
Content and Application Tier
Client Browsers & Other Applications
Standards
W3C
Privacy
Intermediary Liability
Copyright
Spam
Interception
E-Governance
Network Neutrality
Services – Wikipedia, Google
Standards
Cloud
Service Tier
Networks
(Decentralised, Adhoc)
Informal Coordination
Security/Malware/Spam/Digital Signatures/Botnets/DoS
Formal Coordination
Confidence Building Measures
Mutual Legal Assistance
Critical Internet Resources Tier
NTIA
IANA
ISOC
ICANN
ALAC
Registrars & Registries
Contracts
Standards Protocols
GAC
Advice
IAB
gTLD
ASN/IP
ccTLD
RSSAC
IRTF
IETF
gNSO
ASO/NRO – 5 RIRs
ccNSO
APNIC (RIR)
13 Roots
Standards
Infrastructure Tier
Software Developers
Equipment Manufacturers
Standards
Standards
3GPP/ITU/IEEE
Registrars
Anycast
NIR
.IN
I,K,F
Licenses
Spectrum
Access
Tariffs
Right of Way
Interconnection
Blocking
Interception
Internet Service Providers
Telecom Service Providers
Infrastructure Providers
Data Centres
Interconnection /Peering
National Internet Exchange of India
IXP
Initial Grant
Appointments
Government

Structural Model: Multi-Tiered Approach (contd..)

Summary:

- Organizational structures and processes for Internet Governance in India are inadequate at all tiers of Internet Governance.
- While some tiers may require the design of new organizational structures, others may require a review of the processes.
- In the current Internet Governance scenario, the structure and processes do not have the characteristics of CAS.
- Taking the example of the Service tier, we show how India would need to tailor its response for cyber-security from the perspective of CAS.

Structural Model: Multi-Tiered Approach (contd..)

Summary (contd..):

- Since cyber-security has ramifications beyond countries that may be involved on specific issues, India would need a framework that allows it to participate in established treaties.
- India could become a part of a process where established cyber-security frameworks could be leveraged to strengthen its own cyber-security as well as help it 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 Financial Action Task Force could be a basis for working on a cyber-security framework for India. (Indias experience with FATF) This approach requires India to have responsive organizations that need to be empowered to take the necessary decisions and be flexible in seeking support from teams for background work. Some of this support could come from established formal linkages while other parts could be through informal social linkages.

Source: (i) http://unctad.org/meetings/en/Presentation/dtl_eweek2016_JFernando_en.pdf, accessed on April 30, 2016.
(ii) https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Sri_Lanka.pdf, accessed on April 30, 2016.
(iii) http://www.fatf-gafi.org/, accessed on April 30, 2016.

Process Model: Framework for Perceived 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.

Process Model: Framework for Perceived Legitimacy (contd..)

- 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 explicit mechanisms to establish legitimacy and to be effective (Underhill and Zhang, 2008; DeNardis, 2010; Skogstad, 2011).
- 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.

Process Model: Framework for Perceived Legitimacy (contd..)

- 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 (Zurn, 2004; Buchanan and Keohane, 2006).

- 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, amongst others (Bernstein and Cashore, 2007). However, there is little work that integrates the various aspects related to legitimacy in the arena of Internet Governance.

Source: http://www.fatf-gafi.org/, accessed on February 20, 2015

Process Model: Framework for Perceived Legitimacy (contd..)

- 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 process framework for Internet Governance. This framework could also be used as a basis for evaluating the quality of any chosen approach.

Developing a Framework for India

- Based on the literature survey above and interviews conducted with different stakeholders.

- The proposed Perceived Legitimacy Framework (PLF) is the first step towards developing a process framework for Internet Governance. This framework could also be used as a basis for evaluating the quality of any chosen approach.

PLF

- **Participation**
  - *Openness to Participation:* by all relevant stakeholders. Perception of legitimacy reduced by exclusion. Further, openness to participation may be evaluated on the basis of:
    - *Diversity and Representativeness of Participation*
    - *Barriers to Participation:* capacity

PLF (contd..)

- **Agenda-Setting and Decision-Making Processes**
  - *Agenda-Setting:* bottom-up or top-down. A bottom-up process is viewed with higher legitimacy as it provides participants at all levels to contribute.
  - *Resolution:* Decision of dominant stakeholder Prevails? Resolution by consensus
  - *Preparedness and Level of Discussions*
  - *Accountability:* We examine the following dimensions:
    - *Transparency*
    - *Capture*
    - *Influence*

PLF (contd..)

- **Outcomes**
  - *"Bindingness" or Adoption Rate*
  - *Constructiveness*

Aligning Theory and Practice: Proposed Design

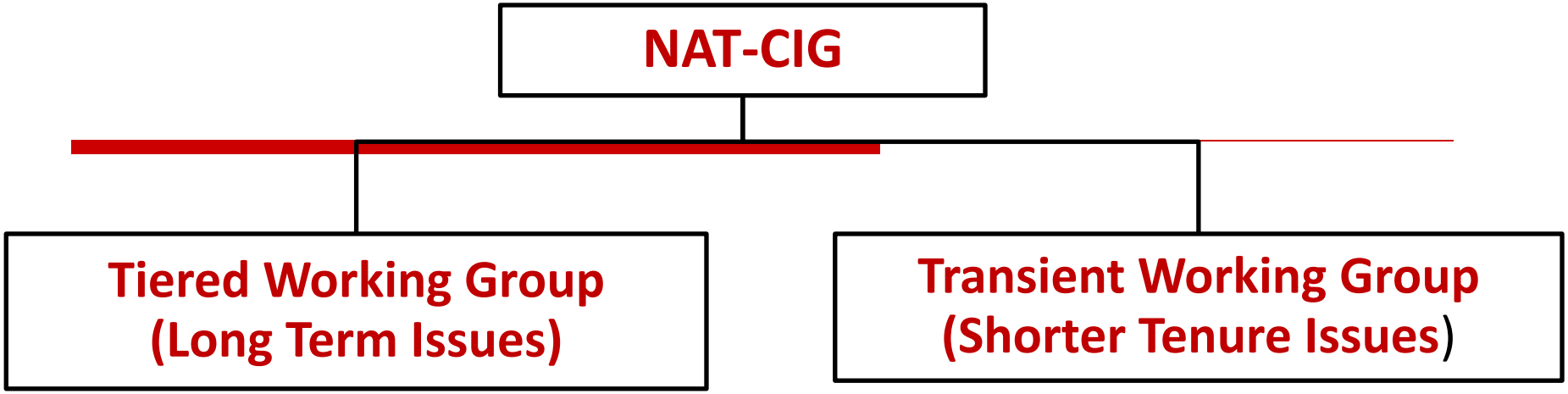
- A multistakeholder organization at the national level – National Council on Internet Governance (NAT-CIG). NAT-CIG would be an apex level Council that provides strategic directions and advises the Prime Minister on strengthening Internet Governance. It is designed to play a dominant role in Internet Governance at the domestic, regional and international level. This conceptualization gives coherence to India's role in Internet Governance by reducing the independent and ad-hoc role of various departments. It provides visibility at the national level and hence a signal about the significance of Internet to India's economy and security.

- There would be a multistakeholder representation from the DoT, DeitY, MEA, Ministry of Home Affairs, National Security Advisor, industry, civil society and academia. The suggested representation from various stakeholders reflects the democratic ethos of the country and the Internet. The composition of NAT-CIG should also find representation from all the tiers of Internet Governance outlined in the paper, i.e. the Infrastructure, Critical Internet Resources, Services, Applications and End-User tiers.

Aligning Theory and Practice: Proposed Design (contd..)

- At the second level, we propose a set of working groups (WG) delineated below. The NAT-CIG should operate through two types of WGs: (i) 'Tiered Working Groups' that deal with relatively longer term issues; and (ii) 'Transient Working Groups' that have a shorter tenure and would be dissolved, once the work is completed. Since creation or winding up of WGs ensures requisite focus and resources on the relevant aspects of Internet Governance, this is a self-organizing and flexible process. A periodic review of the existing WGs and their roles would enable the system to prevent proliferation of constituent modules and over modularization.

- The "Tiered WGs" would reflect the tiered architecture of the Internet, while the "Transient WGs" should reflect the current issues that have a specific time bound outcomes such as IANA transition, IPv6 migration etc.



- Infrastructure Tier (Exchange Points, Broadband Access, Access Standards)
- Critical Internet Resource Tier (DNS, IP Addresses, IDN, ccTLD, gTLD, Protocols, Standards)
- Services Tier (Security, Spam)
- Application and Content Tier (Intermediary liability, privacy, local language content, data localisation, network neutrality)
- End user tier (capacity and awareness building)

- Policy Issues
- IANA transition issues
- ITU Plenipot
- New gTLD applications
- Ipv6 Transition

Aligning Theory and Practice: Proposed Design (contd..)

- Each type of WG is envisaged as a multistakeholder, thus allowing for multiple perspectives. Such mechanisms allow for management of uncertainty (Holland, 2006; Ethiraj and Levinthal, 2004). WGs are envisaged as flat structures, with equality in level of representation from the constituent members. The interactions between working groups may happen through co-opted members from the external world or other WGs. This supports organizations in dealing with issues beyond their scope, by providing expertise from multiple sources. This mechanism allows for quick responses as there a few hierarchies. There could be concerns over the relative jurisdictions of the existing organizations such as DeitY, DoT etc. But since the WGs would work within the overall guidance of NAT-CIG, that has representation from the relevant departments coherence would be ensured.

Aligning Theory and Practice: Proposed Design (contd..)

- Further, NAT-CIG would be the body that would channelize response on all important regional and international issues. Since it is empowered to set up the required mechanisms either formally or informally for drafting responses, it could effectively deal with emergent issues. Since it has a multistakeholder composition, it would have access to a diversity of inputs, enabling integration of multiple perspectives. Since the NAT-CIG would operate through multiple WG, each of which is multistakeholder in its composition, NAT-CIG's response would be multi-layered and nuanced. This aspect is important when dealing with a rapidly changing uncertain technological and political environment.

- The tiered WGs help us to modularize Internet Governance by isolating the specific functionality and provide a basis for design that reduces complexity. It helps to define the scope of different entities.

Aligning Theory and Practice: Proposed Design (contd..)

- This mechanism of transient WG helps to operationalize the concept of self-organizing emergent entities in a CAS. By designing for such WG, there is a lot of flexibility to bring in responsiveness to emergent issues such as IANA transition. Details of the tiered and transient WGs are as follows:

'Tiered WGs'
(long term policy issues)

- Infrastructure Tier
- Critical Internet Resource Tier
- Services Tier
- Applications and Content Tier
- End-User Tier

'Transient WGs'
(current policy issues)

- WG on IANA Transition Issues
  WG on ITU Plenipot
- WG on WSIS 2015
- WG on New gTLD Applications
- WG on IPv6 Transition

Aligning Theory and Practice: Proposed Design (contd..)

- The Working Groups must mandatorily hold open consultations with all stakeholders including civil society, industry associations, academia, technical community, and the Government. The participation, agenda setting and decision making processes followed by NAT-CIG and its Working Groups would need to be accountable and transparent and should be evaluated using the Perceived Legitimacy Framework.

Summary

- The paper provides a theoretical basis for viewing Internet Governance. It models it as a CAS. Although CAS has been applied in several contexts, it has not been done in the context of Internet Governance to our knowledge. This is a contribution. On the basis of identified characteristics of CAS, the authors develop a structural and process model for Internet Governance for India. For the structural model, the authors developed a Multi-Tiered approach to Internet Governance organizations. For the process models, the authors developed the Perceived Legitimacy Framework. The suggested approach for India integrates both the structural and process models. Although, the paper is in the Indian context, it would find application in other developing countries that are also characterized by weak institutional infrastructure, lack of focus on Internet Governance and inadequate human resource capabilities.

Thank you