THE INTERNET AND ITS GOVERNANCE: Comparative Approaches in India and China

M.M.K. Sardana*

[***Abstract:*** *India joined the internet bandwagon ahead of China. However, China overtook India soon on the strength of its advanced telecommunication infrastructure and strong base in electronics manufacture and also because of its systemic advantage of taking and implementing decisions. India, on the other side, was in an advantageous position in terms of deriving immediate benefits by increasing its software exports because it not only had the requisite trained manpower, but also emerged as an able partner in the value chains headed by multinational software companies. China foresaw that the free flow of information on the internet may not be conducive to its political system; however, they could not afford to miss on the internet, sensing it as an inescapable tool. The challenge posed by their state motivated them to develop their own numbering system on the lines of the International Numbering System, enabling them to come up with their very own national internet system with powerful servers of international standards. The web feeds using international internet were to be channeled through government controlled companies. Thus, the Chinese developed a firewall to regulate the flow of information on the internet. Challenging the American hegemony of the name and numbering system and related internet protocols, the Chinese honed their expertise by interacting with ICANN, which was, to an extent, established for setting up independent systems. The Chinese approach to internet governance is centered on the sovereignty of nation states in their respective cyberspace with freedom to control the flow of information to preserve the order of their societies. The Chinese have come to occupy a position of eminence in the internet world in terms of growth and penetration. They have not only made tremendous economic gains and built up a strong scientific and technical base, but also assumed capacity to preserve the integrity and stability of the internet. It is adherent to the intergovernmental control under the aegis of the United Nations for the administration of internet resources. India has also been in favour of the governance of international internet under the aegis of the United Nations in terms of the mandate accorded by the World Summit on Internet Service (WSIS) and the UN World Group of Internet Governance (WGIG)—falling short of advocating UN control of technical arrangements as exist currently. Because of its poor manufacturing base in electronics and less than adequate telecommunication infrastructure, India has been lagging behind China even though it may soon surpass the US in terms of internet access. Inadequacy in manufacturing base and other infrastructure have left India far behind when it comes to competency to combat cybersecurity and cyber-related crimes. This has impelled India to seek greater access to the DNS system and to bring it under the UN regime.*]

India joined the internet bandwagon in 1988, six years ahead of China. However, by 1999, China raced ahead of India in the field of internet in all its dimensions[1]. Ever since, China remains in the lead and the latest statistics reveal that the "lead" by

* The author is a Visiting Fellow at the Institute.

1、Press, L., W. Foster, P. Wolcott and W. McHenry (2003), 'The Internet in India and China,' *Information Technologies and International Development*, Vol. 1, No. 1, Pp. 43–60.

China has significantly widened. The projected trends made for the year ending in 2018 also emphasize that the trend of increasing differentials would continue despite the digital India initiative being undertaken during the period 2015–18[2]. According to a study conducted in 2003[3], the following underlying factors were identified for driving the growth of internet in China:

I) China decided to accord priority to internet development from the earliest stages of its introduction.
II) China's economic reform initiatives, commencing in early 1980s, provided both the capital and the openness to internet.
III) China has already created a robust infrastructure of telecommunication and is providing optimum support for rapid growth of the internet.
IV) The faster diffusion of internet was made possible because the Chinese were able to execute their action plan through decree rather than spending their time and resources for consensus building among stake-holders.
V) China devised a mechanism to generate competition among the then-existing government companies, thus saving on time required to bring about legislative changes for raising private capital.
VI) The Chinese were able to establish competitors to the incumbent telephone companies relatively rapidly.

The Chinese have been alive to the realities of their political system, requiring the regulation of information flow both within and outside their domain. Therefore, right from the very beginning in 1990, the Government of China set up four state-owned entities to provide internet access throughout China; this arrangement has persisted post 1997 when private internet access was permitted. While the Chinese government has kept ownership and control over the access routes to the internet, it allows private enterprises and individuals to rent bandwidth from state-owned enterprises. The state-controlled entities own the physical backbone of the internet in China, which is very different from other countries, including that in India where

[2] Mahajan, Ambika C. (2014), '3.6 Billion Active Internet Users Worldwide By 2018 With Nearly 50% Penetration!,' Dazeinfo, November 26.
[3] *Op. cit*. 1

private internet service providers compete with each other under the jurisdiction of the state. Thus, the Chinese government has an effective control on everything that happens in the cyberspace. The internet in China is run on state-owned hardware servers, state-owned fiber optics, via state-owned switches, and is "government allowed". For establishing an enabling infrastructure, China injected a large amount of money—to the tune of 4.3 million Yuan—from 1997 to 2009 into building a nationwide optical communication network with a total length of 8.267 million km[4]. This type of control that the Chinese government exercises on the internet has led to a quasi-separation from the rest of the world[5].

India, on the other side, was open to the idea of developing an international gateway market and by 2002, had granted permission to operate 55 international gateways in 17 cities. Many government and private organisations have been engaged in managing international gateways. Service providers are free to directly purchase capacity from undersea cable operators. Freedom was given for installing VSAT internet connection. VSAT has played an important role in India since 1999 because there was little international cable connectivity[6]. In the field of internet there was no denial regime to which India had been earlier subjected to when it wanted to foray into frontier areas like nuclear energy. Sourcing of equipment for the internet was not a problem. Also, India did not face the usual challenge of developing indigenous technologies to circumvent the denial regime and did not care for developing controls as envisaged by the Chinese. Rather, following an initiative of the Electronics Commission of India, easy availability of hardware for creating internet infrastructure provided opportunities for development of indigenous manpower, equipped with knowledge base and intellectual capital. The Electronics Commission in the early seventies had proposed setting up hubs of manpower development and infusion of informatics and technology into local economic processes in preference to developing large-scale hardware production base. Implementation of this policy of the Electronics Commission along with the creation of supportive institutional bases

4 *Ibid*.

5 Herold, David. K. (2011), 'An Inter-nation-al Internet: China's Contribution to Global Internet Governance?" Social Science Research Network, September 5.

6 *Op*. *cit*. 1

such as CMC (Computer Maintenance Corporation Ltd.), NIC (National Informatics Centre), Tata-InfoTech, Patni Computer Systems and Wipro in government and private sectors helped build a strong base of software service providers. The aforesaid single decision of the Electronics Commission has been in the nature of modifying the earlier emphasis on electronic design, manufacturing and semiconductor technology and would be somewhat accountable for India missing the microchip revolution that propelled Hong Kong, Singapore, Taiwan, South Korea and later China to leadership positions in electronic manufacturing in the world. During the 1980–90 decade, Japan and China collaborated to develop critical technologies relating to fabrication, electronic design and production, thus paving the way for a high performance engine to boost the growth of the electronics manufacturing industry. China went on to consolidate its gains by providing institutional backup in relevant subsectors, including in Information Technology. In 1997, when the Ministry of Industry and Information Technology was created in China, it had a strong manufacturing base at its command. Another initiative that China took in the 1980 decade was to do away with the telecommunication deficit when the Chinese government decided to import programme control switching devices, and later license or produce them domestically. It laid the nationwide network of telecommunication. By 1990s, the Chinese government had made the development of indigenous telecommunication equipment a national priority; and, the results are astounding[7].

Thus, when internet emerged in India followed by China a few years later, the Indians lagged behind because of deficient electronic manufacturing and telecommunication infrastructure compared to the Chinese. This edge over India proved beneficial for the Chinese in terms of providing a sound base for accelerated growth in internet penetration. The Chinese had considerable competence in the area of hardware based infrastructure—a requisite to developing their own network while maintaining sovereignty on the internet as well as controlling information flow. However, on the other side, India had an edge over China in terms of contribution to

[7] Swaminathan, R. (2014), 'India's Electronic Sector: Policies, Practices, and Lessons from China,' Observer Research Foundation, ORF Occasional Paper No. 52, June.

software development. Further, the advantage of a large pool of English-speaking manpower also complemented India's edge over China in the area of software development. For developed country entities, Indian companies became a preferred destination for collaboration for value added software development. There is data available to demonstrate that the differential between India and China with regard to hardware is widening whereas China is fast catching up with India in software development capacity.

As for the status of internet in China, the Chinese internet companies face no competition from international giants like Google, Yahoo and Twitter, thus pushing the frontiers of innovation; a comment on the fact that the presence of international giants had made a material difference to how Indian companies have fared. The Chinese have taken advantage of their lack of English language proficiency. That is, the sites that fare really well in China are the ones running in a Chinese-language parallel universe, which serves as a "linguistic Great Wall" for foreign players. Scholars observing the Tech Race in Asia have noted that the difference between internet infrastructure in China and India is what leaves China better positioned for growth. India is now in the process of auctioning telecom spectrum in high frequency range—almost two decades after economic liberalization was first ushered in. And even now, services have not been rolled out, given the absence of adequate infrastructure[8]. While on the one hand Indian policy makers are wary of foreign investment in print and electronic media, on the other hand, the world of internet lends itself to unhindered foreign direct investment. This is to say that though it leads to more and more innovation, the inadequacy of such investments because of policy constraints prevents free play in the process of innovation. Even in China, the homegrown internet companies like Youku Inc. (user-generated video portal, modeled on youtube) and Ren Ben Network (a social networking site similar to Facebook) are mere clones of top international sites.[9]

[8] Bose (2012), 'China's Online Revolution is Growing and India is Nowhere Close,' TECH2. Available at: http://tech.firstpost.com/news-analysis/chinas-online-revolution-is-growing-and-india-is-nowhere-close-209597.html

[9] *Ibid*.

On the wings of a strong infrastructure base and with a proven capacity to develop their own networks in competition to the technical infrastructure supporting the international internet, the Chinese have seamless avenues for innovation in the frontier areas of networking and the internet. Despite massive differences in their approach towards international internet governance (this aspect would be dilated later in this Note), China and the US have never been as closely interconnected as in cyberspace. That is, China is the biggest overseas market for American internet companies and almost all leading US companies have made great profits in China. Nearly a thousand US investment funds have designated China as their priority, reaching every corner of the Chinese internet market and accounting for more than half of their total overseas investment in the field. The success or failure of some of the US companies is closely related to the Chinese market. The US is the main overseas IPO destination for Chinese internet companies, almost 50 of which are listed in the US with a total market value of nearly US $500 billion. US shareholders have profited from the development of internet market in China. Not long ago, Alibaba's IPO in the US—the largest IPO ever in the world—raised over US $125 billion. The investments made by US shareholders in Alibaba demonstrate they have great confidence in the Chinese internet, the Chinese market and the future of China. Economic gains accruing to the US and Chinese in equal measure owing to the growth of internet in China somewhat puts the political issues surrounding the governance on the back burner as the respective side attributes these gains to cooperation from both sides, bearing testimony to the correctness of the respective approaches in their eco-system[10].

In contrast to the above scenario, India's position in global information technology ecosystem remains dependent on OECD countries which account for 90 per cent of India's software and service industry exports of more than $100 bn.[11] This factor and also the fact that India is largely dependent on international giants like Google, Yahoo, Facebook, Twitter, etc., for maintaining internet related services without having a support base of its own, it would be stymied when it comes to taking an

[10] Wei, Lu (2015), 'Cyber Sovereignty Must Rule Global Internet,' *The Huffington Post*, May 14.

[11] Bhattacharjee, S. (2014), 'Modi Government's Approach to Internet Governance Position and Regime Must be Strengthened,' *The Economic Times*, September 12.

independent stance even on network security issues, not to speak of seeking a voice in internet governance issues at the international level. The Government of India has placed in position both enabling legislations for protecting against the misuse of cyberspace and a cybersecurity policy. However, the available tools are woefully inadequate and are circumscribed by the complexities of the cyber domain system. Consequently, India has been unable to detect criminals behind cyberattacks against government establishments, even when classified information is transmitted overseas. In India, cyberattacks are rising alarmingly, as is noticed from the available data. There were 13000 cyberattacks in India in 2011, and the number rose to 62000 by mid-2014.[12] Cybersecurity is emerging as a grave concern worldwide and is significantly affecting nations across the globe. Quite often, as per the evidence available, state parties have a tendency to dismiss the issue on the established practice of nations spying on each other; which is a fig leaf defense. There have been instances when many nations in unison have accused the US of snooping, even on its allies. Revelations by former NSA contractor Edward Snowden about the US government's intrusive surveillance of communication is one of the latest stance which invited sharp reactions from across the world, including Germany and Brazil. In sharp contrast India's reaction, if any, was muted and bordering on deafening silence despite the fact that India figured fifth on the list of most spied nations in the world behind Iran, Pakistan, Jordan and Egypt and ahead of Russia, Brazil and China.

Despite such revelation, India does not seem to have at its disposal the wherewithal to make the task of snooping countries like the US at least more costly. Rather, India remains mute amid speculations on whether the US would assist India in advancing cybersecurity and countermeasures against terrorism. Even Snowden leaks have not shaken this belief.[13] The real factor is that unlike China, India lacks the competence to retaliate because of technological dependence for maintaining internet services and economic dependence on account of its linkage to earnings from export of the software products to US and its allies. On account of its handicap of a nonexistent

[12] Ranjan, Amitav (2015), 'Govt Admits Cyber Attacks, But Says Can't Identify Culprits,' *The Indian Express*, February 12.

[13] Chaulia, Sreeram (2013), 'Snowden Fallout: India's Meow, Brazil's Roar,' RT, September 29. Available at: http://rt.com/op-edge/india-brazil-china-nsa-fallout-448/

hardware base, it has missed out on having its own internet infrastructure. It thus remains dependent on internet giants like Google, Yahoo, Facebook, Twitter, etc., opening for them a vast market to operate and earn revenues in tune with internet growth in India. It may be stating a reality if one were to say that the Indian cyberspace is open to foreign internet giants for exploitation to subserve their economic and strategic interests.

In contrast, right from the days of foraying into the field of internet, China has been meticulous in ensuring it maintains control over the lever in its hands and that too firmly. Instead of going the easy way of making quick economic gains from the emerging field of internet, it went whole hog in working towards the development of its own domain system with confidence and success, relying on the existing telecommunications infrastructure and the manufacturing base in electronic products. In this task, the motivating force was the perceived necessity to contain the influence of free flow of information through the internet platform and the concurrent need of China being linked to the external world through the medium of internet as well as through trade. They realized that to reconcile these objectives they would have to devise their own control system in order to build a wall around the internet environment—which was to be free and private-based, and more capitalistic than China's rulers would prefer. It was instantly clear to them that internationally, the internet was subject to a technical infrastructure bearing on American hegemony. In the internet world, China realized that, as required by its political system, it had to move against the grain of the internet regime, promoting sovereignty and intergovernmental institutions in opposition to the new, transnational, and private-sector internet governance institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) and Regional Internet Registry (RIRs). For China, ICANN was an objectionable entity for two reasons: first because of its status as a non-state actor that supplants or competes with states in the exercise of policy making and governance responsibilities; and second, because of its unilateral establishment by the US and its contracts that make

it beholden to the US Department of Commerce.[14] To address its concern with regard to ICANN's technical component of international internet ecosystem, it used a three-pronged strategy. It clearly understood that ICANN is the peak body co-coordinating technical administration and policy development for internet name and number resources, with authority over domain name usage and allocation of IP address. Through centralized administration, ICANN ensures that the internet interoperates globally, without fracturing or becoming Balkanized into numerous sub-global networks. Beijing, which decided to participate in ICANN's Governmental Advisory Committee (GAC) meetings—burying its resentment aroused at the advisory role of the Government of China wherein the final decision rests with a non-government entity under the hegemony of the US to advance its interest in relation to Internationalized Domain Name (IDN) policy and following the ICANN's approval of the addition of IDNs to the Global root—informed the ICANN that China would apply for fast track country-code IDN in the first round. Beijing determined that GAC participation was necessary to exercise influence over the Global Internet Governance. Despite its reservations—as expressed in international fora—Beijing, while engaging with ICANN, made efforts to bridge the gap for greater expansion of internet development, so much so that it offered facilities to ICANN for opening its first "new global engagement office" in 2013. China encouraged its private sector and civil society groups (who remain influenced by the Chinese Government) to associate themselves with ICANN to maintain the overall influence of the Chinese, mainly in IDN-related matters. Most Chinese state actors have pursued interest in Chinese language IDNs within ICANN. Civil society groups like China Organizational Name Administration Centre (CONAC) are increasingly engaged in ICANN's policy and administrative processes. This part of the strategy is dictated by the reality that operating a Chinese internet wholly outside of ICANN's administration will be detrimental to China's economic and technical goals, but at the same time it needs to influence the GAG's technical component for consolidating its expertise and the

[14] Mueller, Milton L., 'China and Global Internet Governance: A Tiger by the Tail.' Available at: http://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CCoQFjAC&url=http%3A%2F%2Faccess.opennet.net%2Fwp-content%2Fuploads%2F2011%2F12%2Faccesscontested-chapter-09.pdf&ei=SkxUVfOGFcO4uASSr4G4Cg&usg=AFQjCNGnzEbIQAkrfOdCbN8RcPXCY80EGg

accompanying gains. Also, for larger acceptability of its approach it requires to demonstrate itself as a responsible stakeholder in the international society.[15]

The second prong of the strategy was to achieve success by creating an alternate DNS root for Chinese-character domain names—China's national alternative to ICANN's global DNS root using the same technical approach pioneered by competing root operator New.net and in the process ensuring that the new domains were globally compatible. Chinese characters would appear as top-level domains inside China. If one of these Chinese character domains was queried from outside China, the uniquely Chinese names would be rendered compatible with the global internet by having name servers add the globally recognized ICANN country code top-level domain, .cn, to the end of that. Three top level domains, namely Zhong guo, Gongsi and Wang lue were created by the Chinese in this fashion by 2003 itself. The feat was not published, and if enquiries were made, the Chinese would downplay terming them "experimental". In 2006, as ICANN began to develop new policies for addition of top level domain, the *People's Daily* openly acknowledged the existence of these domains and advised that the Chinese internet users don't have to surf the web via servers under the management of ICANN. The initiative taken by China led to ICANN implementing a "fast track" approach for the recognition and creation of new "country code top-level domains" (CCTLDs) in Roman scripts and making these CCTLDs operational instantaneously. The fast track approach was worked out assigning two-letter codes using the Roman alphabet to specific geographic territories without having to pay exorbitant and recurring fees. Countries having deeper internet penetration like China, Russia and India were accommodated further to obtain new top-level domains representing their country names in native script in the hope that this type of accommodation would be demonstrative of the accommodative attitude of ICANN regime.[16]

[15] Galloway, T. and B. He (2014), 'China and Technical Global Internet Governance: Beijing's Approach to Multi-stakeholder Governance within ICANN, WSIS and the IGF,' *China*: *An International Journal*, Vol. 12, No. 3, Pp. 72–93.

[16] *Op*. *cit*. 14

Having established their pre-eminence in the technical aspects of the internet and consolidating on a sound base of supporting infrastructure of telecommunication within their country with proven capabilities of regulating the international flow of information**,** China was enabled to firmly announce its approach to internet governance as contained in their White Paper on the subject published in 2010, salient features of which would be brought out in the following paragraphs.

The Chinese government recognizes that the internet is central to a country's socio-economic system, and that therefore the government of individual countries should be empowered to both safeguard and control it in the interest of their national well-being. Once each country's internet system comes under the purview of its government, the global networking of the separate national internets should be regulated through the application of existing and continuously evolving treaties between nation states, similar to all other national and international concerns. Instead of a global, unregulated cyberspace, a regulated and a diverse "internet of nations" would result wherein different countries could promote their own cultures according to their legal needs and wishes, under the aegis of the UN, and not the US controlled ICANN.

Many argue that the internet represents the emergence of a new kind of society, arising out of "networking" effects and its value as part of "information and communication technologies" thus placing emphasis on the offline users who are connected to each other through technology as well as the changes caused offline owing to technological innovation. This approach to the internet has proved fruitful and has provided the basis for very valuable studies of societal developments over the last two decades. However, it has failed to take into account developments in the non-academic world wherein state sectors are shaping the future of internet—radically transforming it from being a global information network into a collection of inter-connected national intranets. A phenomenon of creeping nationalization of the internet appeared on the horizon when states and their courts sought to invoke national jurisdictions—when the free flow of information on the internet was perceived to be prejudicial to the orderly conduct of their societies. In such

endeavours, governments like that of the US and those within EU are also no exceptions—even though on political fora they would not be tired of vouching for the freedom of internet from state control. The effect of states' concern on the internet as a whole is measurable in terms of the degree to which the internet has become localized during the past decade. Giants like Google and Yahoo have offered location-aware makeovers that offer end users different results and a different interface based on their IP address. Thus, splintering of internet has become a reality—an answer to nation states' control over and the responsibility for making the internet accessible to their citizens.

Encompassing the real world situation, it becomes that Chinese approach to the internet and its people and more so to its political system has been pragmatic, which other nation states including the votaries of the free flow of information and freedom of expression and thought have come to follow when encountering real life situations.

Besides, the Chinese in their White Paper emphasize that without doubt internet plays an irreplaceable role in accelerating the development of the national economy, pushing forward scientific and technological advancement, expedites transformation of societies and is an instrument for bringing about international harmony. Thus, the supervision of the internet by national governments is logical and unavoidable in as much as any fact of the "national economy" that plays an "irreplaceable role" has to be safeguarded against the external as well as internal threats and policed as necessary. Therefore, while the Chinese state has, from the outset, abided by the law-based administration of the internet, it has created a healthy and harmonious internet environment, and built an internet that is reliable, useful and conducive to economic and social development. However, it is administered and utilized in a manner that fully takes into account the concerns of national economic prosperity and development, state security and social harmony, state sovereignty and dignity and the basic interests of the people. Inference from the statements in the Chinese White Paper is that in their view the internet and related technologies are not merely instruments of information and communication, but is something more than

that. Also, its importance to the national economy turns "cyberspace" into a legal territory under the jurisdiction of the nation states. Viewed thus, not only are end users of the internet, or the parts of the internet accessible to them, but all internet data on servers located inside the Chinese territory are duty-bound to adhere to the laws of the land. Thus, the internet sovereignty of the State must be respected.

The White Paper being recalled here recognizes that national situations and cultural traditions differ among countries and so concerns about internet security also differ. Concerns about internet security of different countries must be respected. Though connected, the internet systems across various countries belong to different sovereignties. Viewed from such an angle, it follows that the states' will work together with a view to strengthening international exchanges and co-operation for establishing a regime based on international evenness.

A corollary to the above approach and scenario would be that ICANN in its present form would have to give way to the internationally governed arrangement as worked out based on international treaties under the legitimate supra-national body—the United Nations (UN).

It appears that the Chinese had long foreseen the realities of the technologies enveloping the internet world that the states all over the world would be called upon to provide security to e-citizens, who were mistaking cyberspace to be the last free space on earth initially. The desire of the citizens to be protected online and the demands by companies for the enforcement of the laws in cyberspace combined with the goal of nation states to "control" has made the splintering of internet unavoidable. More and more stakeholders have come to accept that the absence of state in the cyberspace or that the protection of internet users from state surveillance is possible only at the cost of the societies, which is dangerous and in many cases irreversible. It would appear that more and more democratic countries including the US and the countries of the European Union, Australia, South American countries and also India are harbouring plans similar to the "authoritarian regime" like that of China—aggressively seeking blocking and censoring the internet. In fact, the US, which is steadfast in propounding the case of "freedom of internet" at any

given forum, brought a plan to generate a "blacklist" to censor citizens' access to certain websites, proposing grant of powers to police and security organisations to add websites to the blacklist that would have to be enforced by all US based ISPs—a proposal as "draconian" as the Chinese system. The US has further gone onto announce that a "cyberattack" against it will be viewed in the same light as any other "act of war" and will be responded to accordingly. Also, if need be, offline it will deploy forces in retaliation—a move which is remarkably in consonance with the Chinese position of cyberspace being as much an offline territory. It appears that nation states, whether they acknowledge or not, are emulating the Chinese way of approach to the internet.[17]

Observers on the subject of international governance on internet have noted that the Chinese vision of state-controlled internet is increasingly attractive to many Western nations wrestling with inter-related threats of cybercrime, industrial espionage, and cyberwarfare. It has been suggested that the United States must actively combat these threats while it works to protect its national interest in the preservation and extension of the internet as a platform for increased efficiency and economic exchange. Protecting the internet on the model that the US desires will require extensive engagement within the internet governance forum to help shape the future of the network in a way that will address security concerns without resulting in a cure worse than the disease. The US should lead by example by taking steps to clean up its national network, work to stop its systems from being used in international cyberattacks making clear that primary goal of its cyberspace is to defend the United States and preserve international connectivity.[18]

It is common knowledge that root-zone—a master list of all registered numbered websites on the IPS—though managed by ICANN is ultimately controlled by the US government.[19] It is unlikely that the US will share this privilege with the others

[17] *Op. cit*. 5

[18] Knake, Robert K. (2010), 'Internet Governance in an Age of Cyber Insecurity,' Council Special Report No. 56, Council on Foreign Relations Press, September.

[19] Drissel, D. (2006), 'Contesting Internet Governance: Global Dissent and Disparaties in the Management of Cyberspace Resources,' *WIT Transactions on Information and Communication Technologies*, Vol. 36.

despite the announcement on March 14, 2014 about its intention to transition stewardship role of their National Telecommunication and Information Administration (NTIA) over key domain functions by September 30, 2015.

NTIA has already stated that it will not accept any transition proposal that would replace its role with a government-led or inter-governmental organisation solution. If NTIA is not satisfied with the transition plan within its parameters, it has the flexibility to extend the existing contract to enable the stakeholders to develop the best plan possible.[20] The fact remains that the US government had categorically stated in 2005 that it would retain its historic role authorizing changes or modification to the authoritative root zone file[24]. Despite the reality that more and more governments are seeking to regulate the internet within their territories and that the US, in recognition of concerns emerging globally that it should shed its hegemony and end its overseeing role in relation to ICANN, the US could not be persuaded to accord the decision-making power to intergovernmental organisations in the DNS hierarchy and related architecture. The Chinese, as in the past, shall continue to engage with the ICANN as it evolves post September 2015 but will maintain and redesign their own infrastructure and internet architecture to address concerns brought on by cyberattacks as well as augment their own espionage activities. Ministry of Defense, Government of India, has acknowledged that the Chinese hackers have also broken into its military networks. Chinese publication, The Science Military Strategy, in its March 2015 issue has admitted that the People's Liberation Army (PLA) has specialized in cyberwarfare units and it is a top military priority to improve upon their capability to wage war in the virtual area. Towards this end, China regularly hacks into the sensitive computer network of countries like India, the US, the UK and Germany. China has at best a couple of hacker brigades, apart from over 30,000 computer professionals in its militia. It also has civilian teams empowered to undertake similar intelligence and computer networks attacks.[21] In light of the US and China both arming themselves with cyber armament, they are

[20] Strickling, L.E. (2015), 'Stakeholders continue historic work on Internet DNS Transition at ICANN Singapore Meeting,' National Telecommunications and Information Administration (NTIA), February 19.

[21] *Op. cit*. 19

involved in a cyber cold war which is a sure recipe for any untoward incident with the potential of causing unimaginable consequences. Already the malicious activities carried out by criminals and spies threaten economic growth and the efficiency that the existence of a single, global interoperable network has brought. If these threats[22] are not addressed constructively through broader engagements globally with US leading the way, some countries may step in and may carve out a solution that may deprive the internet of the very characteristics that US is trying to preserve because it had made the internet "valuable" in the first place. The US and other global players work towards re-architecting the internet's underlying protocols to make them more secure with a view to preserving and extending the economic value derived from internet.[23]

In the preceding paragraphs of this note, mention has been made of the laid-back approach of India to governance issues surrounding the internet while basking in the glory of increased incomes from the export of software; and becoming a partner in value chains of foreign multinational companies. There have developed consequent inefficiencies; and, minimum security features have not been built to preserve the sovereign integrity and public order of a society—which is complex, diverse and fiercely democratic with an overbearing judiciary. Government lacks the wherewithals to contain threats from cybercriminals and also does not have an independent mechanism to determine the identity of such elements and force them to face the law despite placing in position legislative instruments like IT Act, policy statements on cybersecurity.

India called for democratization of global internet governance and in October 2011 proposed the setting up of a Committee for Internet Related Policies (CIRP), accountable to the United Nations General Assembly (UNGA), to deal with International public policies relating to the internet. Instead of discussing the pros and cons of different elements of the proposal, there was an orchestrated cacophony in the media designed to drown any reasoned debate. Calls were made to

[22] Pandit, Rajat (2015), 'Defence Ministry Sounds Fresh Red Alert on Web Spying,' *The Times of India*, March 23.
[23] *Op. cit*. 18

force India to withdraw its proposal—which was characterized as catastrophic, threatening a UN takeover of the internet, and doomed to bring down Indian IT firms. IT majors and industry associations rose in defense of the current model of internet governance bearing US hegemony; after all many of them depend on global internet majors for their business, and have always spoken and acted on their behalf. At the political level, however, India's policy on the subject of global governance of internet had been consistent over the decade, at least until 2011. The initial calls or democratization of global internet governance were made at the World Summit on the Information Society (WSIS) held in Geneva in December 2003 and in Tunis in November 2005. Nitin Desai from India served as the Secretary-General's Special Adviser for WSIS. India pursued the implementation of both the Working Group on Internet Governance (WGIG) and the Tunis Agenda, which mandate that the management of the internet be made multilateral, transparent and democratic. WGIG had identified significant governance gaps with regard to the internet: these include unilateral control of the root zone files and systems and lack of accountability of root zone operators; concerns over allocation policies for IP addresses and domain names; confusion about application of IP rights in cyberspace; substantial higher connectivity costs in developing countries located far away from internet backbones; lack of multilateral mechanisms to ensure network stability and security; lack of effective mechanism to prevent and prosecute internet crimes and spam; barriers to participation of multiple stakeholders; restriction on freedom of expression; inconsistent application of privacy and data protection rights; absence of global standards and global rights; insufficient progress towards multilingualism; and, insufficient capacity building in developing countries. The Indian proposal in 2011 had only suggested that the above-mentioned issues as well as the policy issues that have evolved since the establishment of WSIS be considered by CIRP. It had not proposed that the UN take over the internet or that prevalent technical arrangement be overturned, as argued by those who derailed the proposal.[24]

While India battled at the UN and other forums, it remained passive in building up its technical competence like China, despite clear signals that the US was not going to

[24] Puri, Hardeep S. (2013), 'Wide Asleep on the Net,' *The Indian Express*, June 27.

share its privileged position in strategic terms regardless of its allies joining its detractors. Rather, it got persuaded to contain its voice in championing the cause of Indian IT companies that were heavily dependent on global internet majors. Such an apprehension is somewhat misplaced. The current model of growth of IT companies has already reached its maxima. For greater good of the sector, it would be beneficial to spawn the next generation of IT companies, which can move up the value chain by creating their own branded products and deliver branded services, thus leading to global innovation in IT. Such a change can only be brought about by modifying the eco-system, architecture and infrastructure, both nationally and internationally, where such ventures can grow. The recent setback to India at the recently concluded UN's International Telecommunications Union (ITV), hosting its plenipotentiary conference in 2014 at South Korea when it was to withdraw its Resolution on ITU's Role in realizing Secure Information Society, would be a testimony to the fact that India and like-minded countries have a long ground to cover. India was motivated to move the resolution as in its perception the current network architecture had security weaknesses, making it difficult to trace the communication trail which raise national security concerns. It wished that ITU should develop and recommend a traffic route plan, facilitating the identification of location/countries. The resolution in no way was towards raising issues about the concentration of central internet resources and also India had no intention to engage ITU in discussions around Human Rights issues.[25] Any effort which may remotely make nation states independent from their historical dependency on multi-stakeholder model of governance will not easily lead to success. India, as in the past, may have to rekindle its spirit of meeting the denials to carve its rightful path to ensure integrity and security of the internet on its cyberspace with courage, conviction and self-belief. As UN prepares to celebrate the 10th anniversary of WSIS in2015, India should reassess its domestic strategy and also join hands with leading democratic and other like-minded countries in the UN Security Council in true spirit of Tunis Agenda to make internet crime-resistant as well as truly multilateral, transparent and democratic.

[25] Hariharan, Geetha (2014), 'Good Intentions, Recalcitrant Text – I: Why India's Proposal at the ITU is Troubling for Internet Freedoms,' The Centre for Internet & Society.