IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

# NATIONAL SECURITY THREATS IN CYBER SPACE

**Shivaansh Maini**
5th Year BBA LLB Learner at Symbiosis Law School, Noida

## ABSTRACT

The Internet, telecommunications networks, computer systems, and embedded processors and controllers are all components of the global information infrastructure, which is an interconnected network of information systems infrastructures. It is believed that with growing rise of Cyber Space users as well as data, the threat from it is on a steep pedestal, of which national security threats are one. The data was analyzed through secondary method of researching and the finding that were researched was firstly, perspective of different countries on national security threats from cyberspace, secondly, national security strategy of India, lastly, security of shared information structure policy. The conclusion reached was even though there is a big threat to nation from cyberspace but cyberspace is also one of the key development technology for growth in the nation, and that, the nations must stay prepared to for such threats.

## INTRODUCTION

The word "cyberspace" was coined by William Gibson in one of his short tales, "Burning Chrome." The importance of cyberspace has risen in recent years, and securing it needs concerted actions on the part of the federal, state, and municipal governments. With the increased usage of the internet, cyberspace has expanded to a worldwide scale, with everyone linked via routers, cables, and switches. In a nutshell, numerous individuals and businesses have exploited cyberspace to expand their industries abroad during the last decade.

In today's society, almost everything is powered by the internet, and the internet has created a social sphere that is integrated into our daily lives. Because everyone utilises the internet on a daily basis, there are subnational groups and government organisations that utilise cyberspace in a variety of ways to aid in a country s growth. Then there are terrorist groups that utilise cyberspace to recruit and train members of their groups; these terrorist groups also use cyberspace to launch attacks against their target organisation or country from whom they seek to get intelligence services.

## RESEARCH METHODOLOGY

For the research, only secondary data is used to attain information, facts and details on the topic. Newspaper, Books, Journals, Research Papers, Articles, blogs etc. were put to use. The research was neither based on

collection of data from people through surveys or interview, the research work is purely from the researcher s own understanding from the data.

## HYPOTHESIS

Almost every device in today s society is connected to the internet and thus has a strong potential of being hacked. In today s world, every country is connected via cyberspace. There are several new criminal behaviours occurring nowadays in cyberspace, where cyber criminals commit cybercrime regardless of their physical location. Nowadays, cybercrime is mostly committed to get sensitive information or commit financial crimes. If there appears to be a national security concern in cyberspace, there are several international collaborations between governments to combat cybercrime, including seminars, joint workshops, and many other activities. These factors contribute to the development of nations cyber-security teams and the creation of a more secure cyber space for their particular countries.

## RESEARCH QUESTIONS

1. What are the various threats to national security in cyber-space?
2. What is strategy of India to strengthen its cyber space?
3. What are the various international cooperation on cyber security?

## SCOPE AND LIMITATION

This research does not take into account future threats from cyber-space to national security and is only limited to the currently identified threats to national security in cyber-space. This research is limited to present situation and not on future interpretations.

## CHAPTERS

### I) National Security Threats

Every country is now connected to the rest of the globe via cyberspace. Combating hackers/criminals has become more challenging as the number of attacks has increased. A country s system, which serves essential defence and intelligence functions, should be secure regardless of its location. The internet has become a tool for political, economic, and military espionage in the modern day. Numerous cyber-attacks have occurred in the past, including the following:-

• According to reports, Chinese hackers targeted Indian vaccine manufacturers Serum Institute and Bharat Biotech in order to obtain knowledge on the Corona Virus vaccine.

• In the summer of 2007, a single attack rendered the Pentagon s 1500 computers inoperable.

• The Pentagon, the United States of America s defence department, reports that it identifies over three million unlawful scans for efforts by attackers to get official data. Numerous cyber-security specialists assert that China and North Korea, among others, are instructing hackers on how to employ cyber warfare methods.

• Estonia s Ministry of Defence stated that a concerted attack on their cyber infrastructure was launched in response to a disagreement with Russia, dubbed "WEB WAR 1."

• According to reports, Chinese military cyberattacks entered the Pentagon, the German Chancellery, and England s Whitehall in 2007.

By the twenty-first century, numerous terrorist organisations had established a virtual presence on the internet. They make extensive use of the internet for a variety of purposes, including psychological warfare, data mining, money raising, recruitment, planning, and coordination. These terrorists act decentralised, making it impossible to monitor them at any particular time. They obtain information for their activities via the internet. Numerous terrorist organisations today seek members with university degrees in computer science. They mostly utilise the internet to disseminate propaganda, raise funds, and attract new members. To successfully combat these dangers, we collect intelligence, conduct investigations, and undertake operations against them. We must combat these by recognising their strategies and developing the ability to operate in the same media. Additionally, to apprehend a thief of this calibre, you must think like them.

We are all aware of the conflicts between India and Pakistan, which resulted in widespread damage, most notably of human lives. Nowadays, conflicts are waged not just with guns and tanks, but also on social media. Since the proliferation of information technology throughout South Asia in the mid-1990s, the speed of cyber war between India and Pakistan has also grown. The first glimpse occurred during India s nuclear testing. Soon afterwards, a gang of Pakistan-based hackers gained access to the website of the Bhabha Atomic Research Centre and began posting different anti-Indian remarks. Such incidents occurred often during the 1999 Kargil War and in December 2001-02.

As a result, the time between 1999 and 2002 was very crucial, as the military exchanged gunfire along the Line of Control, and hackers attempted to shut down the websites. Fortunately, the cyber war was brief, as both countries just defaced websites.

## II) National Cyber security Strategy for India

A framework for a national plan to safeguard cyberspace should be critical for economic development and national security, and this should be a public-private cooperation. Only through collaboration can a safe future in cyberspace be possible. To make a strategy work, there must be a comprehensive plan that encompasses a large cross-section of the country. To create a safe cyberspace, there should be collaboration between government, industry, academia, and non-governmental organisations. National-level discussions and seminars should be held around the country.

Harvard University s "National Cyber Power Index 2020" evaluated the capabilities and intentions of 30 nations interested in acquiring "cyber power," with India ranking 21st. It was certain that India s internet deterrence efforts had met with minimal effectiveness. This is a grave worry, as China is continually attempting to expand along its northern and eastern borders.

The National Cyber Security Policy, which was established in 2013, guided the federal government s cybersecurity policies. Following that, technology has grown at a breakneck pace, necessitating that these issues be handled at the highest level and with a comprehensive manner.

In December 2019, the National Security Council Secretariat released a request for proposals for a National Cyber Security Strategy (NCSS) for the period 2020-2025. The NCSS would "ensure the Nation s cyberspace is safe, secure, trusted, resilient, and lively."

## III) Collaboration to Ensure the Security of Shared Information Infrastructure

The Indian and US governments have collaborated to solve national security concerns arising from their respective countries reliance on network information systems. At President George Bush and Prime Minister Atal Bihari Vajpayee s 2001 meeting in Washington, DC, the primary topic of discussion was how to improve the security of shared information. This effort began in April 2002 with the formation of the US-India Cyber Security Forum. It was a group focused on collaborating on policy, procedural, and technological concerns confronting both nations in the area of cyber security. After both governments pledged to enhancing collaboration, a joint Indo-US Cyber Security Initiative was launched. The initiative will focus on developing a strong cyber security team through expert exchange, training, information sharing, and expanding the private-public partnership. Since 2002, six groups have established a framework for a Cyber Security Forum to address particular issues:

• Legal Cooperation and Law Enforcement (co-chaired by the Department of Justice of the United States and the Indian Ministry of Home Affairs)

• Research and Development (co-chaired by the Ministry of Defence s Development Organization and the Department of State and Defense Research)

• Critical Information Infrastructure, Watch and Warning, and Emergency Response (co-chaired by the US Department of Homeland Security and the Indian Department of Information Technology s Computer Emergency Response Team)

## CONCLUSIONS AND SUGGESTIONS

The cyberspace is a showcase for your inventions and prosperity, as well as a tool through which we may increase global wellbeing. However, because of the breadth of its loose and light digital infrastructure, it represents a significant threat to governments, private sector, and people.

The government should assume responsibility for informing the nation's citizens about possible risks. We should understand that cyber security is the most critical national security concern in today s society. Cyberspace is vast, and there are several potential issues. The nation's digital infrastructure must be considered as a national asset and safeguarded. In the case of an attack, every effort should be taken to quickly identify the threat and recover.

Nowadays, since our reliance on and usage of computers has expanded, every nation is vulnerable to cyber-attack. The best way to deal with this is to remain prepared. We cannot be startled by a cyber-attack nowadays, since they may occur at any moment and to anybody.

## REFERENCES

1. D M Chudasama, L K Sharma, N C Solanki, Priyanka Sharma , "A Comparative Study of Information Systems Auditing in Indian Context", IPASJ International Journal of Information Technology (IIJIT), Volume 7, Issue 4, April 2019 , pp. 020-028 , ISSN 2321-5976. UGC Approved (S. No 45786).

2. D M Chudasama, L. K. Sharma, N. C. Sonlanki, Priyanka Sharma, "Refine Framework of Information Systems Audits in Indian Context", International Journal of Computer Sciences and Engineering, Vol.7, Issue.5, pp.331-345, 2019. ISSN: 2347-2693UGC Approved (S. No 63193).

3. D M Chudasama, Kathan Patel, Parshwa Dand, "Awareness of Data Privacy Breach in Society", International Journal of All Research Education and Scientific Methods (IJARESM), Vol.8, Issue.10, pp.303-307, 2020. ISSN: 2455-6211UGC Approved.