

Cyber Sovereignty and the Challenges of Cyber Security in Contemporary World

Narendra Singh¹, Arpit Parakh^{2,*}

Abstract

With the advancement of technology and cyberspace, basic principle of International law i.e. Sovereignty has been shaken up. Initially only users were leading over internet and therefore basic notion was that it is immune from sovereignty of state because of its cross-border nature. But in current scenario with the outburst in number of internet users, and various laws and regulations framed by different nations to govern cyber sovereignty and security of cyber data, cyber space is not wholly immune from state governance. Now a day Cyber security has become worldwide issue & is on the path to become top most security menace for all countries. As the internet user are growing day by day across the globe, states desired greater sovereignty over the cyberspace due to increase in number of cyber threats. This Research paper will discuss the concept of Sovereignty over Cyberspace, Challenges to Cyber Security and Indian position dealing with Cyber Security and Governance of Cyberspace.

Keywords: Cyber security, cyber sovereignty, cyber terrorism, global commons, sovereign domain

INTRODUCTION

Cyberspace faces more challenges in terms of security and regulation than outer space. Despite the fact that the universe is limitless, each planet or structure within it have physical limits. Cyberspace on the other hand has zero. The Internet lacks borders as a result of a lack of boundaries. Cyberspace poses new set of legal questions, and old rules can't justify it. Every law is a territorially based either concerned with the sovereign state or between the states.

The cyberspace has revolutionized the globalized world like never before. The nation has invested hugely to set up information and communication technology infrastructure to get more citizens online and benefit them from the facilities online. With the tremendous growth of cyberspace also comes along challenges of cyber security [1].

Cyber security has become worldwide issue in contemporary era & is on the path to become top most security menace for all countries.

Cyber Security has a vital role to play in this era of IT (Information Technology). One of the main issues in today's scenario is how to protect information. "Cyber Crime" a term which popped up in our minds when we talk about the concept of cyber security & these types of crimes are continuously increasing now days.

In this research paper author has discussed about the concept of cyber sovereignty, jurisdiction over cyberspace, cyber security and its challenges, and finally end the paper by discussing Indian position on such cyber problems.

*Author for Correspondence

Arpit Parakh
E-mail: parakharpit2108@gmail.com

^{1,2}Student, Department of Law, Maharashtra National Law University, Nagpur, Maharashtra, India

Received Date: August 19, 2022
Accepted Date: August 25, 2022
Published Date: September 13, 2022

Citation: Narendra Singh, Arpit Parakh. Cyber Sovereignty and the Challenges of Cyber Security in Contemporary World. National Journal of Cyber Security Law. 2022; 5(1): 20–26p.

CYBER SOVEREIGNTY

The Central base of contemporary international order is sovereignty of countries, concept that many scholars relate back to the “*Peace of Westphalia 1648* [2].”

As to understand the core role of the sovereignty is necessary, but the typical job is to define the term Sovereignty accurately. According to dictionary of Black Law, it is “i) *Supreme dominion, authority or rule* ii). *the supreme political authority of an independent state* iii) *the state itself* [3].”

In 1990 many internet organizations believed that sovereignty over the internet was in the hands of the user only. It was the user who was having control over the cyberspace. It was not governed by any states. It was that time it was argued that cyberspace break the physical borders and creates a different set up of man-made activities & decline the viability and legality of legislations which is built on physical boundaries.

It is contended by internet proponents that policymakers do not control cyberspace, even though they have the ability to do so. Cyberspace fundamentally destroys the connection between physical position & authority of a native sovereign’s attempts to govern universal occurrences.

“Cyberspace is Not Immune from the State Sovereignty” & Following are Some Reasons

- I. The Cyberspace has no limits and no boundaries. In order for cyberspace to survive and operate, it must be managed by someone. Users would not be able to enter cyberspace without a physical structure. However, since the concrete structure is based on the earth, it inherently comes below the state where these physical resources are stored. It does, however, include a physical dimension that contains computers, integrated circuits, wires, and networking networks. It also has a technical layer made up of machine logic, data packets, and electronics, as well as a social layer made up of humans. This physical equipment is owned by states and corporations and is situated within a state’s jurisdiction. As a consequence, cyberspace does not exist outside of the real universe, but rather is a part of it. Sovereignty of state can be exercised on the cyber networks in its geographical boundaries as well as over people within its territories and outside its borders. Now there are two explanations as to why there is no immunity from the sovereignty of State:
 - a. Any particular entity must govern this cyberspace so as to maintain its existence & proper functioning as it necessitates a physical arrangement, because in absence of such thing users would have no entrance. This physical arrangement is place somewhere on earth only and hence it comes under the control of state where these physical units exist. Moreover this cyberspace itself needs regulation and control [4]. E.g. Internet Corporation of Assigned Names and Numbers (ICANN) is an association which undertakes and manages important issues such as allocating DN (domain names) & IP addresses [5].
 - b. Economical connections in cyberspace require legislations to manage & oversee these connections and transactions [6].

As a result, the concept of sovereignty extends to state’s electronic operations, owing to their right to control certain matters within their geographical boundaries and exercise autonomous state powers.

- II. The state has right to exercise its sovereign rights over cyber assets in its territories solely and unilaterally. Any states prefer to restrict certain aspects of cyber activity on their soil, such as the collection of personal data and the content that is permitted on the internet. Some states place more strict restrictions on internet access and personal records. Like in United States, they came up with various cyber laws so as to regulate the cyberspace. U.S came up with the “*Computer Fraud and Abuse Act, 2012*” and the “*Electronic Communications Privacy Act, 2012*.”
- III. If we consider cyberspace to be immune from the state sovereignty then all those financial transactions which takes place on the cyberspace would be unsubstantial. There must be a law to govern these transactions therefore the states from both the side plays an important role while governing the cyberspace. Therefore it is quite evident that the cyberspace has no immunity towards sovereignty of states.

- IV. Each state governs the material available on the cyberspace as per their needs. Certain states have banned the illicit pornographic content including India also. Recently, In India, Government of UP will be accessing the search history of the residents of UP. This clearly shows that cyberspace has a control over it not cross border but indeed within the borders.
- V. Cyberspace plays a crucial role in National security. Nuclear activities, national records all are stored in the cyberspace. Recently there was a hacking activity all over the country. And prevent form such attacks in future state takes appropriate steps to regulate the cyberspace. This cyber sphere is not in any way dissimilar from that of other spheres where states use to preserve its right to defend its safety. As a concern of national security, states are progressively required to prove their existence in this cyberspace. A number of states are conducting and has started several operations and infrastructure projects from cyberspace [7]. If it is determined that use of force is important for cyber security of state, then states would have use such force in cyber space as they use to do in other spheres.

CYBER SPACE IS GLOBAL COMMON OR NOT?

It is not required to become global common that the particular area is “natural asset outside natural jurisdiction [8].” Relatively global common is generally characterized by following five exclusive features:

- i. It has an International Treaty to govern it.
- ii. Such treaty allows definite uses and restrictions of it.
- iii. It has boundaries and it can be defined.
- iv. Countries have decided to relinquish its claim of specific sovereignty on any part of it, or otherwise leave it undeclared as in the case of Antarctic.
- v. No particular single country can control it.

We can say in different words that global common does not mean that there is no sovereignty at all but it means that a shared universal sovereignty is present over it. So after having this consideration, it is not correct to classify cyberspace as global common because abovementioned five exclusive prerequisite of global common are not fulfilled by cyberspace.

ISSUE OF RECOGNIZING CYBERSPACE AS A “SOVEREIGN DOMAIN”

One of the central problems regards bringing the concept of sovereignty over cyberspace is how to persuade countries that cyberspace is also such sphere where states can declare their sovereignty. Secretary of Defense entered the “National Military Strategy for Cyberspace Operations” in 2006 which provides that cyberspace is also one of its domains like other domain such as sea, air etc. [9]. However considering it as a specific domain is surrounded by disagreements. Even some people from the defense dept. were of the views that it is not separate domain [10]. But this kind of disagreements and debates over its separate domain nature should not opaque the important fact that it is also man-made creation, and so states can proclaim its control on cyberspace.

Cyberspace needs a specific physical structure to sustain, it requires regulations formed by government so as to work properly, and nations are trying to impose more control on it [11].

ANALYSIS OF JURISDICTION OVER CYBERSPACE

In recent time the ideology of cyberspace being governed by the states is changing into a state to state control. There are issues between different states and not between individual person and state in existing cyber governance & cyber sovereignty. Fundamentally, the USA, its allies and European countries contend that it is not and should not be under control of sovereign state, on the other side, Russia, China & some other states contend that cyberspace should be controlled by sovereigns either individually or by forming arrangement.

States play an important role in regulating the cyberspace thus to find out a solution states have to surrender our territorial notions in order to establish a long-term solution to the issue of cyberspace

regulation. Countries must join together to build both short and long term options. Regarding a long-term, an international solution must be developed. In this regard states should confer to make and enter into a treaty which deals strictly with the Cyberspace. This convention should define international law that regulates intellectual property issues as well as all other legal issues related to internet, with each member country upholding it. If required, such a convention could also overcome the jurisdictional problem by designating Cyberspace as its own jurisdiction and forming an international judicial system for Cyberspace as a subject matter jurisdiction.

Recent developments have signaled a positive change in how nations handle security problems, with an emphasis on working to fix cyber issues that can't be addressed in a single sovereign nation. Cyber war, cyber espionage, and cybercrime are problems that go beyond a single state's regulatory forces, necessitate collaboration and support from all sovereign states, and increase prospect of state dispute above the disputed realm of "cyberspace".

Thus at present it can be concluded that cyberspace is not at all immune from sovereignty of the states as they are playing active role in regulating their internal cyberspace ranging from transactions to what needs to show people.

CHALLENGES OF CYBER SECURITY

The increasing Cybercrime & Cyber terrorism is the large threat to cyber security now days, not limited to India but a universal problem. It has become worldwide issue & is on the path to become top most security menace for all sovereign countries.

At present we can send, receive any kind of material which may be in form of e-mail, or video merely by pressing a key but did you ever thought about safety of your data which you are transferring to third person, is such data safe [12]?

And the answer to this is in concept of Cyber Security. Internet in our life is one of such infrastructure that is developing day by day with high speed. A number of newest technologies are coming in current high tech environment and creating changing effect on human life. On the other hand with growth of recent technologies, we are facing a lot of problems in protecting our personal data in proper manner & this leads to enhancement in cybercrimes with every passing day.

This is one of the largest concerns for countries and societies today as they move from agro-industrial age to the Information Age. It is paradoxical that on one hand information and communication technologies (ICT) are at the heart of all facets of human life and are central to national, economic and human security, and on other hand the level of their penetration creates certain vulnerabilities [13].

It is very necessary to increase this security for cyberspace & protect important info for security and economic wellbeing of every country. As almost every state and its government is making, enacting, and implementing stringent legislations to deal with this issue so as to stop such leakage of critical data and resources.

There are various threats to Cyber Security which we can categorize on the basis of offenders & their purpose in four sectors as: cyber warfare, cyber terrorism, cyber espionage and cybercrime [14].

These offenders mostly use various kinds of loopholes in cyberspace for accomplishing their acts. These people use to derive unwanted benefits from feebleness of software designs by using different kind of malwares. Some tricks like hacking is usual method of penetrating the safeguards in secured systems & intervening functioning of these systems. Another common way is identity theft. The possibility of cyber offences and creating loopholes in it is enhancing day by day.

Cyber Warfare

Though there is no specific definition of this term anywhere, yet cyber warfare means those activities of one state towards other state in order to attack their information system so as to disrupt their proper infrastructure. There are some instances such as website attack 2007 in Estonia, & in 2008 attack in Georgia. Every nation is recognizing that 21st century war is going to be highly based on cyberspace. Instances of this can be observed from Russian attack on Estonia & Ukraine. It was totally cyber intervention in Estonia whereas it was blend of cyber & kinetic attack in Ukraine, “wherein the bits preceded the bullets [15].”

Cybercrimes

Cybercrimes pose an actual danger now days & they are rising quickly in term of intensity & difficulties with the advancement in internet & mobile phones. As dismal as it may sound, cybercrime is outpacing cyber security. About 80% of these cyber-attacks are in form of cybercrimes. There are many types of cybercrimes such as hacking, phishing, phreaking, identity theft, etc.

These crimes are expected to rise rapidly due to number of factors such as various sectors like virtual currency, cloud technology, robotics, etc. Dark net is exploiting for sale of drugs, weapons, recruiting terrorist, etc.

Cyber Espionage

Now days we came across instances of this crime on daily basis as we come to know about news of exfiltration of huge amount of data & intellectual property which amount to millions in rupees from websites of government & also private entities.

As the internet is now one of the strong and fast sources of collecting intelligence in order to fulfill national, military, economic & diplomatic objectives.

According to one estimate, about 90 percent of open source data related to intelligence is usually acquired from this cyber world.

This particular crime is also used for theft related to technology & also for hurling probe operation on complex infrastructure so as to exploit it later.

Cyber Terrorism

It is a form that is being used as a channel so as to plot different terrorist attacks, also for recruiting sympathizers, or as a novel dome for assault in chase of the terrorist’s social & political purposes [16].

In current scenario, these terrorists are also known to have utilized this cyberspace for number of purposes like “communication, command and control, propaganda, recruitment, training, and funding purposes.” And so from this viewpoint, the challenges of these non-state actors to security of nation are tremendously severe.

INDIAN POSITION IN DEALING SUCH CYBER PROBLEMS

India is very vulnerable to cyber challenges and threats because major population here is actively using internet in its day to day life for every kind of activity like shopping, banking, studying etc. There is increasing frequency of cyber-attacks in India such as leak of personal information of 3.2 million debit cards (2016), Data theft at Zomato (2017), Wannacry Ransomware (2017) etc.

Indian parliament enacted Information Technology Act in 2000 which was earlier centered around theme of giving legal recognition to electronic transactions. But later on it covered data protection, privacy, cyber offences such as cyber terrorism etc.

Section 36 of Information Technology (Amendment) Act, 2008 provides that Indian Computer Emergency Response Team (CERT-In) would be national agency to deal with incidents of cyber security.

Information Technology Act, 2000 contain following provisions to deal with offences related to computer sources:

- Section 43 of this act provides for compensation to victim in case of unauthorized access to computer system and certain other events as given in this provision [17].
- Section 65 of the act deal with the tampering with computer source documents [18].
- Section 66 provides for punishment to person who committed any act under section 43 with dishonest or fraudulent intention [19].

By virtue of amendment act 2008, new sections i.e. Section 66B to 66F were added which provides for punishment in case of identity theft [20], cheating by personation [21], cyber terrorism [22] etc.

Ministry of Communication and Information Technology notified the National Cyber Security Policy 2013 (“NCSP”) with number of objectives including dealing with an aim to strengthen the regulatory framework for ensuring a secure cyberspace ecosystem and to enable effective prevention, investigation and prosecution of cybercrimes.

CONCLUSION

In 21st century global economy, we can conclude that cyber space is one of those important aspects that links number of actors together, boosts efficiency, opens fresh marketplaces and facilitates managing arrangements which are flatter, and also have an outlying further wide reach. No single country can ensure fully protected cyber security regime on its own without establishing worldwide infrastructure by joining hands with other countries.

So it has to be a combined effort that warrants international cooperation. Some few regional initiatives such as “Budapest Convention on Cybercrime” are there since decades. These types of initiatives can be combined in form of universal applicable convention for cyber security and to govern cyberspace. Therefore it is now high time that there is need to form an “International Convention on Cyber Security and Governance of Cyberspace.”

REFERENCES

1. Anis Ahmad, Cyber Security Challenges: Some Reflections on Law and Policy in India, 1 HPJ (2017).
2. Marie Baezner and Patrice Robin, Cyber sovereignty, Cyber defense Trend Analysis, Center for Security Studies (CSS), ETH Zurich (2018).
3. Sovereignty, Black’s Law Dictionary (11th ed. 2019).
4. See Internet Assigned Numbers Authority, Introducing IANA, <http://www.iana.org/about/> (last visited December 15, 2021).
5. See Internet Corporation for Assigned Names and Numbers, ICANN Factsheet, <http://www.icann.org/en/factsheets/fact-sheet.html> (last visited December 15, 2021).
6. Jack L. Goldsmith & Tim Wu, Who Controls The Internet?: Illusions of A Borderless World 29-46 (Oxford University Press, New York 2006).
7. For example, “The National Strategy to Secure Cyberspace lists a number of critical infrastructures that are dependent upon cyberspace such as Banking & Finance, Chemical, Oil, Gas and Water.”
8. Supra note 3, at 17.
9. See U.S. DEP’T OF DEF., The National Military Strategy for Cyberspace Operations 3 (2006), available at <http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc 1.pdf>
10. David R. Luber & David H. Wilkinson, Defining Cyberspace for Military Operations, 93 MARINE CORPS GAZETTE, 40 (2009).

11. *Supra* note 5.
12. Reddy, G. N. & G. J. U. Reddy, A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies, ArXiv (2014).
13. Lieutenant General Davinder Kumar, Cyber Security: Fundamental to India's Sovereignty (Vivekananda International Foundation, 2018).
14. India's Cyber Security Challenge, Cyber Security-An Overview, IDSA Task Force Report 21 (March 2012)
15. *Id.* at 9.
16. *Id.* at 24.
17. The Information Technology Act, 2000, § 43, No. 21, Act of Parliament, 2000 (India).
18. The Information Technology Act, 2000, § 65, No. 21, Act of Parliament, 2000 (India).
19. The Information Technology Act, 2000, § 66, No. 21, Act of Parliament, 2000 (India).
20. The Information Technology Act, 2000, § 66B, No. 21, Act of Parliament, 2000 (India).
21. The Information Technology Act, 2000, § 66D, No. 21, Act of Parliament, 2000 (India).
22. The Information Technology Act, 2000, § 66F, No. 21, Act of Parliament, 2000 (India).