Volume 20, May 2022 ISSN 2581-5504

"An evolving concern for National Cyber Security in India"

***Shubham Patkar**
UPES, Dehradun

****Anjali Dhakad**
Symbiosis Law School, Nagpur

ABSTRACT

In the Information, Communication, and Technology (ICT) age, cybersecurity has evolved into a complex and rapidly security concern (ICT). As the world's reliance on ICT grows, cyberthreats to seem likely to infiltrate every nook and cranny of national economies and facilities; undoubtedly, the growing reliance on computers and Internet-based networking has been associated with increases in cyberattack occurrences specific people, businesses, and governments around the world. Meanwhile, some countries are increasingly viewing ICT as either a strategic partner to be harnessed for national security and a battlefield on which strategic wars might be fought. This study investigates the importance of cybersecurity in today's security discussion, focusing on the area of cybersecurity first from standpoint of India. In the context of the information, communication, and technology revolutions, cyber security has evolved as the cornerstone of a linked world. Within the scope of this transformation, the united nations came face to face with the new cyber world, where opportunities, such as connectivity, as well as challenges, are becoming increasingly important. As a result, the globe is witnessing a variety of hazards and perils that have never been seen before in history, and India is no exception. In addition, in today's world, the present risks to the global security environment arise from technology progress and are not limited to local sources, but rather extend to include worldwide networks. Such perils exist beyond the confines of time and place, posing a constant and universal threat. As a result, inter-state interactions are drowning in securing economic and security risks while putting severe restrictions on the online world. Furthermore, cyber-attacks have the capacity to compel states into actual acts of aggression, because the cyber realm has no power balance. In this context, the article aims to investigate the regions of cyber security outside of conventional security conceptions, and to place India at the forefront of the research, taking different countries' responses into account. In addition, an effort is made to detect problems and possible diagnoses.

Keywords: India, Cyber security, Internet based Networking, United Nation, ICT Grows, Threats,

Volume 20, May 2022 ISSN 2581-5504

INTRODUCTION

Security is a crucial term in the theory of international relations. Recently, security analysis was primarily concerned with state security, considering it as a function of the degree of dangers that states confront from those other states, and the method and efficacy with which states respond to so challenges (Rather and Jose 2014). However, following the Cold War's end, researchers switched their focus away from the state-centric conception of security, broadening the term to include individual safety (Buzan 1991). [1]In the same period, the nature of threats shifted from external attacks to intra-state conflicts caused by wars, environmental degradation, financial suffering, and human rights violations. In this setting, national security developed to encompass challenges other than territory security, including such as poverty, industrial competitiveness, educational crises, environmental risks, drug and people trafficking, and resource scarcity. Finally, the modern Information, Communication, and Technologies (ICT) revolution — which includes the Web, email, social media, and satellite links — has transformed every area of human existence, bringing new threats to national security.

Nevertheless, in the digital world, public safety is confronted with hitherto threats intended to destroy a state's technological infrastructure.[2] It is an evident fact that the Internet and ICT Infrastructure are critical for economic and social progress in a globalized world, which constitutes a digital key infrastructure on which societies, businesses, or governments rely to execute their basic duties. The Internet's largely open nature ensures that it is a dangerous environment on multiple levels (Pilli 2012). As a result, cyber security has come to cover a wide range of challenges, including cyber security, cyber terrorism, cyber threats, privacy concerns, cybercrime, and cyber warfare.

Cyber threats are emerging and increasing at a rapid pace inside the first years of the twenty century.[3] They are still begun by criminal actors, but they are also initiated by new sources, such as international states and political organizations, and may have goals other than monetary gain. The complexity of cybercriminals, the emergence of cyber espionage, and the well reported actions of hacker collectives have all contributed to the idea that attacks are becoming more coordinated and sophisticated, with unmistakable signs of formalization.

[1]Cavelty, M. D. (2012). "The Militarisation of Cyber Security as a Source of Global Tension." In Mockli, Daniel, Wenger, and Andreas, eds. *Strategic Trends Analysis*. Zurich: Center for Security Studies.

[2]Buzan, B. (1991). *People, States, and Fear: An Agenda for International Security Studies in the Post Cold War Era*. London: Harvester Wheatsheaf.

[3] DSCI. (2013). *Analysis of National Cyber Security Policy (NCSP–2013)*. New Delhi: Data Security Council of India.

[4]. http://www.dot.gov.in/sites/default/files/NTP-06.06.2012-final_0.pdf.

Volume 20, May 2022 ISSN 2581-5504

Given this context, states have increasingly identified cyber security as a priority security issue, which will certainly grow in importance over time.[4] Simultaneously, cyber security has arisen as a national policy issue that must be tackled holistically, taking into account socioeconomic, economic, cultural, legal, legislation, technical, diplomatic, military, and intelligence-related factors. "Sovereignty considerations" have grown in importance.

TERM AS WELL AS CONDITIONS RELATED TO CYBER SECURITY

Because most government and banking institutions, military organizations, corporations, healthcare facilities, and other business owners store and process a large confidentiality of sensitive information on computers, internet backbone outages, virus attacks, data conferred by hackers, as well as other occurrences affect our lives in a variety of ways ranging from inconvenient to life-threatening.[5] As a consequence of the rise volume & complexity of attacks, there is a greater need to secure private information and sensitive corporate information, as well as to protect national security.

As a consequence, "cyber security" refers to a collection of tools, rules, regulations, training, activities, and identified the concept and protections, risk management approaches, assurance, and technology that can be utilized to protect and secure the cyber environment as well as organizational and user assets (ITU 2009).[6] Furthermore, cyber security strives to secure information systems and focuses on safeguarding computer programmes, networks, and data, as well as preventing unauthorized users from accessing information and preventing unintentional change or intended/unintended destruction.[7]

In particular, cyber security is critical to the continuous development of technology including Internet services State economic and security well-being are becoming increasingly dependent on the successful safeguarding of crucial information infrastructures. As a result, keeping the Internet as safe as possible is a fundamental part of the creation of government policies as well as new services in many nations. The remainder of this article discusses the extent toward which India has dealt successfully with this emerging dilemma to yet.

BACKGROUND RELATED TO CYBERSECURITY IN INDIA

In the Indian context, officials have paid comparatively little attention to cyber security, to the point where the government is unable to address the country's rising demand for a powerful cyber security infrastructure.[8] In brief, India lacks strong offensively and defensively cyber

[5]IDSA. (2012). *India's Cyber Security Challenges*. New Delhi: Institute of Defence Studies and Analyses.
[6]KPMG. (2010). *Indian Defence Sector: The Improving Landscape for US Business and Indo-US Commercial*, KPMG International, Swiss.
[7]Human Security: Evolution and Conceptualization." *European Academic Research*, 2 (5): 6766–6797.
[8]*Cyber Threats to Mobile Phones*. United State: US Department of Homeland Security.

Volume 20, May 2022 ISSN 2581-5504

security capabilities, which is aggravated by a lack of access to critical mechanisms for dealing with complex malware such as Iran, Flame, and Black Shades.[9]

Furthermore, as compared to other developed countries, India has considerably less cyber security projects and activities. Many of the key projects planned by the Indian government have merely been offered on paper. Furthermore, approved projects such as India's National Important Info Critical Infrastructure Agency (NCIPC) or National Cyber Coordination Centre (NCCC) have yet to materialize. Worse, India's 2013 National Cyber Policy has failed to provide positive outcomes, as its execution appears to be lacking in a variety of areas, including privacy violations in general and encroachment into civil rights in particular.

At same time, India confronts a significant need to secure important infrastructure from cyber-attacks, such as institutions, observatories, computerized power grids, or thermal power plants 2014).[10] The Indian government recognizes a significant increase in cyber-attacks targeting institutions such as the financial and banking services sectors. Malicious Internet sector of India has ranged from viruses to hacking, identity theft, spamming, email-bombing, online defacement, cyber defamation, and denial of service.

If For example, despite ranking 85th in the world in terms of internet connectivity, the country ranks under seventh in terms of cyber-attacks In 2013, cyber security threats and attacks on government institutions increased by 136%,[11] while efforts targeting Indian financial services businesses increased by 126%. Approximately 69 percent of attacks targeted large corporations. Finally, per a Symantec research, four out of every ten assaults in 2014 targeted nontraditional service industries such as business, hotel, and personal care (Indo-Asian News Service 2014). As a result, there is an obvious need for India to build an efficient cyber crisis management plan in order to tackle these and other difficulties.

CYBER SECURITY IN INDIA: IN-DEPTH

The Indian IT industry has developed as one of the most important drivers of the country's economic growth, as well as an essential component of the country's business and governance.[12] The industry has a positive impact on the lives of Indian inhabitants by directly or indirectly contributing to the improvement of numerous socioeconomic factors such as living standards, employment, and diversity. Furthermore, information technology has played a critical part in

[9]Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization: Cyberterrorism, Information Warfare, and Internet Immobilization. IGI Global.

[10] Analyses and Discussions of the Blackout in Indian Power Grid." *Energy Science and Technology* 6 (1): 61–66.

[11] Spy Game: India Readies Cyber Army to Hack into Hostile Nations Computer Systems." *Economic Times*, New Delhi, August 6.

[12]Cyber Security Plan to Cover Strategic, Military, Government and Business Assets." *The Hindu*, New Delhi,July 2

Volume 20, May 2022 ISSN 2581-5504

transforming India into a worldwide leader in the provision of business solutions and also world-class technology solutions.

Simultaneously, the expansion of the IT sector has indeed been associated with a substantial and growing demand to safeguard the compute cluster, and the requirement to instill enough trust and confidence in this sector.[13] For example, often these financial institutions and the financial sector have incorporated IT into their operations, opening up countless growth opportunities while also making these institutions susceptible to hacking attacks in their daily operations and making the apparent lack of strategies to deal with all these kinds of threats particularly concerning.

The government, for its part, has facilitated greater adoption of IT-enabled services and programme, such as the Unique Registration Development Board of India (Study . the research design) and Nat'l e-Governance Programs (NeGP), by building a massive IT infrastructure and encouraging corporate participation. Critical sectors such as defense, banking, energy, telecommunications, transportation, and other public agencies rely significantly on computer systems to transmit data for business operations and a source of communication and information. To date, the administration has ambitious goals to expand e commerce operations, cyber connectivity, and overall IT use in communications.[14] In this context, Indian Prime Minister Narendra Modi's declaration that "the cabinet has approved the ambitious 'Digital India' initiative that aims to connect all local government areas via broadband internet, promote e-governance, and turn India into a connected knowledge economy" is typical .

Notably, greater reliance on IT has left the systems that serve India's key military and intelligence communities vulnerable to intrusions.[15] Indeed, assaults on government equipment enhance the risk of the theft of military and state secret. Unsurprisingly, several organizations under the purview of the Indian Defense ministry have taken on the task of dealing with cyber security. For example, the Indian Army established the Digital Security Establishment in 2005 to protect the army's systems at the division level and to undertake safe cyber security audits. In addition, the army created a cybercrime laboratory at the Military Academy of Telecommunication Engineering in Madhya in 2010 with the goal of providing officers with specialized training in security procedures for its signal and data transmission networks.

The Indian Minister of Communications Technology has released a draught National Cyber security Policy in March 2011, with an emphasis on critical infrastructure security and protection, development activities, and public-private collaborations. Under the aegis of the Security Council, a proposal to establish the National Important Info Infrastructure Protection

[13] ECIL Website Hacked, Sensitive Data Leaked." New Delhi, August 2

[14] *The Cyber Index: International Security Trends and Realities*. New York and Geneva: United Nations Institute for Disarmament Research.

[15] *The Cyber Index: International Security Trends and Realities*. New York and Geneva: United Nations Institute for Disarmament Research.

Volume 20, May 2022 ISSN 2581-5504

Centre in accordance with the draught policy was established in June 2012. The goal was to secure the state's essential infrastructure in collaboration with national and enterprise Computerized Emergency Services (CERTs) (Joseph 2012). In May of the same year, the Defiance Research and Development Organization built an indigenous cyber defense system to safeguard the safety and security of network sectors.

Energy and cyber security

In India, the security of energy industry has been emerged as a significant non-traditional security problem. The country is ranked 4th in term of primary energy demand; yet, average capita consumption is quite low. Data on attacks and device weaknesses inside the Indian energy industry is almost non-existent due to weak regulations of sharing of information and insufficient organizations to promote it. However, based on international cyber security trends, we may assume that the sector is increasingly being targeted by advanced attacks, especially as India has begun to link it with contemporary technologies in order to fulfill expanding energy needs.

Nevertheless, with the introduction of new technology in this industry, a slew of new issues emerged. For example, following India's nuclear test since May 1998, a gang of hackers placed in anti-India and the anti-nuclear remarks on the Bhabha Atomic Research Center (BARC) website.[16] Furthermore, an internet hacker known as Electronic health records (ehrs OzenMyst attacked BARC's official website and exposed some of its sensitive material as a demonstration against ongoing government activities in the occupied area of Kashmir. Moreover, the key infrastructure that underpins all economic growth in India is entirely dependent on the electricity industry; this sector's reliance on ICT has highlighted a number of cyber security challenges. It is believed that between 1994 and 2004, over 60% of all cyber attacks against India's autonomous power systems occurred. [17]Most recent times, on July 30 and 31, 2012, northern India saw a significant blackout that disrupted about 670 million people's everyday life and work, causing damage to all regional services, notably road traffic and trains. Concurrently, there have been reports of deadly fires or explosions in major refineries, resulting in significant losses of life, all the while pipelines ruptured and oil flow was blocked.

Defense and cyber security

India has a substantial military industrial base and the world's third-largest armed forces. At the same moment, it has connected its defense sector to modern technologies, exposing the country to a slew of ever-changing threats as a result of its reliance on such technologies and reliance on integrated networks. In 2012, for example, hackers attempted an assault on the Indian Navy's

[16] India's Electrical Smart Grid: Institutional and Regulatory Cybersecurity Challenges." Seattle:Henry M. Jackson School of International Studies.

[17] *The Cyber Index: International Security Trends and Realities*. New York and Geneva: United Nations Institute for Disarmament Research. . and A. K. Sharma. (2014).

Volume 20, May 2022 ISSN 2581-5504

eastern command computer systems, that supervise the testing of India's attack submarines and maritime actions in the China Sea. The navy computers were attacked with a malware that stealthily captured and transmitted critical papers and files to Chinese IP addresses.

Although Indian officials have still yet to reveal the nature of the material targeted in this attack, the Naval may not be the only Indian defense institution to have been subjected to such occurrences; the Nsa (NSA) as well as the Air Force have also proven to be vulnerable. In 2010, hackers targeted the NSA's headquarters and several computers of the Indian Air Force, allowing confidential files and documents to be stolen through a series of small windows. In that year, the country saw its largest cyber attack to date, in which more over 10,000 email accounts of high government officials, mostly military leaders, the Prime Minister's Office (PMO), military, home ministry, external affairs, among intelligence agencies, were compromised.

Challenges to the Indian military are typically posed by actors with political, economic, or quasi-political goals, with a negative impact on national security, public safety, or economic well-being. As a consequence, there is a need to create a cyber defense environment in order to secure the military sector's technology and capabilities in real time while also offering protection and incident response. In this regard, V. K. Saraswat, former Director-General of India's Defense Research and Development organization (DRDO), stated that "the DRDO, in collaboration with some premier institutions, is developing India's own Computer System as a response to a growing concern over cyber attacks, as we are primarily dependent on operating systems today."

Finance and cyber security

India has one of the world's fastest expanding economies, with IT adoption serving as a driving force behind this rapid expansion. However, growing reliance on IT has resulted in new vulnerabilities. Most cyberattacks, it has been alleged, are motivated by financial or financial gain. Moreover, the sheer complexity banking and financial exposes them to assaults from both state and non-state actors. The interconnected advent of contemporary technologies has aggravated the situation by opening up new avenues for deception, extortion, as well as other forms of abuse. Acknowledging this, previous Indian Telecom Minister Kapil Sibal stated, "cyber security is vital for economic stability, and any failure to secure cyber security will result in economic destabilization."

In recent years, the Indian financial sector has seen an increase in network security vulnerabilities, data leakage, identity fraud, information larceny, as well as other fair skinned crime, leading the financial sector to face massive losses far exceeding traditional methods of bank robbery. Financial damages from certain attacks had climbed by 30% a year later. It is also predicted that India ranks in the top five countries in the world in terms of the prevalence of crime including such identity theft, ransomware, and phishing. Furthermore, the Reserve Bank (RBI) has issued information on commercial banks that are being targeted for fraud, including

through online banking and Atms (debit/credit) cards. The amount of such instances increased from 4,049 lakh in 2010, - 5267 lakhs in 2012. In these conditions, it is self-evident that India must adopt a comprehensive cybersecurity policy to completely defend the banking industry.

Telecommunications and cyber security

Telecommunication has emerged as a critical engine of India's social and economic development. Today, India is regarded as one of the world's fastest expanding telecom markets, with the amount of telephone connections reaching 943 million in February 2012. In same month, the nation had 911 million mobile connections and almost 160 million Daily users, about half of them were on social media.[18] Apparently Indian government has indicated its intention provide the 600 million broadband services by 2020, as well as achieve 100 percent tele - density.

Around the same time, this sector's rapid rise has indeed been followed by a slew of cyberthreats. Due to the rising frequency of cyber scams, it is stated that information poses the greatest risk to the telecommunications sector. For example, on August 7, 2013, hackers infiltrated India's Bharat Sanchar Nigam Limited (BSNL) database and placed malware in the systems. On October 12, the same year, the BSNL Corporate Domain was hacked again, and some sensitive information was stolen. Meanwhile, on June 9, 2013, some unknown hackers used DDoS to enter the Mahanagar Telephone Nigam Limited (MTNL) website; the goal of the attack was to fight Internet restrictions purportedly sponsored by the MTNL

.Yet, on a more personal level, cell phones are being used to store various such as email, contact details, and passwords, as well as other potentially risky activities. Recent advancements in mobile business have enabled users to conduct money transactions over the phone, perform point-of-sale payments, and even pay at cash registers using smart phone applications such as Paytm, MobiKwik, and many others. Such open and profitable networks are now becoming increasingly vulnerable targets for cyber-attacks. As of 2014, roughly 7.9 % of portable devices had been targeted, and the country placed second on the list of such device cyberattacks.

CONCLUSION

As the previous pages demonstrate, cyberattacks on India's important information infrastructures, such as electricity, financial services, military, and telecommunications, have the potential to harm the economic growth and public safety. From the viewpoint of national security, securing essential information infrastructure has become a primary concern, mirroring regulations already implemented by other digital nations. Indeed, the increasing interconnection of the digital domain across borders has resulted in the creation of cybersecurity as a critical part of national

[18] *The Cyber Index: International Security Trends and Realities*. New York and Geneva: United Nations Institute for Disarmament Research.

Volume 20, May 2022 ISSN 2581-5504

security strategy other states throughout the world. India should never be slow to follow their lead.

REFERENCES

- Aiyengar, S. R. R. (2010). National Strategy for Cyberspace Security. New Delhi: KW Publisher.
- Athavale, D. (2014). "Cyberattacks on the Rise in India." The Times of India, Pune, March 10.
- Bamrara, A., G. Singh and M. Bhatt (2013). "Cyber Attacks and Defence Strategies in India: An Empirical Assessment of the Banking Sector." International Journal of Cyber Criminology, 7 (1): 49–61.
- Dilipraj, E. (2013). "India's Cyber Security 2013: A Review." Centre for Air Power Studies, 97 (14): 1–4
- Gercke. (2009). Understanding Cybercrime: A Guide for Developing Countries, Geneva: ITU publication
- Government of India. (2012). "National Telecom Policy (NTP) – 2012." Ministry of Communication and Information Technology (NTP). New Delhi, June 13.
- Jain, S. (2014). Cyber Security: A Sine Qua Non.
- Joseph, J. (2012). "India to Add Muscle to Its Cyber Arsenal." Times of India, New Delhi, June 11
- Kaushik, R. K. (2014). "Cyber Security Needs Urgent Attention of Indian Government.
- Madaan, N. (2013). "More in City Fall in Net Trap." Times of India, Pune, September 8
- OECD. (2012). "Cybersecurity Policy Making at a Turning Point."