isdg **Policy Brief**

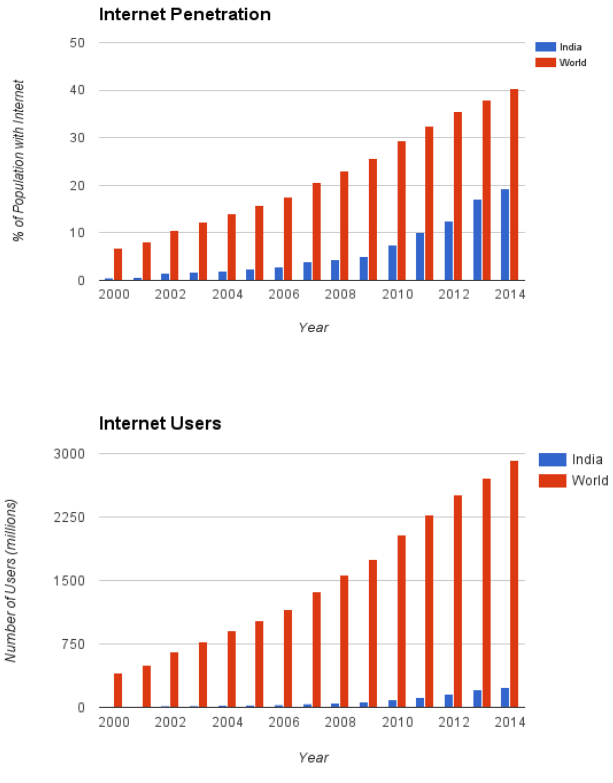
Cyberspace Governance and Security

Introduction

Cyberspace governance may be defined as the process of applying technologies, network systems, rules, policies, laws, procedures and institutional resources to manage regulate and facilitate the processes of communication and information in cyberspace through internet-enabled devices such as computers, tablets and smart phones. Cyberspace governance has immense implications in the way power is used and managed by big businesses, governments and powerful countries. A recent study defines "cyber governance as the network of formal and informal institutions, mechanisms and processes that guide or restrict activities in cyberspace on a global or regional scale, thereby organising and articulating collective interests in cyberspace. This includes concrete cooperative problem-solving solutions negotiated by international bodies, governments, and on-state actors aiming to improve the management of cyber risks" [1]. Though the cyberspace governance is a relatively a new term, it is closely linked to the concept of internet governance. Internet governance is defined as the development and application of shared norms, principles, rules and decision making procedures that affect the evolution and use of internet .[2]

Cyberspace governance is necessarily a political process of exercising power through multiple means, modes and methods. There are essentially two aspects of cyberspace governance. Firstly, how power as applied through cyberspace affect various arenas - governance in the state, market and civil society. Secondly, how technology, information, laws, and policies affect the management of communication and information in the multiple channels and arena of the cyberspace. Both these aspects have immense implications for almost all dimensions of of governance. The issues of connectivity, digitalisation, networking and consolidation and use of data and information (big data) affect the arena of human interaction as well as that of economy, society, culture and politics. Hence, cyberspace governance is not only about technology or laws, but also linked to new ways of consolidating and managing power that affect everyday life of people in multiple ways.

Information and communication technologies (ICTs) have become an integral part of everyday life of vast majority of people across the world, though half of the people of the world live beyond the virtual world of internet. It is estimated that half of the world's population will be online by 2017. Mobile smart phones have percolated to every nook and corner of the world and according to the Worldwide Quarterly Mobile Phone Tracker, sales of smartphones exceeded 300 million units in shipments for the first time in the second quarter of 2014. As per the estimates of the International Telecommunication Union (ITU) the number of networked devices will reach 25 billion by 2020. Cyberspace has become the dominant platform for communication and collaboration for individuals, communities, businesses and the government. These technologies are a key factor fuelling social networking, economic development, innovation and growth. The internet has in effect transformed into a global neural system. "Whoever has control over this neural network begins to wield unprecedented power — economic, political, social and cultural".[3]

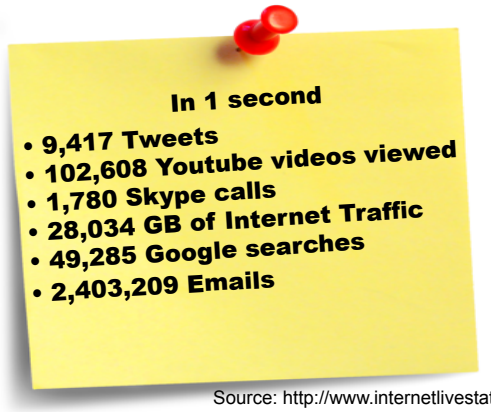


Source: http://www.internetlivestats.com/

1. Risk Nexus: Global Cyber-governance.
2. Report of the Centre for global Economy and Politics and Zurich, 2015
3. Singh, Parminder Jeet (2015, June 6). Who rules cyberspace? The Hindu

Cyberspace governance is also an emerging area for research and analysis. There are debates about the appropriate role of governments, corporations and institutions in operationalizing technology, laws and policies to exert power in economy and society. Despite the exponential growth of internet, there are still, a lack of reliable and comprehensive information, research and analysis in this area. Various aspects of cyberspace governance include issues related to cyber-security, rights to communication, expression and privacy; the increasing concern about surveillance by the government agencies; growing incidence of cybercrimes including harassment, frauds, theft of data, destruction of data and use information and communication that create violence or harm the greater common good; and also how e-commerce, new media and e-governance affect different aspects of economy, government and society.

There are emerging areas such as internet of things (IOT) and internet of everything (IOet). A study by the Cisco Systems indicate that by 2022, USD 14.4 trillion in value is at stake in connecting up what is now connected through the internet of everything. In the next few years, big data, additive manufacturing, unmanned aerial vehicles and autonomous cars etc are going to change the business practice, social life and economy in a significant manner. With the exponential growth of internet, social network and mobile technology, the instances of cyber-crimes have also increased. It is estimated that in the U.S. alone, the annual costs of cybercrime are estimated at USD 100 billion.



Source: http://www.internetlivestats.com/

Cyberspace governance: Issues with the current global framework

There are multiples issues that are being debated in relation to global cyber governance. On the one hand, there is an increasing concern over surveillance by different government agencies , particularly those of the US government. The issues of censorship of cyber-space and social network are discussed in relation to the right to communicate and express as well as the ability to access information. In many countries, there are restrictions placed on the use of social networks and information available on the internet. Another issue with implications for cyberspace governance is the increasing trend of monopolisation of data and information by big business enterprises and companies (such as Monsanto and big pharma companies) .However, the most discussed issue is the increasing instances of cyber risks and security.

Cyber surveillance has become an international issue when German Chancellor Angela Merkel and Brazilian President Dilma Rousseff protested against US surveillance on many leaders and governments. The almost unilateral dominance of the USA in terms of technology and ability to influence the international decisions and governance have attracted alternative discourse on cyber governance seeking for more democratisation of global cyber-governance. Responding to global concern on cyber surveillance, the international technical community involved in the internet governance - Internet Corporation for Assigned Names and Numbers (ICANN); five Regional Internet Registries (RIRs)ie. African, American, Asia-Pacific, European and Latin American; two standard setting organisations -World Wide Web Consortium (W3C) & Internet Engineering Task Force(IETF); the Internet Architecture Board (IAB); and Internet Society (ISOC)- issued the Montevideo Statement on 7th October, 2013. The statement expressed "strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance." The statement called for "accelerating the globalization of ICANN and IANA functions...towards an environment in which all stakeholders, including all governments, participate on an equal footing"[4]. The increasing concern over the cyber surveillance also led to the issue of human rights to express, communicate and to the right to privacy. Hence, there is a call of multi-stakeholder approach and multilateral forums to ensure to rights of people to communicate as well their right to privacy.

The Working Group on Internet Governance report has four categories for public policy issues that are relevant to Internet governance[5] :

(a) Issues relating to infrastructure and the management of critical Internet resources, including administration of the domain name system and Internet protocol addresses (IP addresses), administration of the root server system, technical standards, peering and interconnection, telecommunications infrastructure, including innovative and convergent technologies, as well as multilingualization

(b) Issues relating to the use of the Internet, including spam, phishing, network security and cybercrime.

4. Montevideo Statement on the Future of Internet Cooperation https://www.icann.org/en/news/announcements/announcement-07oct13-en.htm.
5. "Report of the Working Group on Internet Governance (WGIG)", June 2005)

(c) Issues those are relevant to the Internet but have an impact much wider than the Internet and for which existing organizations are responsible, such as intellectual property rights (IPRs)

(d) Issues relating to the developmental aspects of Internet governance, especially capacity-building in developing countries.

While many of these policies will have to be negotiated among different stakeholders -, governments, business, and civil society - in multi-lateral forums, there is a need for a cohesive international framework on cyberspace governance internet governance. The internet governance forum(IGF) is a global initiative that facilitates such a multi-stakeholder approach to address the issues of cyber-space governance, risks and security.

According to a recent report titled "Risk Nexus: Global cyber governance" the issues related to cyber governance may be located in a broad spectrum. On one end of the spectrum is technical governance which helps network systems function properly by ensuring that all the infrastructure and devices constituting the internet are interoperable, that is, they can talk to each other. At this end of the spectrum, global governance is largely effective – following a multi-stakeholder model based on a loose, bottom-up consensus. These actors are mainly interested in maintaining cyberspace as an open, cohesive place to secure connectivity, manage infrastructure in the right way and enforce cyber security.On the other of the spectrum is cyber warfare and includes issues relating to state-sponsored cyber-attack, espionage between states, and cyber-attacks on critical infrastructure for political purposes. Here, a global governance framework is absent, mutual understanding progressively more difficult, and the role of international organizations, far from being effective. A bilateral method prevails between governments, and no change is expected in the medium term due to the sensitive political nature of homeland security, content control, or privacy protection involving individual governments. Here, in this end of the spectrum, the U.S. has asserted its hegemony via its control of

1) The global telecommunications network comprising the fibre optic cables, submarine cables and the global satellite and microwave communications networks,

2)The US based giant Internet companies such as Google, Microsoft, Yahoo and Facebook whose levels of monopolization in the Internet space facilitate the gathering of global citizens' data on an unprecedented scale

3) The US based network equipment companies whose status as designers and manufacturers of much of the world's network equipment (switches and routers etc) facilitates access to large swathes of the internet through the proprietary "back doors" of their network equipment [9].

Between these two extremes is a 'gray zone'. Issues addressed in this space include intellectual property rights, cyber-attacks by non-state actors or individuals, criminal activity and data protection. The international institutions within this group are thus unsurprisingly very diverse in nature and purpose. Neither the bilateral approach of cyber warfare, nor a multi-stakeholder model dominates. It is in this gray zone, with its complex set of governance models and organizational cultures, that the international community can most significantly improve cyber governance with the aim of mitigating cyber threats

Cyber governance: India-specific issues

Freedom of Expression-Upheld by the Supreme Court

Civic activists and human rights activists challenged 66 A of the Information Technology Act 2000 on the ground that it infringed on the rights guaranteed by the Artile 19 of the Indian constitution. In 2012, two 21-year-old girls, Shaheen Dhada and Rinu Shrinivasan, in Palghar town in Thane district of Maharashtra, were arrested under Section 66A of the I.T. Act 2000 for a Facebook post criticising the shutdown in Mumbai during Shiv Sena chief Bal Thackeray's funeral. Although they were granted bail, and the charges against them dropped, the arrests created a nation-wide uproar against the use of Section 66A to quell social media dissent. Section 66A was inserted in the I.T. Act, 2000, through an amendment, after the second United Progressive Alliance government came to power in 2009. The provision was titled "Punishment for sending offensive messages through communication service, etc." On March 24, 2015 a Supreme Court Bench declared Section 66A of the Information Technology (I.T.) Act unconstitutional and upheld the freedom of expression in cyber space. The Supreme Court had found that Section 66A infringed on the fundamental right to free speech and expression and was not saved by any of the eight grounds covered in Article 19(2) of the Constitution [2].

Net Neutrality - Fate to be decided by Cabinet

Net neutrality indicates the equal access that internet service providers give their customers to all lawful websites and services on the internet, without giving priority to any website over another.

In March 27 2015, the Telecom Regulatory Authority of India (TRAI) released a formal consultation paper on Regulatory Framework for Over-the-top (OTT) services seeking comments from the public. Over The Top (OTT) services compete with Telco voice and sms services. Applications like WhatsApp, Skype, Viber which allow text/voice messaging and calls over the internet comprise OTT services. Telecom companies claim that these apps have significantly reduced their revenue in terms of voice and SMS services [3]. Hence, the telecom companies demand that such apps be licensed, and that consumers (or the apps themselves) shell out money over and above the data charges for such usage. The consultation paper was widely recognized as being biased towards the interests of Telco operators and against the principle of net neutrality. The public response was overwhelming. On April 23, 2015 the TRAI received over a million emails demanding net neutrality [4].

On June 1 2015, the Department of Telecom (DoT) panel on net neutrality submitted its report to the Communications & IT Minister Ravi Shankar Prasad. The minister, who had made a commitment in the Rajya Sabha [5] that the government would not compromise on net neutrality, said that the cabinet would make a final decision based on the reports of both the DoT and TRAI.

Cyber Surveillance- No legal protection against surveillance

A report released in September 2014 by the Software Freedom Law Centre (SFLC) titled "India's Surveillance State" revealed that the Indian state is violating the privacy of its citizens through use of internet monitoring systems [6].Legislative enactments such as the Indian Telegraph Act and the Information Technology Act allow Indian law enforcement agencies to closely monitor phone calls, texts, e-mails and general Internet activity of citizens on a number of broadly worded grounds. This opaque surveillance regime is run solely by the Executive arm of the Government without any provision for independent oversight [7].

Furthermore, the NDA government has pledged to expedite the Orwellian Central Monitoring System (CMS), an ambitious programme aimed at giving the state the ability to listen and record phone calls and read private emails as well as text and multimedia messages [8]. The CMS lacks checks against abuse - It allows senior bureaucrats from several government agencies, including the CBI and IB too much discretion in approving requests for surveillance. No court warrant is required to get permission to monitor a citizen. Moreover, there are also no laws to safeguard the data so collected.

India urgently needs a law to protect its citizens' privacy from arbitrary surveillance.

References

1. Bijoe Emmanuel v. State of Kerala, (1986) 3 SCC 615.
2. http://www.frontline.in/the-nation/in-defence-of-free-speech/article7048980.ece?utm_source=RSS_Feed&utm_medium=RSS&utm_campaign=RSS_Syndication
3. https://www.saddahaq.com/human-interest/netneutrality/trai-consultation-on-net-neutrality-and-ott-services-what-do-these-terms-mean
4. http://timesofindia.indiatimes.com/tech/tech-news/Trai-receives-1-million-emails-on-net-neutrality/articleshow/47024829.cms
5. http://indianexpress.com/article/technology/social/govt-supports-non-discriminatory-access-to-internet-telecom-minister/
6. http://www.thehindu.com/news/national/india-violating-privacy-of-internet-users-report/article6381469.ece?utm_source=RSS_Feed&utm_medium=RSS&utm_campaign=RSS_Syndication
7. http://sflc.in/indias-surveillance-state-our-report-on-communications-surveillance-in-india/
8. http://indianexpress.com/article/opinion/editorials/the-snooping-state/
9. Prabir Purkayastha and Rishab Bailey, 'Evolving a New Internet Governance Paradigm', Economic and Political Weekly, Vol. XLIX, No. 2, 11 January 2014..

Institute for Sustainable Development & Governance
TC No 5/2555 (2), Palm Dale, Golf Links, Kowdiar P.O 695003, Thiruvananthapuram.
Phone: 0471-2433358
Email: *isdg@ccds.in*
Website: *www.isdg.in*
Facebook: *www.facebook.com/isdgindia*
Prepared by: John Samuel, Zuhail Sainudeen,