CYBER-SOVEREIGNTY IN INDIAN CONTEXT

Mr. Kshirod Kumar Moharana*

Abstract

Cyber-sovereignty, otherwise called internet freedom is a phrase describes the government to exercise control over the internet within their own boundaries including economic, political, cultural and technological activities. Cyber-attacks, cyber espionage, Surveillance are realistic issues of countries for adopting cyber-sovereignty without any hindrance. Countries are also discussing about to produce new international legal instruments to deal with the security situation in cyberspace for avoiding cyber-terror and cross boundary cyber-crimes. Sovereignty on the internet has many manifestations such as 'data sovereignty' that has gained importance in the Post-Snowden Era. The evolving uses of the internet only adds to the complexity created by these competing notions of sovereignty and its application to the online spaces resulting in differing interpretations of cyber-sovereignty. Countries such as Russia, China, France and Saudi Arabia are stepping towards cyber-sovereignty movement. These countries are also pointing their justification for their activities and evidence of U.S hypocrisy on internet freedom issues. The world's highest Internet connectivity country China is using Chinese versions sites like as *Bidu* and *Sina Weibo* instead of *Goggle, Face Book* and *Twitter* for the sake of cyber-sovereignty. Now India is going to be a part of the cyber-sovereign country like China, U.S and Russia. India is going to boycott foreign technology by adopting the cyber-sovereign and indigenous technology with great extent. Countries may be big or small ought to be equal and they should respect each other's in cyber-sovereignty, Internet governance, major concerns and cultural differences. They should strengthen communication, increase understanding and broaden consensus. No country can achieve absolute security without the overall security of international cyberspace. Peace between major countries may not result in a peaceful cyberspace, but distrust will definitely bring chaos. A responsible major country should never restrain others for its own development, or infringe on other countries' security to

* Lecture in Law, Biraja Law College, Jajpur, Odisha.

protect its own security. No country can achieve absolute security without the overall security of international cyberspace. India is going to be diversity on cyber-sovereignty after the BRICS summit. This paper basically analyzed the importance of cyber-sovereignty and its merit and demerit in Indian context.

Key words: cyber-sovereignty, cyberspace, cyber-crime, communication, indigenous

Introduction

Cyber-sovereignty, otherwise called internet freedom is a phrase describes the government to exercise control over the internet within their own boundaries including economic, political, cultural and technological activities. Cyber-attacks, cyber espionage, Surveillance are realistic issues of countries for adopting cyber-sovereignty without any hindrance. Countries are also discussing about to produce new international legal instruments to deal with the security situation in cyberspace for avoiding cyber-terror and cross boundary cyber-crimes. Sovereignty on the internet has many manifestations such as 'data sovereignty' that has gained importance in the Post-Snowden Era. The evolving uses of the internet only adds to the complexity created by these competing notions of sovereignty and its application to the online spaces resulting in differing interpretations of cyber-sovereignty. Countries such as Russia, China, France and Saudi Arabia are stepping towards cyber-sovereignty movement. These countries are also pointing their justification for their activities and evidence of U.S hypocrisy on internet freedom issues.

Now China-U.S. relations in the field of the Internet is an important component of the new model of major power relationship is positive and making progress in a steady manner in spite of hurdles. The main features are deep fusion and high stakes with disagreements and frictions. The world's highest Internet connectivity country China is using Chinese versions sites like as *Bidu* and *Sina Weibo* instead of *Goggle*, *Face Book* and *Twitter* for the sake of cyber sovereignty. Now India is going to be a part of the cyber-sovereign country like China, U.S and Russia. India is going to boycott foreign technology by adopting the cyber-sovereign and indigenous technology with great extent. Countries may be big or small ought to be equal and they should respect each other's in cyber-sovereignty, Internet governance, major concerns and cultural differences. They should strengthen communication, increase understanding and broaden consensus. No country can achieve absolute security without the overall

security of international cyberspace. Peace between major countries may not result in a peaceful cyberspace, but distrust will definitely bring chaos. A responsible major country should never restrain others for its own development, or infringe on other countries' security to protect its own security. No country can achieve absolute security without the overall security of international cyberspace. As long as we take a long-term view and prepare for a new era of shared governance, we can translate the diversity of development into the driving force of world Internet development. India is going to be diversity on cyber-sovereignty after the BRICS summit.

A communication with legal consequence may never result in the production in of some physical objective bearing the information communicated. Conversation may take place between computes; acting on their own initiative and with no involvement from human actors. So internet is fundamentally no more than a means of communication and that the new issue of internet law arises from the differences between internet and physical world. Cyber-sovereignty is one of the advent steps towards preventing cyber-crime thought the country.

Due to the anonymity and invisibility of cyber-criminal and it's potential to affect in several countries at the same time, which are different from the place of operation of the cyber-criminal. Hacking, Virus, Trojans And Worms, Cyber Pornography, Cyber Stalking, Cyber Terrorism, Cyber Crime Related To Finance, Cyber Crime With Mobile And Wireless Technology, Phishing, Denial of Service Attack, Distributed Denial of Service Attack, E-Mail Bombing, E-Mail Spoofing, Data Diddling, Salami Attacks, Salami Techniques, Logic Bombs, Internet Time Thefts, Web Jacking etc. are more vulnerable cyber-crimes through E-contract which creates very much difficulty in all over the world.

In Indian law, cyber-crime has to be voluntary and willful, an act or omission that adversely affects a person or property. The IT Act-2000[1] provides the backbone for E- Commerce and India's approach has been to looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. There is the need to take in to consideration the security aspects. In the present global situation where cyber control mechanism are important we need to cyber law. Cyber-crimes are a new class of crimes to India rapidly expanding due to

1 IT ACT-2000 came into force on I7th October 2000.

extensive use of internet. Getting the right lead and making the right interpretation are very important in solving a cyber-crime.[2]

Cyber-sovereignty

The term 'cyber' is derived from cyberneties which is used to describe entire range of things made available through the use of a computer. Internet governance is a very broad term and has a wide ambit that is rather pervasive. It is indeed a reflection of diverse perceptions and priorities that countries and stakeholders have with regard to internet governance.[3] The various models of governance are a result of the divergent views of internet governance. Lack of internet governance creates cyber-crime where cyber-criminals are perpetrate fraud and other crimes against companies and consumers and they steals a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programmers.[4]

Cyber-sovereignty is a modern phrase which describes the Governmental control over Internet restricting websites whose content may harm the sovereignty of the nation. With the advent of technological advancement, liberalization & globalization, this has become a bone of contention between public and authorities. Cyber-sovereignty in actual terms become cyber-bullying, and many unnecessary websites are blocked due to improper monitoring of content. If the filter is not done property, it results in violation of Art. 19(2) and has a chilling effect on right to speech, dissent and right to Know. Growth in technology has led to proxy sites & various other means which give an easy access to the blocked sites. These proxy sites instead are a much larger threat to national security. More circulation of black money as piracy business gains flow through underground market. Various measures can be adopted instead of taking the extreme route like placing a statutory body to monitor and track content, forming a committee of experts from different nations to evolve a common consensus, treaties among nations protecting each other's sovereignty.

The term 'cyber-sovereignty' has been phrased out to draw attention on internet governance within the boundary of a nation

---

2 Talwant Sing, *Cyber Law and Information Technologies*.

3 *Available at* https://ccgnludelhi.wordpress.com/tag/cyber-sovereignty, retrieved on 6-11-2017

4 Andrew Grand, *Adamson Cyber-Crime*, Mason Crest Publishers, 2003 .

to protect its internal interest.[5] The government exercises control over Internet within their own borders, including political, economic, cultural and technological activities. With the advent of Internet, the liberty given to it has caused to connect one continent form the other. But at the peak time it has pose may question in front of the policy maker. We have number of such examples of cyber attacked which has been done allegedly, but none of the suspected attackers has taken responsibility for it. *Stuxnet* which suspected combined attack by USA & Israel on Iran's nuclear facility and economic espionage by hacking the private networks of companies etc. are the examples.

Cyber-sovereignty has come as a reaction to the cyber threat. There are a team of hackers which are operating worldwide just to accomplish the targeted job. China allegedly has such team which has attacked the UN, USA and India numbers of times but they are refused to accept this allegation. So cyber-sovereignty is the need of the hour to ensure internal security and strategic interest of the country as it also giving rise to the terrorist activities.[6] Logically, the concept of cyber-sovereignty holds little water and cannot be placed on the same platform as national sovereignty. It should not give governments' unchallenged powers to suppress dissent and ban websites in the name of sovereignty. Moreover, it should not act as hindrance to information inflow and outflow that is increasingly contributing to awareness among citizens.[7]

However, certain reforms can be brought out in cyberspace governance which is today largely controlled by the US government based on *Talinn Manual*. A unified policy framework that is democratic in nature needs to be worked out so that no country feels left out in cyberspace governance and punitive measures are taken against cyberspace violation and malware attacks.

Cyber-sovereignty involves a sovereign cyber network of a nation or any region where the authority exercises censorship and controls the cyber data circulating within as well as leaving the territories of the country. The advantages of cyber-sovereignty are:

---

5 *Available at* http://www.insightsonindia.com/2015/12/17/5-understand-cybersovereignty-critically-examine-good-cybersovereignty-age-globalization-internet/, retrieved on 06-11-2017.

6 *Ibid.*

7 *Ibid.*

- Ensuring sovereignty of the internet, it tries to protect the cyber data from foreign attack or hacks;
- Governing internet in accordance with nation's requirement by the legislative authorities in order to maintain a basic 'order';
- Regulating the domestic data reduces problems of internet extremism and cyber-terrorism; and
- It prevents foreign MNCs to capture the domestic market, spurring innovation in technology and growth of domestic startups.

Disadvantages of cyber-sovereignty are:

- Excessive control of cyber data leads to curtailment of freedom of citizens to express disregard for the authorities;
- Foreign companies spur competition and fuel product development led customer satisfaction. Banning them would mean subordinate facilities to the customers; and
- Domestic startups need collaboration with the established companies. In an atmosphere of censorship, they are compelled to use costlier technologies.

Cyber-sovereignty allows the state to regulate the internet within the domestic boundary of the state. It allows the state to regulate data and control any provocative content that can disturb peace in the state. It controls efforts of money laundering or financial terrorism. It also prevents defacing of government websites which could otherwise lead to denial of service to citizens. Preventing attacks on critical infrastructure like defense, energy and communications systems required for smooth governance.

However, this idea has drawn criticism because of the seamless connectivity cannot be ensured in case of excessive restrictions on internet. Citizens' data are constantly under surveillance thus intruding into their private space. Internet is shared space and excessive regulations can lead to its fragmentation Thus, it can be said that a better approach would be to beef up security through technological measures rather than putting excessive restrictions that hamper individuals' freedoms.

Cyber-sovereignty is a modern phrase which describes the Governmental control over Internet restricting websites whose

content may harm the sovereignty of the nation. With the advent of technological advancement, liberalization & globalization, this has become a bone of contention between public & authorities. Cyber-sovereignty can count the radicalization of youth through social media as all around the globe; terrorism through widely available diverse content is becoming a menace. It can Control cyber terrorism and keeping secure the important and un-disclosable data.

Cyber-sovereignty is the institutional mechanism of internet governance in which a nation starts to monitor the internet traffic and weeds out all the criticism against the party incumbent in Govt. It involves the suppression of even the righteous facts, justified criticism of government policies which are essence of democracy. China is classic example of this which banned Google. In the age of globalization cyber-sovereignty is not good because, It is against freedom of speech, the Punishments evoke self-regulation to freedom of expression, the non-participating and passive public opinion or response to Government efforts and against the principles of democracy.[8]

In the era of globalization and E-commerce along with every facility or resource availability digitally this can hamper the overall development of society and its objective values. Though it is good to ban the websites which are hate mongering and conspiring against state but that must pass the test of country's laws and banning every criticism in globalized interconnected world may lead to isolation of society. Supreme Court annulment of 66A is a welcome step to end such.

Sovereignty and cyber-crime

The term 'cyber-crime' is misnomer; this term has nowhere been defined in any statue/act passed or enacted by the Indian parliament.[9] The concept of cyber-crime is not radically different from the concept of conventional crime which causes breach of rules of law and counter balanced by the sanction of the state. Cyber-crime is an evil having its origin in the growing dependence on computers in modern life, in a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computer. Cyber-crime has assumed rather sinister implications.

---

8 *Available at* http://www.insightsonindia.com/2015/12/17/5-understand-cybersovereignty-critically-examine-good-cybersovereignty-age-globalization-internet/, retrieved on 06-11-2017.

9 *The Chief Legislation Regarding Cyber-Crime in India*, IT Act-2000.

In the field of Internet governance cyber-sovereignty is used to describe government's control over the Internet within their boundaries, including political, economic, cultural and technological activities. In the age of globalization where the Internet is intertwined in all aspects of society cyber-sovereignty is critical to national sovereignty because:

- The threat of cyber-attacks poses challenge to the physical security of the nation. E.g., cyber-assault on Estonia by Pro-Russian hackers caused temporary shutdown of many governmental and private sector operations.
- Cyber-attacks have the potential to destroy the economy of the nation and may pose challenge to energy security. For 'Shamoon' virus that damaged thousands of computers in Saudi Arabia with an intention to pose threat to its oil production. Similar is the case with 'Stuxnet' malware that damaged centrifuges in Iranian nuclear facility.
- Pornographic and vulgar content in the Internet pose challenges to healthy development and adolescents and children.
- Now-a-days social media in the Internet has been vigorously used by terrorists to attract youth as in case of IS.
- Countries like U.S utilizes Internet to spy other countries as evident in PRISM programme of US.

However in the name of cyber-sovereignty government's control over the Internet limits the freedom of people and restricts the seamless connectivity which is one of the basic premises of the Internet. But national security and sovereignty are utmost important to every nation. So it is still good to have cyber-sovereignty even in the age of globalization but the restrictions imposed the government should be rational and should serve the purpose of the day.

In Indian law, cyber-crime has to be voluntary and willful, an act or omission that adversely affects a person or property. The IT Act-2000[10] provides the backbone for e-commerce and India's approach has been to looking at the vast opportunities and the need to sensitize the population to the possibilities of the information age. There is the need to take in to consideration the

10 IT ACT, 2000 came into force on I7th October 2000.

security aspects. In the present global situation where cyber control mechanism are important we need to cyber law. Cyber-crimes are a new class of crimes to India rapidly expanding due to extensive use of internet. Getting the right lead and making the right interpretation are very important in solving a cyber-crime.[11]

Police in India are trying to become cyber-crime savvy and hiring people who are trained in the area. The pace of the investigations however can be faster; judicial sensitivity and knowledge need to improve. Focus needs to be on educating the police and district judiciary. IT institutions can also play a role in this area. Most cyber criminals have a counter part in the real world. If loss of property or persons is caused the criminal is punishable under the IPC.

IT act cases are not getting reported and when repotted are not necessarily dealt with under the IT Act. A lengthy and intensive process of learning is required. A whole series of initiatives process of learning is required whole series of initiatives of cyber forensics were undertaken and cyber law procedure resulted out of it. This is an area where learning takes place every day as we are all beginners in this area. We are looking for solutions faster than the problems can get invented. We need to move faster than the criminals.

The real issued its how to prevent cyber-crime for this, there is need to raise the probability of apprehension and conviction. India has a law on evidence that considers admissibility authenticity, accuracy and completeness to convince the judiciary. The challenge in cyber-crime cases includes getting evidence that will state scrutiny in a foreign court. For this India needs total international cooperation with specialized agencies of different countries. Police has to ensure that they have seized exactly what was there at the scene of crime, is the same that has been analyzed and the report presented in court is based on this evidence. It has to maintain the chain of custody. The threat is not from the intelligence of criminals but from our ignorance and the will to fight it.

The Information Technology Act, 2000 specifies the acts which have been made punishable. Since the primary objective of this act is to create an enabling environment for commercial use of I.T, certain omissions and commissions of criminals while using computers have not been included. With the legal recognition of electronic records and the amendments made in the several

11 Talwant Sing, *Cyber Law and Information Technologies.*

sections of the IPC vide the IT Act-2000, several offences are also registered under the appropriate sections of the IPC.

Intelligence Reform and Terrorism Prevention Act[12] mandates in America, that intelligence are "provided in its most shareable form" that the heads of intelligence agencies and federal departments "promote a culture of information sharing." The IRTPA also sought to establish protection of privacy and civil liberties by setting up a five-member Privacy and Civil Liberties Oversight Board. This Board offers advice to both the President of the United States and the entire executive branch of the Federal Government concerning its actions to ensure that the branch's information sharing policies are adequately protecting privacy and civil liberties.

An example of information technology law is India's Information Technology Act, 2000, which was substantially amended in 2008. The IT Act, 2000 came into force on 17 October 2000. This Act applies to whole of India, and its provisions also apply to any offense or contravention, committed even outside the territorial jurisdiction of Republic of India, by any person irrespective of his nationality. In order to attract provisions of this Act, such an offence or contravention should involve a computer, computer system, or computer network located in India. The IT Act 2000 provides an extraterritorial applicability to its provisions by virtue of section 1(2) read with section 75. This Act has 90 sections.

India's The Information Technology Act 2000 has tried to assimilate legal principles available in several such laws (relating to information technology) enacted earlier in several other countries, as also various guidelines pertaining to information technology law. The Act gives legal validity to electronic contracts, recognition of electronic signatures. This is a modern legislation which makes acts like hacking, data theft, spreading of virus, identity theft, defamation (sending offensive messages) pornography, child pornography, cyber terrorism, a criminal offence. The Act is supplemented by a number of rules which includes rules for, cyber cafes, electronic service delivery, data security, blocking of websites. It also has rules for observance of due diligence by internet intermediaries (ISP's, network service providers, cyber cafes, etc.). Any person affected by data theft, hacking, spreading of viruses can apply for compensation from Adjudicator appointed under Section 46 as well as file a criminal

12 Intelligence Reform and Terrorism Prevention Act, 2004.

complaint. Appeal from adjudicator lies to Cyber Appellate Tribunal.

Digital evidence collection and cyber forensics remain at a very nascent stage in India with few experts and less than adequate infrastructure.[16] In recent cases, Indian Judiciary has recognized that tampering with digital evidence is very easy.[13]

India's first exclusive Cyber Crime enforcement agency is Cyber-Crime Police Station, Bangalore.

Other such enforcement agencies are:

- Cyber-Crime Investigation Cell of India's Mumbai Police.
- Cyber-Crime Police Station of the state Government of Andhra Pradesh, India. This Police station has jurisdiction over the entire state of Andhra Pradesh, and functions from the Hyderabad city.
- In South India, the Crime Branch of Criminal Investigation Department, in Tamil Nadu, India, has a Cyber-Crime Cell at Chennai.
- In East India, Cyber-Crime Cells have been set up by the Kolkata Police as well as the Criminal Investigation Department, West Bengal.

Even the notion of not interfering with the internal affair of other countries is bizarre; it happens constantly all around the globe, with or without the use of internet. From corporate lobbyists to outright coup d'état, this is how the world operates; nations are always interfering with the internal affairs of others either directly or indirectly. It's a sad fact, but no digital sovereignty is going to change that. Don't like what country X is doing? Impose a trade-embargo. Technically you aren't interfering with their internal affairs, just your own, but effectively you are having a massive effect on their internal affairs. Are we directly interfering with the internal affairs of North Korea or respecting its sovereignty? Nah, we just condemn them and let them starve until they change how the way they conduct their internal affairs.

---

13 Bera, Poonam. "Presentation of electronic evidence in court in light of the Supreme Court judgment in Anvar P.K. v. P.K Basheer & Ors. *Read more* Presentation of electronic evidence in court in light of the Supreme Court judgment in Anvar P. K. v. P.K Basheer & Ors.". *ipleaders.in*. iPleaders. Retrieved 6 December 2014.

Conclusion

Cyber-sovereignty in actual terms become cyber-bullying, and many unnecessary websites are blocked due to improper monitoring of content. If the filter is not done properly, it results in violation of Art 19(2) and has a chilling effect on Right to speech, dissent and right to know. Growth in technology has led to proxy sites and various other means which give an easy access to the blocked sites. These proxy sites instead are a much larger threat to national security. More circulation of black money as piracy business gains flow through underground market. Various measures can be adopted instead of taking the extreme route like placing a statutory body to monitor and track content, forming a committee of experts from different nations to evolve a common consensus, treaties among nations protecting each other's sovereignty. The 21st century vision of "Digital India" with restrictions on internet would be like a travel agent who books only bus ticket. Hence few rational measures are required in this Indian context. If we compare to china country, India's position is better than in the IT field but as a sovereign, secular and democratic country over the worldwide, it takes time to introduce cyber-sovereign in Indian context.