INDIA'S STAND ON INTERNET GOVERNANCE: OXYMORONIC OR OPPORTUNISTIC?

ASHISH GUPTA

The internet, as we know it today, is often hailed as a *beacon of knowledge*, a harbinger of freedom through empowerment, a strong proponent of freedom of expression and a place for exchanging ideas without fear of prosecution or punitive action. The birth of the internet shook the very foundation of sovereignty as propagated by the dominant 'Westphalian conceptions'. The internet was wild, unhindered and unencumbered by anyone or anything, transcending the physical boundaries with impunity and hubris. The virtual space used by the internet and its operatives became so well recognised that it was even christened with an appropriate name: cyberspace. Independence was the structural yarn used for weaving the fabric of the internet as we know it today. The agnostic nature of the standards and protocols used does not differentiate between creed, culture or countries. An attempt to block internet traffic is treated as a technology hitch and the traffic is rerouted through seemingly infinite networks. "The Net interprets censorship as damage and routes around it."[1] There is a widely held view that it "is not a physical place—it defies measurement in any physical dimension or time space continuum. It is a short-hand term that refers to the environment created by the confluence of cooperative networks

Wing Commander **Ashish Gupta** is Research Fellow at the Centre for Air Power Studies, New Delhi.

1. "John Gilmore's Maxim", http://techpresident.com/networked-public-sphere. Accessed on January 25, 2015.

During the 'the Cuban crisis', the lack of exchange of information, cogently and coherently, among several of the powers involved, exacerbated the situation and brought the world to the brink of a global nuclear war.

of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web."[2]

The precursor to the internet comprised collective efforts, in the backdrop of strategic imperatives of the US to design a system capable of withstanding missile attacks. The Cuban missile crisis of 1962 was arguably a catalytic factor that fuelled the dramatic development of the internet. During the 'the Cuban crisis', the lack of exchange of information, cogently and coherently, among several of the powers involved, exacerbated the situation and brought the world to the brink of a global nuclear war. Taking cognisance of its impact on the situation, under direct orders from President Kennedy, the National Security Council (NSC) constituted an interdepartmental committee to examine the communications networks and institute changes. In 1963, in order to provide improved communication support to critical government functionaries during emergencies, President Kennedy established the National Communications System (NCS). The NCS was mandated to link, improve and extend communications to components of various federal agencies, focussing on interconnectivity and survivability. In this backdrop, in August 1962, computer scientist JCR Licklider at the Massachusets (MIT) conceptualised the "Intergalactic Computer Network",[3] envisioning a global network of computers through which everyone could quickly access data and programmes from geographically dispersed sites. Later that year, Licklider moved over to the Defence Advanced Research Projects Agency (DARPA) to head the development project. In 1964, Paul Baran of the RAND Corporation, proposed architecture of a new kind of a network of computers, a packet-switched network, capable of surviving an enemy attack due to its inherent

2. Thomas C. Wingfield, "The Law of Information Conflict: National Security Law in Cyberspace", August 21, 2000.
3. "Internet Hall of Fame Pioneer J.C.R. Licklider", http://www.internethalloffame.org/inductees/jcr-licklider. Accessed on January 25, 2015.

resilience[4]. In 1967, driven by Licklider's vision and Baran's architecture, the Advanced Research Projects Agency (ARPA) embarked on a research project to build a network. The first four nodes of the ARPAnet became operational in early 1970. By 1981, the ARPAnet had grown to about 200 nodes and a basic suite of protocols (TCP/IP, FTP, Telnet, SMTP) was developed. During this time, the Europeans' endeavours in the field of networking culminated in development of the ISO (International Standards Organisation) seven-layer model of protocol architecture. By 1990, the emerging internet had grown to over 150,000 computers and was expanding exponentially.

In the year 1989, Tim Berners-Lee, a computer scientist specialising in networking, was working at the "Conseil Européen pour la Recherche Nucléaire" or European Council for Nuclear Research (CERN) in Switzerland. Using the initial vision of Licklider and Nelson as the springboard, he proposed a paper on information management systems that discusses, "The Problems of Loss of Information About Complex Evolving Systems and Derives a Solution Based on a Distributed Hypertext System."[5] Though it was termed as *"vague, but exciting"* by his boss, Berners-Lee was permitted to continue on the project. By 1990, Berners-Lee could define the web's basic building blocks, the URL, http and html and wrote the first browser and server software. Working on the 'NEXT' computer at CERN, he named the first web server as 'Info.cern.ch' and the world's first web page was addressed as 'http://info.cern.ch/hypertext/WWW/ Project.html', containing information and details of the world wide web project. As CERN was primarily using particle accelerators and detectors to boost beams of particles to high energies and was at the helm of high-energy-physics, in 1991, an early version of a world wide web system was released to the high-energy-physics community that included a simple browser, server software and a library of essential functions for designing custom software. In 1993, CERN put the web in the public domain, ensuring that it would remain an open standard and released the source code of Berners-Lee's hypertext project, 'World Wide Web' on the same day. The move, while heralding the expansive and unhindered growth of the internet,

4. "Paul Baran and the Origins of the Internet", http://www.rand.org/about/history/baran.html. Accessed on January 25, 2015.
5. "The Birth of the Web", http://home.web.cern.ch/topics/birth-web. Accessed on January 25, 2015.

The internet, conceived in the era of limited computing and time-sharing, has not only survived, but thrived, and has grown by leaps and bounds. New technology, standards of networks and computational methodologies, have been seamlessly adopted and assimilated by the internet.

saw the 'World Wide Web' accounting for most of the internet traffic.

On October 24, 1995, the Federal Networking Council (FNC), in consultation with members of the internet and intellectual property rights communities came up with the definition of the term "internet"[6]. As per the definition, the "internet" refers to the global information system that:

- Is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/ follow-ons.
- Is able to support communications using the Transmission Control Protocol/ Internet Protocol (TCP/IP) suite or its subsequent extensions/ follow-ons, and/or other IP-compatible protocols
- Provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein.

The internet, conceived in the era of limited computing and time-sharing, has not only survived, but thrived, and has grown by leaps and bounds. New technology, standards of networks and computational methodologies, have been seamlessly adopted and assimilated by the internet. An enterprise conceived, developed and nurtured by a small group of dedicated researchers, from a humble beginning has grown to become an all pervasive entity intricately woven into the fabric of the social and political life of all *inhabitants of this planet*. A sterling example of commercial success, the internet dictates the way businesses are negotiated, facilitated and conducted. If we take into account the indelible impact of the internet on today's society, the issues related to its management and governance become paramount over insular and parochial interests of *individuals, societies and nations.*

6. "Definition of Internet", https://www.nitrd.gov/fnc/Internet_res.aspx. Accessed on January 25, 2015.

INTERNET GOVERNANCE

Since the time the internet made its foray into the public domain and opened to commerce, the term "**internet governance"** has evolved. The term, at first referred to the policy issues for its portability, operability, sustenance and reliability, and later encompassed the issues related to management of domain names and IP addresses. As the internet became ubiquitous, the definition also broadened considerably. In 2005, the UN-sponsored World Summit on the Information Society defined internet governance as "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the internet." [7] An equitable distribution of internet resources, unfettered and multilingual access to all and a stable and secure functioning of the internet constitute the core of internet governance .

However, some nations are wielding the internet's unprecedented growth to extract greater political and economic mileage in international arenas. The issues related to internet governance have become highly contentious and political, leading to acrimonious confrontations between the developed and developing states. Technologies over which the internet rides and resides in, historically, came into being during the initial development, consolidation and refinement phases. With the emergence of new challenges such as freedom of expression, internet infrastructure security and stability, the policy role of internet companies, efficacy of internet protocols, internet control systems such as the Domain Name System (DNS) and the relationship between intellectual property rights enforcement and internet architecture, the issue of internet governance has become more complex and variegated. Preservation of national security, protection of economic interests, prevention of societal disharmony and containment of internal dissident elements are some of the concerns, adding further complexities to the already tumultuous realm of internet governance.

At the heart of internet governance is designing and administration of the technologies necessary to keep the internet operational followed by a formal and substantive mechanism governing the use of these technologies. This

7. Château de Bossey, "Report of the Working Group on Internet Governance", June 2005, p.4.

At the heart of internet governance is designing and administration of the technologies necessary to keep the internet operational followed by a formal and substantive mechanism governing the use of these technologies.

technical scaffolding involves critical internet resources, technical standards for integrity and interoperability, interfaces for man-machine interaction such as search engines, information access and exchange points, etc. Some of the challenges which need to be addressed before a consensus and conceptual framework for internet governance may be built are given below.[8]

Agnostic Arrangement of Technical Architecture

The technical foundation used to build the internet may appear pragmatic and agnostic in nature, free from the shackles of political and cultural imperatives. However, as Jasanoff puts it, technology "both embeds and is embedded in social practices, identities, norms, conventions, discourses, instruments, and institutions—in short, in all the building blocks of what we term the social." [9] Technology, *per se* is an inanimate entity used as a tool to set in motion, and to sustain, the momentum generated by the internet. Internet governance decisions are often based as much upon technological imperatives as on how to regulate and control the usage of these. For example, technology dictates that the domain name and corresponding internet address need to be globally unique, but allocation and control call for institutional coordination and control. The issue has become central to the global struggle for internet governance since the early 1990s.

Use of Internet Governance Technologies for Content Control and Information Censorship

The enactment of policies governing the use of internet technologies for content control and censorship has become the norm, albeit a draconian one, among many nations. In the garb of intellectual property rights protection, law enforcement functions or for strangulation of voices calling for political reforms, internet governance technologies are increasingly leveraged to curtail

8. Laura Denardis, *The Global War for Internet Governance* (Yale University Press, 2014), p.7.
9. Sheila Jasanoff, *States of Knowledge: The Co-Production of Science and the Social Order* (Routledge, 2004), p. 3.

free flow of information and for content control. Traditionally, institutionalised centres of power have resorted to censorship of information and after sieving the information through the mesh of their perceived values and interests, made it accessible to the masses. The internet has deprived these centres of the power of being selective or in denial mode about information and its flow deemed detrimental to their core interests. Internet governance infrastructure is routinely used to block, filter or censor access to information, to disseminate misinformation or to create a system of mass surveillance.

Traditionally, institutionalised centres of power have resorted to censorship of information and after sieving the information through the mesh of their perceived values and interests, made it accessible to the masses.

Privately Owned and Controlled Internet Governance Technologies

Historically, most internet governance functions were executed out of the domain of governments, via private ordering, technical design and new institutional forms. Internet governance policies were enacted in specific contexts of technological and social change. Sovereign governments, in an effort to regulate activities within or through their boundaries as constitutionally legally mandated or otherwise, oversee many internet governance functions such as enactment of laws against cyber crime, cyber terrorism, espionage, computer fraud or social disharmony.

Internet as an Instrument in Global Conflict

The use of the internet as a tool by exploiting its implicit character via technology, policy formulation and restrictive regulation, for political, commercial and security reasons, has given rise to global tensions. In a blatant digression from its promised goal of upholding democratic values and freedom of expression, internet governance control is being used for content censorship, mainstream media control, mass surveillance of citizens and shaping the public opinion for the furtherance of nefarious designs. Central to internet governance are conflicts over issues of ethicality, morality, cultural and political rights, intellectual

property rights protection and national security.[10] Earnest efforts for conflict resolution over these issues require technical innovation, governments' intent and private participation. Articulation and implementation of policies and procedures to have internet control/regulation points directly have exacerbated in building up global tensions.

Parochial Geo-political Outlook in Internet Globalisation

The stability and security of the internet is in the common interest of all nations. Nations have to deal with enduring global problems such as terrorism, environmental degradation, climate change and contagious diseases, which require cumulative, collective and congruent efforts. While losing sight of greater goals, the petty squabbling to grab a larger share of the pie over internet governance is denying the global aggrandisement of internet governance .

Globally, a loose consensus, comprising certain shared fundamental economic, political and social beliefs, is developing to unshackle the internet from the historic and hegemonic control of US companies supposedly protecting US interest. Central to this debate is disagreement among many internet governance stakeholders over who controls the "Critical Internet Resources (CIR)." Though not physical, these virtual resources are finite and indispensible for use, access and operation of the internet. Without the virtual resources such as internet addresses, domain names, and Autonomous System Numbers (ASNs), even with the swankiest computer and high speed fibre optic network, the internet will be as elusive as the proverbial unicorn.

An Internet Protocol (IP) address is a numerical value assigned to each device (e.g. computer, printer) willing to be a part of a network that uses the Internet Protocol for communication. Every device accessing the internet requires a unique binary number called an IP address. The domain names provide a humanly recognisable and easily memorable form, dispensing with the requirement of making sense of an esoteric string of binary numbers. Domain names, such as www.google.com are used to locate web sites. When a domain name is typed into a browser address bar, the internet's Domain

10. Ibid.

Name System (DNS) translates this name into unique binary numbers for locating the web site. An ASN is a binary number assigned to a network operator that connects to the global internet. These network operators are usually described as autonomous systems. ASNs are valuable because receiving a globally unique ASN is a prerequisite for an internet service provider's network to become part of the global internet.

The structural framework over which the internet governance infrastructure is stitched together came into being as part of viable and workable technological solutions. No legal or commercial considerations were factored in during the development phase. The growth and transnational reach of the internet has seen significant changes in objectives, roles and administrations of institutions responsible for coordinating CIRs. Understanding the functioning of these groups involves circumnavigating through an acronym thicket of global institutions, including Internet Assigned Numbers Authority (IANA), Internet Corporationf for Assigned Names and Numbers (ICANN), Regional Registration Registries (RIRs), root zone server operators, domain name registrars, registries, and various other entities. The nuances of internet governance can be captured by familiarisation with institutional structures that centrally oversee critical internet resources, control root zone files, operate DNS servers, manage registrar systems for assigning domain names and distribute internet numbers via RIRs.

IANA AND ICANN

In early internet history, management of names and numbers began with a single person. Christened as "God of the internet", Jon Postel, a computer scientist from the University of South California (UCLA), who was involved in early work of the ARPANET, along with his colleagues, performed the role of the central coordinating functionary for assignment of names and numbers. As the Internet Assigned Numbers Authority (IANA), Postel and his colleagues, under contract with the US Department of Commerce, were responsible for:

- The coordination of the assignment of technical internet protocol parameters.
- The administration of certain responsibilities associated with the internet DNS root zone management.

Formed in 1998 under a contract with the US government, ICANN is a private, non-profit entity with an official mandate to provide technical coordination of core internet resources, most notably domain names.

- The allocation of internet numbering resources.
- Other services related to the management of the Address and Routing Parameter Area (ARPA) and INT Top-Level Domains (TLDs).[11]

Though the work was crucial, it was bereft of any major controversy. During that period, the network was primarily an American phenomenon and was yet to realise its full potential of having a global presence, and close to four billion users. IANA eventually became a function under the Internet Corporation for Assigned Names and Numbers (ICANN). Formed in 1998 under a contract with the US government, ICANN is a private, non-profit entity with an official mandate to provide technical coordination of core internet resources, most notably domain names. Though incorporated in the state of California, it wields considerable authority, directly or indirectly, over all users of the internet. To rein in unbridled growth of the internet without order and regulation, ICANN is mandated to create, enact and promulgate enforceable regulations. However, depending on one's frame of reference, the creation and functioning of ICANN can be prescribed as a panacea for, or branded as the root cause of, the ailments.

Transition of communications over the internet is different from our understanding of the classical communication process, which requires establishment of a dedicated channel over which transition of information takes place as one unbroken entity. Over the internet, messages are broken up into manageable packets and are exchanged over many independent networks following different paths, from source to destination. The lack of a central communication channel or information pathway makes the process of policy promulgation and enforcement across all the information traffic over the internet extremely difficult. ICANN realises this through its control of the

11. "C.2.9 of Contract Between US Department of Commerce (DoC) and Internet Assigned Numbers Authority (IANA) dated Jul 02, 2012", http://www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_ sacs.pdf. Accessed on January 30, 2015.

internet's DNS. Internet addressing, as realised in the DNS, is centralised and provides the control point from which to regulate users. Denial of access to domain names is the equivalent to declaring someone a pariah from the internet community. The DNS also defines jurisdictions on the internet. The logical organisation of the DNS allows authority to be mapped onto distinct zones. Collectively, these features render ICANN capable of governance .

The lack of a central communication channel or information pathway makes the process of policy promulgation and enforcement across all the information traffic over the internet extremely difficult.

ROOT ZONE MANAGEMENT

Root zone refers to the highest level of the DNS structure. It contains the names and the numeric IP addresses for all the top level domain names such as the Generic Top-Level Domain (gTLDs) (.com, .net, .org, .jobs), and all the Country Code Top Level Domains (ccTLDs), for example (.us, .uk .ph), including the entire list of all the root servers.[12] "Root Zone Management" involves the processes by which changes are made to the root zone file and root WHOIS (a query and seek protocol for querying databases of registered users of the internet resource). Root zone management involves three roles performed by three different entities mandated to do so under the provisions of legal agreements.

- IANA is responsible for managing the content of the root zone based on the policies adopted by ICANN. It transmits requested changes in TLD data to the Root Zone Maintainer (Verisign) and the Administrator (NTIA).
- The NTIA as administrator approves any changes, additions or deletions from the root zone file.
- Verisign under a cooperative agreement with NTIA, performs the role of the root zone maintainer. After approval from NTIA, Verisign implements changes in the root zone file. While IANA is supposed to determine the *content* of the root zone file, VeriSign actually edits the root zone data, cryptographically signs it and distributes the resulting content to the root server operators.

12. "Root Zone", http://icannwiki.com/index.php/Root_Zone. Accessed on January 25, 2015

Operation of the Root Name Servers

The root zone files are contained in a group of servers for distribution of this information to the world. This system of root name servers is controlled by 12 organisations with 13 distinct root server implementations. Each of the root name servers contains the most current root zone database. These root servers are the gateway to the DNS so operating these servers is a critical task involving great responsibilities in both logical and physical management. Many of these server implementations are operated by American institutions such as governmental agencies, including the National Aeronautics and Space Administration (NASA) and the Department of Defence (DoD), American universities, including the University of Maryland, and corporations, including VeriSign and Cogent.

CONTROLLING INTERNET NUMBER DISTRIBUTION

Internet access is possible only with a legitimate IP address, which is usually provided through an Internet Service Provider (ISP). ISPs are generally allocated with a block of IP addresses for sub-division. In addition, to be a network operator further requires an ASN. The organisations that control the allocation and assignment of these numbers serve an essential internet governance function. IANA has retained its historic role as the organisation centrally responsible for allocating IP addresses and ASNs, albeit now formally under the auspices of ICANN. IANA, in turn, delegates reserves of addresses and assignment authority to five Regional Internet Registries (RIRs), central and influential institutions in the internet governance landscape. For example, APNIC (Asia-Pacific Network Information Centre) has been delegated with the responsibility of the Asia-Pacific regions. These RIRs, in turn, allocate address space to Local Internet Registries (LIRs) or selected National Internet Registries (NIRs) for further allocation or assignment to ISPs and end user institutions. For example, the Indian Registry for Internet Names and Numbers (IRINN) provides allocation and registration services of IP addresses and AS numbers in India.

CRITICAL INTERNET RESOURCES (CIR) MANAGEMENT

The availability and accessibility of CIR, coupled with historical aspirations

and future premises, has triggered a high profile, prolonged and hostile debate over centralised control, consensually agreed regulations and enactment of legally binding rules. A number of formally enacted agencies as well as a multitude of loosely connected organisations are providing platforms for debating internet governance issues, championing the cause of specific groups of stakeholders. Topping them all is the lack of consensus over the acceptance of a global model for internet governance. The proponents and opponents of the 'multi-stakeholder' model and 'multilateral' model are at loggerheads with each other. There is still another school of thought, propounding the idea of identifying the internet as one of the 'Global Commons' at par with the high seas; the atmosphere; Antarctica and, outer space, outside of the political reach of any one nation-state. Many advocate the 'multi-stakeholder model' in which all stakeholders, whether from the private sector, government, academia, civil society or non-governmental organisations, participate in the policy development process. The multilateral model provides a level playing field for participants in which all participants, large and small, have an equal say in policy decisions.

NETMUNDIAL

Edward Snowden's revelations comprised a defining moment in more ways than one. These have amply demonstrated that internet technologies, though transformative and emancipatory, have existential and potential risks to cause global disharmony. The general disposition among those who feel alienated and angry after the Snowden revelations can be gauged by the tone and tenor of discussions at the NETmundial on the "International Telecommunication Union (ITU) Plenipotentiary in November 2014" in São Paulo, Brazil, on April 23 and 24, 2014. In Portuguese, "NETmundial" implies the future of internet governance. On the implementation of a different model of internet governance, the Brazilian government and representatives of the European Commission articulated that internet governance should be:

- Open, multilateral and democratic governance , carried out with transparency by stimulating collective creativity and with the participation of society, governments and the private sector;

- A real multi-stakeholder governance model based on the full involvement of all relevant actors and organisations[13].

During the NETmundial, a roadmap for a different model of internet governance was proposed, incorporating the following:

- Combating all violations of human rights in cyberspace;
- Consolidation of a decentralised multilateral internet governance, interoperable and truly established in a consensual way with all users of public space: the governments, the entrepreneurs of the private sector and the civil society organisations;
- Guarantee of defence of net neutrality, against the restrictions arising from the economic interests of some monopolies in the business of telecommunications;
- Construction of mechanisms to prevent the illegal practices of surveillance and espionage of military and private industries in cyberspace;
- Restoration of confidence, credibility and tranquillity in cyberspace, from the creative and collective work maintained by the representative actors of governments, entrepreneurs of the private sector and civil society organisations.[14]

INDIA AND INTERNET GOVERNANCE

India in its official submission at the NETmundial, while acknowledging the importance of an open, stable and secure internet as crucial to global connectivity, innovation and economic development, recommended a transformational shift from the internet of today to the "Equinet" of tomorrow. While proposing the structure of internet governance as multilateral, transparent, democratic and representative, with the participation of governments, the private sector, civil society and international organisations, in their respective roles, India acknowledged these as the foundational principles of internet governance.

Prior to NETmundial, at the World Summit on the Information Society (WSIS), the endorsement by the UN General Assembly of the "Tunis Agenda

13. "Roadmaps for a Multilateral Decentralized Internet Governance ",http://content.netmundial.br/ contribution / roadmaps-for-a -multilateral-decentralized-internet-governance/217". Accessed on January 25, 2015.
14. Ibid.

for the Information Society' of 2005 saw the creation of the 'Internet Governance Forum' (IGF) as a platform for a multi-stakeholder policy dialogue. The IGF aims to provide a unique multi-stakeholder platform for the discussion of public policy issues related to key elements of internet governance in order to foster the sustainability, robustness, security, stability and development of the internet.[15] In its official statement at the NETmundial, India endorsed, "International law and in particular the Charter of the United Nations, is applicable and is essential in maintaining security and stability and promoting an open, secure, peaceful and accessible ICT environment. All governments should have an equal role and responsibility for ensuring stability, security, and continuity of the internet."

India is at pole position to swing the outcome of any debate on internet governance. India's assertive role in this respect is highlighted by the opening statement made by the Indian representative at the NETmundial, "With over 200 million internet users, soon going to cross half a billion in the coming years, over 900 million mobile telephone subscribers, and a thriving and robust internet ecosystem, India is well poised and willing to play an important and constructive role in evolving the global internet governance ecosystem and in the process, make it more credible."[16] Though the representatives did not support the consensus view on the NETmundial outcome document, India's active participation was a measure of willingness to bridge the "trust deficit". India's position on the future of internet governance at the NETmundial can be gauged by the following official statement:

- The global credibility and universal acceptability of the internet governance ecosystem is possible if it is "representative, democratic, transparent and accountable, involving governments and other stakeholders as per the Tunis Agenda"[4].
- The second is that "given its profound importance, there is also a need for the various facets of the [*sic*] internet governance , including the core

15. "World Summit of the Information Society WSIS Action Lines Executive Summaries (Achievements, Challenges and Recommendations) WSIS+10 High-Level Event Geneva 2014", www.itu.int/wsis/review/ inc/docs/phase6/v/r /wsis10-5-3.pdf. Accessed on January 25, 2015.
16. "Statement by Mr Vinay Kwatra, Indian representative at the Global Multistakeholder Meeting on the Future of Internet Governance in Sao Paulo (April 23-24, 2014)", http://mea.gov.in/ Speeches-Statements.htm? dtl/23246/Statement+ by+Mr+Vinay +Kwatra+Indian+represent ative+at+the+Global+ Multistakeholder+ Meeting+on+the+Future+of+Internet+Governance +in+Sao+Paulo+April+2324+2014. Accessed on January 25, 2015.

The global credibility and universal acceptability of the internet governance ecosystem is possible if it is "representative, democratic, transparent and accountable, involving governments and other stakeholders as per the Tunis Agenda".

internet infrastructure, to be anchored in [an] appropriate international legal framework"[5].

These two statements echo the Indian government's resolve to tackle "strategic and policy challenges" to bring in more credibility and transparency in the global internet governance ecosystem. It unequivocally raised the following concerns:

- Lack of a truly representative and democratic nature of the existing systems of internet governance, including the management of critical Internet resources leading to a trust deficit in the system;
- Need for the internet governance ecosystem to be sensitive to the cultures and national interests of all nations, not just of a select set of stakeholders;
- Apparent inability of the current structures of internet governance to respond to some of the core and strategic concerns of the member states;
- Need to broad base and internationalise the institutions that are invested with authority to management [*sic*] and regulate the internet.[17]

The inequitable distribution of power in managing the internet resources and greater influence wielded by a few have been some of the reasons for the discord for India and other developing countries since the Tunis phase of the WSIS. Globally, a loose consensus, comprising certain shared fundamental economic, political and social beliefs, is developing to unshackle the internet from the historic control of a few. However, replacing the multi-stakeholder and dispersed model of internet governance with a centralised model may not translate into empowering the users. Government led control may be used to limit, restrict or deny the content on the internet. This will result in strengthening the "content control mechanism" at least in countries with oppressive, autocratic and oligarchic governments.

17. Ibid.

MULTI-STAKEHOLDER Vs MULTILATERAL MODEL OF INTERNET GOVERNANCE

On the issue of internet governance, the terms 'multi-stakeholderism' and 'multilateralism' have been used in many platforms by the Indian government. Both terms have evolved contextually in reference to the internet governance ecosystem over the last decade. Multi-stakeholder organisations such as ICANN have brought in a mechanism to improve its accountability. The UN has also acknowledged multi-stakeholderism through the 'Multi-stakeholder Preparatory Platform' for the WSIS+10 High Level Event in June 2014. There is wider acceptability towards consequential contributions made by non-government stakeholder groups. India, while commenting on the NETmundial draft outcome, noted: "There are no references to the Geneva Principles as well as the Tunis Agenda which form the bedrock for the ongoing global discourse on internet governance. Despite a clear recognition in the Tunis Agenda to a multilateral process apart from the multi-stakeholder approach in the evolution of the future roadmap on internet governance, we find no reference to it in this initial draft outcome document which you are considering now."

The Government of India, while articulating the model for the internet governance ecosystem, has reiterated "full involvement of governments and all other stakeholders". In other words, India is not entirely impervious to acceptance of some form of multi-stakeholderism – albeit as encapsulated in the Tunis Agenda. The limitation of this approach is that the "Tunis Agenda" acknowledges the role of civil society as a contributor "at community level"[14] only without defining the role it can have in policy-making. Moreover, in the NETmundial outcome, the Government of India's request for the incorporation of the provision of "sovereign right of governments as international policy authority for internet-related public policy issues" was also not entertained.

India's stand on internet governance can be gauged by its official position at various international platforms for debating the issue. At times, India may seem to have left little room for manoeuvre towards advocacy of the multi-stakeholderism model, central to its position on the "role of civil society' and 'assertion of state sovereignty over international internet -related public policy issues". Acceptance of India's viewpoint and its assimilation in policy

formulation in future may be speculative at this point of time. However, there is a global acceptance that the existing internet governance ecosystem needs reforms, irrespective of these being multi-stakeholder or multilateral in nature.

CONCLUSION

Internet governance is a highly complex and ever evolving form of governance which requires cognitive and technical scaffolding and Information and Communications Technology (ICT) resource management to fulfil the aspirational goals of civil societies, uphold civil liberties, and address national security imperatives. From being executed under the supervision of one person, today its enormous complexity has rendered even a multitude of agencies grappling to find viable and workable ways to make the internet governance ecosystem globally acceptable to all users. The policy-making has also evolved from predominantly US institutions to new global entities. India is at the cusp of the digital revolution and at pole position to swing the outcome of any debate on internet governance. The year 2015 will see many critical issues for internet governance being discussed globally. The WSIS is scheduled to provide the reviewed goals and envisaged policy framework to the UN General Assembly. The contract between the US Commerce Department and ICANN will expire in September 2015 and as per the US assertion,"It (US) would eventually transfer key internet domain name functions to a global multi-stakeholder community." In an official release, Dr. Stephen D. Crocker, chairman of ICANN's board, said, "Even though ICANN will continue to perform these vital technical functions, the US has long envisioned the day when stewardship over them would be transitioned to the global community. In other words, we have all long known the destination. Now it is up to our global stakeholder community to determine the best route to get us there."[18] India needs to leverage this opportunity for furtherance of its envisaged objectives for internet governance by formulating a coherent policy and creating a team of technocrats, diplomats and members from academia for spearheading its efforts.

18. "Administrator of Domain Name System Launches Global Multistakeholder Accountability Process", https://www.icann.org/resources/press-material/release-2014-03-14-en. Accessed on January 28, 2015.