JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

INDIA'S QUEST FOR CYBER SECURITY: A CRITICAL APPRAISAL

Dr. Yogendra
Assistant Professor
Department of Defence and Strategic Studies,
Kunwar Singh P.G. College, Ballia (U.P.)

ABSTRACT

The threat of cyber security has significantly increased for India's national security. India is dealing with a variety of cyber threats, including harmful cyber-attacks, cyber-crime and cyber espionage. In 2021, ransomware attacks against Indian businesses rose by 218%. Since computer networks, systems, and related technologies are now utilised by all types of organisations, both public and private, as well as by individuals, the majority of cyber-crimes are now carried out with the intent to get personal information or engage in fraudulent activities. Modern gadgets are almost universally internet-connected, putting them at a significant risk of cyber-attacks. These dangers might significantly harm the nation's economy, society, and security. Prosperity requires national security. India's economic success is founded on the smooth operation of its administrative, military, public service, and social infrastructures, all of which in the present era are totally dependent on the internet. As a result, protecting national security necessitates assuring cyber security because it is no longer an option to defend cyberspace. India is taking steps to ensure the infrastructure for its cyber security, but the threats are still significant. To address the issue, the Indian government has implemented certain preventive measures through its "Cyber Security Policy 2020". But more drastic measures are needed. The main goals of this research study are to analyse existing cyber security policy and to identify and evaluate the cyber security difficulties that India is now facing.

Keywords: Cyber Attacks, Cyber Security, Cyber Space, Cyber Threats, National Security.

1. INTRODUCTION

We are in the digital era. The advent of digitalization has had a profound impact on every element of human life. The media's and information technology's unprecedentedly rapid and extensive penetration have ushered in the digital age. Globalization has not only unified the world but also sparked economic expansion. The new

catchphrases of this digital transformation are technology and information. We are living in a linked world with new commercial and cultural perspectives. With billions of dollars moving daily across the globe, business is conducted at the speed of light. A new security paradigm, with new risks to both national and human security, has also been brought about by the change from the industrial to the information era **(Kumar, 2016**). In fact, national security in this technocratic era is threatened by hitherto unidentified threats that try to demolish a state's infrastructure. It is undeniable that modernization and technology are essential for social and economic development in a world that is more interconnected. For governments, businesses, and communities to carry out their basic functions, there must be a sophisticated technology-based infrastructure. However, the internet is a dangerous place on many levels because of its huge, unobservable universe **(Naha, 2022)**. As cybercrime and hazards have grown significantly, information technology utilisation has been proving to be a double-edged sword. Cyberspace has emerged as a critical issue of national security as India moves toward increasing digitization in all domains. India recorded 52,974 incidences of cybercrime in 2021, up more than 5% from 2020 (50,035 cases) and more than 15% from 2019 (44,735 cases) (**Drishti IAS, 2022**).

2. REVIEW OF LITERATURE

Brenner (2004). This paper explains the first method for coming up with indicators for measuring cybercrime. The researcher provides a straightforward taxonomy of harms consisting of three types: individual, systemic, and collective, despite the fact that defining metrics and scales for cybercrime is extremely difficult due to concerns about apprehension, size, and evidence.

Sims (2011). According to this paper, a new cyberspace has emerged because of the Information Age, reducing necessary borders and fostering international collaboration while strengthening enemies. Governments are in charge of ensuring both the general welfare and national security. The country will need to establish laws that address cyber threats, hold perpetrators of cyber attacks accountable, and develop regulations requiring security in specific sectors.

Chertoff et al. (2015). Address the state of Internet jurisdiction law today and the challenges involved in determining the proper venue for a lawsuit that involves many states. They provide four possible formulations for identifying the prevailing jurisdiction in a transparent and equitable manner.

Van Slyke et al. (2016). The study creates a taxonomy of harms for white-collar crimes by concentrating on the victimization part of these crimes.

Patel and Chudasama (2021). The report identifies the cyber threats that various nations face on a global scale. Nearly every device in the modern world is internet-connected and has a good probability of being compromised. Nowadays, there are a variety of new illegal activities that are carried out in cyberspace, where criminals commit cybercrime from anywhere in the world. Most cybercrimes committed nowadays are motivated by financial gain or the desire to obtain sensitive data.

Alik (2022). According to this paper, India must pursue an offensive cyber warfare strategy as a means of maintaining strategic balance. Cyber warfare is challenging to identify and combat, because it has the potential to seriously damage infrastructure and financial resources while needing little funding. Given India's expertise in this area, an aggressive approach to cyber warfare is a real possibility.

3. OBJECTIVES

- To identify and evaluate the main cyber security challenges faced by India.
- To analyse India's current cyber security policy.

4. METHODOLOGY

The study is purely descriptive. In this study, content analysis and observation were utilised as methodologies. An examination of secondary sources, such as books, book chapters, journals, papers, articles, websites, blogs, and other pertinent documents connected to this research work.

5. CYBER SPACE

The term "cyber space" describes the virtual computer environment and, more specifically, an electronic medium that is utilised to support online communication. Cyber space typically consists of a sizable computer network made up of numerous global computer sub-networks that use the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol to facilitate communication and data exchange. The main characteristic of cyber space is the virtual, interactive setting it provides for a wide spectrum of users (***What Does Cyber Space Mean?*, 2022**).

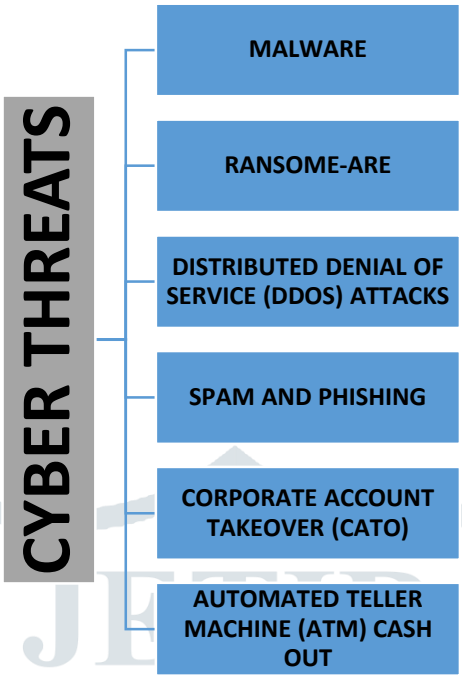
6. CYBER THREATS

An expression of intent to damage or engage in violent behaviour against someone or something referred to as a threat. An expression of threat may be verbal, written, or symbolic. **(The University of Arkansas, Little Rock, n.d.).**

Any situation or occurrence that may negatively affect an organization's operations, assets, users, other organisations, or the country through a system, whether through illegal access, information deletion, disclosure, modification, or denial of service, is called a cyber threat (**National Institute of Standards and Technology, 2011).**

Figure.1

Current Cyber Threats



Source: **Commonwealth of Massachusetts (n.d.)**

6.1 Malware: Malware is referred to as malicious software or malicious code. A programme called malware is injected into a system to jeopardise the availability, confidentiality, or integrity of data. Malware has the potential to disrupt and cause extensive damage.

6.2 Ransomware: Malware-based ransom ware restricts or prohibits users from accessing their systems. Ransomware demands that you use online payment methods to pay a ransom in order to recover access to your system or your data. Virtual currencies like bit coins are frequently used in online payment systems.

6.3 Distributed denial of service (DDoS) attacks: DDoS attacks disable an online service by saturating it with a lot of traffic from many places and sources. During a DDoS attack, a website's response time slows down, blocking access. By installing malware, cybercriminals create massive networks of compromised machines known as Botnets. It's possible that a DDoS assault is not the main cybercrime. The attacks frequently serve as a diversion while other fraud and cyber breach attempts are made.

6.4 Spam and Phishing: Spam encompasses emails and messages that are undesired, uninvited, or unwelcome. Phishing is a type of social engineering that involves attempting to obtain sensitive data. Phishing attempts will look to come from a reliable source.

6.5 Corporate Account Takeover: CATO is a type of business entity theft in which online criminals pretend to be the company and send fraudulent wire and Automated Clearing House (ACH) transfers. The unlawful funds are transferred to the cybercriminal's accounts.

6.6 Automated Teller Machine (ATM) Cash out: This kind of ATM scam involves big money. Cash-outs include multiple ATM withdrawals of significant amounts of money at once from various locations. It might also involve multiple hefty ATM withdrawals.

7. CYBER SECURITY

The use of technologies, procedures, and policies to defend systems, networks, software, hardware, and data from online threats is known as cyber security. By lowering the danger of cyber attacks, it seeks to safeguard against unauthorised use of systems, networks, and technology (**What is Cyber Security?, n.d.).** Cyber security, also known as information technology security, refers to the methods used to safeguard computers, networks, programs, and data from unauthorised access or attacks that are intended to exploit vital information infrastructure and cyber-physical systems. Cyber-physical systems connect physical infrastructure and things to the Internet and to one another by integrating sensing, computation, control, and networking. Examples include smart grids, robotics systems, water systems, and industrial control systems (**Drishti IAS, 2022).**

8. IMPACT OF CYBER THREATS ON INDIA'S NATIONAL SECURITY

In order to facilitate access and convenience of use and keep up with our rapid growth, more and more systems are being moved to virtual space. This trend's drawback is that such systems are now more susceptible to cyber-attacks (**Next IAS, 2021**). Cyber attack is defined as illegal system or network access by a third party. Hackers or attackers are those who conduct a cyber attack **(Emeritus, 2022).** If hackers are successful in breaching a nation's banking, energy, or nuclear systems, for instance, there is concern of widespread harm and enormous loss. Power is a necessity for practically every area of the economy, so the collapse of the power system might have a significant effect (**Next IAS, 2021**).

A Chinese organization by the name of Red Echo has dramatically increased its use of tools like malware to target "a big swathe" of India's power sector. ShadowPad is a piece of malware that uses a backdoor to access servers and was utilized by Red Echo **(Drishti IAS, 2022).**

According to a 2021 study from the American cyber security company **Palo Alto Networks**, Maharashtra was the most often attacked state in India, receiving 42% of all ransomware attacks. India is one of the most economically lucrative countries for hacker groups; thus, these hackers demand ransom payments from Indian companies in the form of cryptocurrency in order to regain access to the data. In 2021, one out of every four Indian businesses experienced a ransomware assault, which is more than the global average of 21%. Among the most targeted industries were software and services (26%), capital goods (14%), and the public sector (9%) **(Next IAS, 2022).** The months of June and July 2022 saw the hacking of almost 2,000 Indian websites; this is one of the most significant cyber attacks against India in recent memory. A letter sent to two cybercriminal organisations, "Dragonforce Malaysia" and "Hacktivist Indonesia," accused them of hacking 2000 Indian websites using computers they controlled in Indonesia and Malaysia (**The Economic Times, 2022**).

9. THE DIFFICULTIES WITH INDIA'S CYBER SECURITY

According to **Next IAS (2021),** there are following cyber security challenges faced by India:

9.1 Low levels of general public digital literacy: Despite being the world leader in the technology sector, India has a low degree of general public awareness of internet etiquette. It is sometimes said that individuals are readily tricked by click baiting into engaging with information that frequently contains malware attached to it. This has the potential to lead to large-scale fraud in the future when combined with the rapid switch to online financial transactions after demonetisation and the COVID-induced lockdown. Therefore, it is essential to educate individuals about the dangers of clicking on shady links.

9.2 System vulnerabilities: It is important to identify and fix any system vulnerabilities that could let in unauthorised users. For instance, it is anticipated that highly sensitive nuclear data will be protected by encryption, yet when people access the systems, they may be susceptible to human error. Similar to this, third-party software occasionally has backdoor access features or malware bundled with the installation file. By carefully monitoring the system and implementing effective user account control, these problems can be resolved.

9.3 Governmental cyber-attacks: A negative tie with China anticipated accelerating cyber-attacks from it. The issue with such state-sponsored attacks is the hackers' access to limitless financing to compromise foreign networks. This means that in order to confront such threats from China or other nations, we must set aside enough resources that can proportionately prevent the systems from being penetrated.

9.4 Continuous Cyber Attacks: Cyber-attacks are unique and creative by nature; thus, they are a constant process. They keep improving, and the upcoming assault is more sophisticated than the one before it.

9.5 Novel problems: Technology is always changing and rapidly expanding; therefore, new problems are constantly emerging in the IT industry. For instance, several apps today allow users to do transactions or hold chats using voice.

9.6 Covert and asymmetrical conflict: Cyber warfare is covert warfare with the potential for plausible deniability, in contrast to traditional combat, which often results in casualties and face-to-face encounters. This means that governments can continue to claim they were not involved even after being exposed.

10. INDIA'S CURRENT CYBER SECURITY POLICIES

According to **Next IAS (2021),** the Indian government has taken following steps:

10.1 Institutional Framework: India has a well-organized structure to control and strengthen the national information technology systems throughout the country. This comprises the Indian Computer Emergency Response Team and the National Cyber Security Council (CERT-In).

10.2 Prohibition of Apps: Apps that could be dangerous to use by Indian nationals have recently been prohibited in India, most of which are of Chinese origin. The apps allegedly sent data to servers outside of India and lacked the necessary security measures to protect Indian residents' private information from unwanted access.

10.3 Personal Data Protection Bill: To protect individual users' data, the bill requires private organisations to upgrade their data infrastructure. Therefore, rather than limiting data protection to the government alone, a focus is being placed on integrating private companies into its scope.

10.4 Future Cyber Security Strategy: The goal of the Cyber Security Strategy is to create a thorough blueprint for preventing and responding to cyber attacks as well as securing the nation's cyberspace. The strategy, for instance, outlines three stages in the world of cyber attacks:

- **The pre-attack or preparatory phase** is when the systems' holes are found and filled in. To ensure that any potential threat is avoided and the system is not penetrated, the emphasis is on fortifying the defence mechanism, the firewalls, and maintaining system updates.
- **Throughout the Attack:** At the moment of the attack, it's important to stop it as quickly as possible and limit system damage. Additionally, it must be verified that the attack does not destroy important assets and data.
- **Post-Attack Phase:** Focus moves to service restoration once the attackers have been driven from the system so that customers do not experience protracted outages.

11. CONCLUSION

The study's findings indicate that, in order to keep the country safe from various cyberattacks and to remain competitive in the continuously evolving sector of information technology, the current infrastructure needs to be improved more swiftly.

There are various cyber threats in our surroundings that harm society and country in some way or another. At present, malware, spam and phishing, ransomware, distributed denial of service attacks, corporate account takeovers, and ATM cash outs are some of the current cyber threats that are affecting users, organisation’s workings, businesses, public, banking sector, and country's system at large. Everyone is on the verge of being attacked, unknowingly. Cyber threats have adverse effects, as critical information loss has a negative impact on public, safety, economy, banking, power system, health sector, and national security.

Public digital literacy, system vulnerabilities, governmental cyber attacks, technology changes, and covert warfare are major cyber security challenges to the national security of India. The rise in these attacks has highlighted the urgent need to improve India's cyber security. The urgent requirement is to develop a futuristic national cyber-security policy that allots sufficient resources and responds to stakeholder concerns.

12. SUGGESTION

- To reduce these risks, it is important to increase people's general knowledge and digital literacy.
- To create new policies for developing the ability to combat cyber threats and improving the ecosystem.
- The private sector is considered a significant innovator, and their help may be crucial in protecting cyberspace; thus, the government should work with them.

REFERENCES:

Brenner, S.W. (2014).Cybercrime metrics: old wine, new bottles?, *Virginia Journal Oflaw & Technology*, *9*(13), 1-52.

Chertoff, M., & Rosenzweig, P. (2015). "A Primer on Globally Harmonizing Internet Jurisdiction and Regulations".

Commonwealth of Massachusetts. (n.d.). *Know the types of cyber threats*. Commonwealth of Massachusetts Division of Bank. Retrieved December 7, 2022, from https://www.mass.gov/service-details/know-the-types-of-.cyber-threats.

Drishti IAS. (2022, September 3). *India's Cyber Ecosystem.* https://www.drishtiias.com/dailyupdates/daily-news-editorials/indias-cyber ecosystem#:~:text=According%20to%20the%20National%20Crime,from%202019%20(44%2C735%20cases).

Drishti IAS. (2022, April 18). National Cyber Security Strategy. https://www.drishtiias.com/daily-updates/daily-news-analysis/national-cyber-security-strategy-1#:~:text=In%202020%2C%20the%20National%20Cyber,and%20vibrant%20cyberspace%20for%20India.

Emeritus. (2022, June 30). *Different Types of Cyber Security Threats & Attacks*. https://emeritus.org/in/learn/different-types-of-cyber-security-threats/

Kumar, D. (2016). Cyber Security : Status and Imperatives. In G. Kanwal (Ed.), *The New Arthashastra : A Security Strategy For India* (pp.268-286).HarperCollins Publishers

Naha, A. (2022). Emerging Cyber Security Threats : India's Concerns and Options. *International Journal of Politics and Security (IJPS),* 4(1), 170-200. DOI:10.53451/ijps.996755.(13/11/22) Patel, K., & Chudasama, D. (2021). National Security Threats in Cyberspace. *National Journal of Cyber Security Law*. 4(1), 12–20.

National Institute of Standards and Technology. (2011, August). *Cyber Threat*. https://csrc.nist.gov/glossary/term/cyber_threat#:~:text=1%20under%20Threat-

,Any%20circumstance%20or%20event%20with%20the%20potential%20to%20adversely%20impact,and%2For%20denial%20of%20service.

Next IAS. (2021, March 10). *Cyber Security*. https://www.nextias.com/news/cyber-security.

Next IAS. (2022, April 18). *Status of India's National Cyber Security Strategy.* https://www.nextias.com/current-affairs/18-04-2022/status-of-indias-national-cyber-security-strategy#:~:text=Budgetary%20provisions%3A,should%20be%20earmarked%20for%20cybersecurity.(20/11/22)

Slyke, S.V., & Benson, M.L. (2016). The Oxford Handbook of White Collar Crime. Oxford University Press,

The growing cyber threat to India from Far East. (2022, August 12). *The Economic Times* https://economictimes.indiatimes.com/news/india/the-growing-cyber-threat-to-india-from-far-east/articleshow/93513855.cms?from=mdr

The University of Arkansas, Little Rock (n. d.). Threat Assessment Team - University Police. Retrieved December 8, 2022, from https://ualr.edu/safety/home/emergency-management-plan/threat-assessment-team/

What Does Cyberspace Mean? (2022, May 30). techopedia.com. https://www.techopedia.com/definition/2493/cyberspace

What is Cyber Security? (n.d.). https://www.itgovernance.co.uk/what-is-cybersecurity