Journal of Technology Innovations and Energy
https://doi.org/10.56556/jtie.v1i2.201
ISSN: 2957-8809

RESEARCH ARTICLE

Emerging Cyber Security India's Concern and Threats

Aadil Ahmad Shairgojri[1*], Showkat Ahmad Dar[2]

[1]Research scholars of Political Science & public administration Annamalai University Tamil Nadu, India

Corresponding Author: Aadil Ahmad Shairgojri, aadilhassan1995@gmail.com
Received: 08 April, 2022, Accepted: 13 June , 2022, Published: 18 June, 2022

Abstract
Cybersecurity has developed into a challenging and constantly changing security issue in today's information, communication, and technology-driven world (ICT). Cyberattacks are expected to grow more widespread as the global economy and infrastructure become more dependent on information and communications technology (ICT). As a result of a growing reliance on computers and the Internet, there has been an increase in cyber attacks globally. The main targets of these attacks have all been people, organisations, and governments. Information and communication technologies (ICTs) are increasingly viewed by some countries as a battlefield where strategic warfare should be fought, even as a strategic asset to be leveraged for national security. This is essential because the national security is at risk. The significance of cybersecurity in the ongoing discussion about security concerns is examined in this essay. The authors examine cybersecurity from the viewpoint of India in order to gain a better knowledge of it.

Keywords: Cyber Security; Threats; ICT; Infrastructure and Framework etc

Introduction

In international relations, security is a major concern. It was previously thought that threats from foreign states and government responses to those threats were responsible for state security. A shift in focus from state-centric security to personal security occurred after the end of the Cold War. The fear of external aggression has given way to the threat of internal conflict as a result of civil wars, environmental degradation, economic hardship, and human rights violations. This definition of national security encompasses challenges like resource scarcity, industrial competitiveness, educational crises, environmental risks, drug and human trafficking, and poverty as well as defence of the homeland. From email to social networking to satellite communications to the Internet, everything about human life has changed. This has led to new national security problems, which we will discuss below.

In the digital age, a state's technology infrastructure is exposed to challenges to national security. As a critical piece of digital infrastructure for governments, businesses, and society as a whole in today's globalised world, the internet and other ICTs are necessary for social and economic progress. Because of its inherent openness, the Internet carries a high level of danger. Defending critical infrastructure from cyberattacks is just one aspect of cybersecurity, which also include dangers like cyberterrorism, data breach, and other forms of cybercrime and terrorism.

Cyberthreats are on the rise in the 21st century. Despite the fact that foreign governments and political organisations with a variety of goals are increasingly using this technique. It is still a criminal enterprise. Stuxnet, political "hacktivism," destabilising activities, and military operations are all examples of cyber espionage, sabotage, and destabilisation (OECD 2012). It appears as if cyberattacks are getting more planned and professional due to the increasing sophistication of cybercriminals, the rise of cyber espionage, and the operations of hacker collectives. States are now aware that cybercrime is a significant security concern to the country. Cybersecurity is currently a national policy issue that touches on the economy, society, education, legislation, law enforcement, technology, diplomacy, military, and intelligence, among other things. The concept of "sovereignty" is gaining in importance (OECD 2012).

The vast majority of political and financial organisations, military organisations, businesses, hospitals, and other industries store and process a great deal of sensitive information on computers, making network outages, virus infections, and hacker data disastrous. As cyberattacks become more common and sophisticated, the need to secure private information, sensitive commercial information, and national security grows. 3 In order to safeguard and secure the cyber environment and the assets of the organisation and its users, a number of tools, regulations, guidelines, training, activities, security concepts, and protections, risk management techniques, assurance, and technology are employed (ITU 2009). By protecting computer programmes, networks, and data, cybersecurity strives to keep information technology safe from unauthorised access and unforeseen damage or

destruction. Cybersecurity is essential to the development of IT and Internet services (UNODA 2011). National security and economic development depend on the protection of critical information infrastructures. Safeguarding the Internet is now a standard prerequisite for new services and government policy in many nations. Against the backdrop of this new threat, we examine India's response.

Research Objectives

Cybersecurity is crucial since it guards against theft and destruction to many types of data. It is a collection of tools, procedures, and techniques created to safeguard programmes, networks, and systems. As digital technology advances, the number of devices and users rises, the global supply chain becomes more complicated, and data becomes more vital in the digital economy, the system in the cyber space has become susceptible and will continue to be so as attacks increase in number. After conducting a thorough examination of the literature, the paper sets out to examine the crucial areas that are vulnerable to cyberattacks and to highlight the difficulties involved. Additionally, the paper illustrates India's cyber security strategies.

Material and method

The majority of the content in this research paper comes from secondary sources, such as articles, books, and official documents that were acquired from the official portals of the Indian government. The facts and relationship have been rigorously examined and explained using an empirical methodology. Qualitative information was acquired and utilised to arrive at a fair conclusion. Direct methods, such as scientific observation and expert interviewing, have also been utilised for this research project. Empiricism, observation, critical analysis, and exploratory approaches have been highlighted in order to contextualise the study's topic. These methods have added fresh, logical information to the body of literature that is supported by empirical data.

Discussion and results

Cybersecurity in India: Background

As a result of their neglect of cybersecurity, India's authorities are unable to meet the country's expanding demands. Anti-malware programmes like Stuxnet, Flame, and Black Shades make India's lack of cybersecurity capabilities even worse. India has fewer cybersecurity projects than other developed countries. In India, a lot of government initiatives are still just on paper. Two approved projects, the National Critical Information Infrastructure Protection Center (NCIPC) and the National Cyber Coordination Centre (NCCC), have not been carried out to their full potential. Adding insult to injury, India's 2013 National Cyber Security Policy has not been properly implemented, resulting in invasions of privacy and human rights abuses.

India must safeguard not only its financial institutions but also its satellites, automated power grids, and nuclear power facilities from cyberattacks. The Indian government has acknowledged the rise in cyberattacks on financial institutions. Cybercrime in India can take many forms, from viruses to hacking to identity theft to spamming to email bombing to website destruction to cyberdefamation. Internet access in the country is ranked 85th, yet cyberattacks are placed 7th (Express News Service 2014). There were 62,000 cyberattacks in the middle of 2014, up from 23 in 2004. Security threats to government organisations rose by 136 percent in 2013, while those to Indian financial services corporations rose by 126%. 69 percent of all assaults target large organisations of some kind (IANS 2014). According to Symantec, four out of every five attacks in 2014 were aimed at commercial, hotel, and personal services. India requires a cybercrisis management strategy to address these and other issues.

Cyber Security in India: In-Depth

India's IT sector has developed to play a key part in the country's economy and governance. Living standards, job prospects, and cultural diversity are all enhanced in some way as a result of the industry's presence among Indians. Thanks to information technology, India is emerging as a prominent participant in commercial services and technological solutions. There is a growing need to protect the digital environment and enhance the sector as a result of the advent of technology (DEITY 2012). Having included IT into their operations, the vast majority of financial institutions and banks are now vulnerable to cyberattacks as a result of routine business processes. Having no mechanisms in place to deal with these concerns is worrying. For example, the UIDAI and NeGP programmes have been promoted by the government, which has also built out a substantial IT infrastructure and increased industry involvement. In the public sectors of defence, banking, energy, telecommunications, and transportation, computer networks are essential for commercial transactions, information sharing, and communication. Computer networks. Advances in telecommunications, online and e-commerce are high priorities for the government. Indian Prime Minister Narendra Modi's claim that the "Digital India" plan, which aims to connect every gram panchayats to broadband internet, boost e-governance, and transform India into a connected knowledge economy, has been approved by the cabinet is typical. A high level of safety. Since Indian military and intelligence agencies are increasingly reliant on IT, they are more vulnerable to cyberattacks. In the event of an attack on government infrastructure, military and government secrets could be taken.. As a result, the Indian Ministry of Defense has delegated responsibility for cyber defence to a slew of organisations. The Indian Army's Cyber Security Establishment was founded in 2005 to protect divisional

networks and conduct cybersecurity audits. The Military College of Telecommunications Engineering in Madhya Pradesh now has a cybersecurity lab for officers to learn about signal and data transmission network security. In March 2011, India's Ministry of Communications and Information Technology (MCIT) drafted a national cybersecurity policy that prioritised infrastructure, development, and public-private partnerships (DEITY 2012). In June of that year, the National Security Council decided to establish the National Center for the Protection of Critical Information Infrastructure. National Technical Research Organisation (NTRO) The state's critical infrastructure was to be safeguarded through the use of CERTs at the national and sectoral levels (CERTs). In May of that year, the Defense Research and Development Organization developed a national cyber defence system to protect network sectors. Project completion reached a half-way point in May 2012. United Nations Development Program (UNIDIR). The Technical Intelligence Communication Centre and the National Defense Intelligence Agency developed a joint team to raise public awareness of cyber vulnerabilities.

Energy and Cybersecurity

India's non-traditional security challenge is the safety of the country's energy sector. The country is fourth in the globe despite its low energy use per person (TERI 2013). Information about cyberattacks and equipment vulnerabilities in the Indian energy sector is scarce because of inadequate regulation and governance. As India ties itself to contemporary technology to address its expanding energy needs, the industry is becoming a target of increasingly sophisticated attacks. A variety of cybersecurity concerns for India's critical infrastructure have surfaced as a result of the power sector's reliance on ICT. 60 percent of all cyberattacks on India's power grid occurred between 1994 and 2004. (2013) The 30th and 31st of July, 2012, saw a huge blackout in Northern India that affected 670 million people and slowed down train and road travel. Traffic lights and related equipment failed, and police were unable to maintain control of the situation. A number of large refineries were damaged by flames and explosions, resulting in numerous deaths, while oil supply was impeded by pipeline breaks (IDSA 2012).

Defence and Cybersecurity

India's armed forces rank third in the world, and the country's defence industry is robust (KPMG 2010). As a result of its reliance on modern technologies and network integration in its defence industry, it has put the country in danger. In 2012, hackers targeted the eastern command computer systems of the Indian Navy, which control missile submarine tests and maritime action in the South China Sea. Infected navy computers sent sensitive documents and data to Chinese IP addresses. In addition to the NSA and Air Force, Indian officials have not said what data was accessed. The NSA and other computers used by the Indian Air Force were breached by hackers in 2010 and 2012, allowing private information and papers to be accessed. Military personnel, the PMO, the defence, home, and external affairs departments, as well as intelligence organisations were all targeted in the same year. Politically aspirant actors endanger India's defence industry, putting national security, public safety, and the country's economy in jeopardy. Real-time cyber defence is necessary to protect the advancements and capabilities of the defence industry (DEITY 2011). "The DRDO is building India's own operating system in partnership with several top institutions in response to 8 the growing concern over cyberattacks as we are mostly dependent on operating systems," said former DRDO director-general V. K. Saraswat.

Finance and Cybersecurity

India's economy is growing at one of the fastest rates in the world because of its reliance on information technology. New concerns have been introduced because of the increased reliance on technology. According to statistics, the majority of hackers are motivated by financial gain (KPMG 2014). In modern banking and financial services, both state-sponsored and non-state assaults are possible since they are so complicated. Fraud, theft, and other wrongdoings have become easier to commit as a result of the modern technology's link (Bamrara et al. 2013). According to former Indian Telecom Minister Kapil Sibal, "Cybersecurity is vital for economic security and failing to ensure it will lead to economic destabilisation. India's financial sector has seen an upsurge in network security breaches, data loss, and other white-collar crimes, putting the banking industry at danger of large losses. In 2013, over $4 billion was lost by Indian firms as a result of cyberattacks. A year later, the cost of such assaults had risen by 30%. Among India's top five cybercrimes are identity theft (11%), ransomware (11%), and phishing (9 percent). Also, the RBI has released data on how commercial banks are targeted for fraud, such as through Internet banking and ATM (debit/credit) cards. In 2010, there were 4,049 million cases, which grew to 5,267 million cases in 2012. India needs a comprehensive cybersecurity policy to protect its banking sector under these circumstances.

Telecommunications and Cybersecurity

Telecommunications have fuelled India's economic and social growth. Indians have 943 million phone lines as of February 2012. In the same month, 9 911 million mobile phone connections and 160 million Internet users—of whom half used social media—were registered. India is expected to have 600 million internet connections by 2020. Cyberattacks have accompanied this industry's rapid expansion. Some argue that cybercrime is the greatest danger to the telecom industry. As of August 7, 2013, BSNL's database was infiltrated with spyware by hackers. On the 12th of October, BSNL's Office Domain suffered a significant data breach (Dilipraj 2014). A DDoS attack on MTNL's website was launched by unidentified hackers

on June 9, 2013, in an attempt to bypass Internet filtering. Referring to Reddy (2012): Passwords, emails, and other contact information are all stored separately on mobile phones. Consumers can now use Paytm, MobiKwik, and other point-of-sale payment methods, thanks to recent advancements in mobile commerce." Networks that are open and profitable are more vulnerable (Ruggiero and Foote 2011). In 2014, 7.9 percent of mobile devices were infected, which ranked the United States in second place in the world.

Cyber security in India issues and challenges

The protection of computer systems and electronic devices from malevolent cyberattacks, opportunist malware, and the unintended installation of malware by users themselves is what we mean when we talk about cyber-security. The breadth of cyberthreats is constantly expanding on a global scale. In the modern world, attempts are made yearly to divulge information for political or financial gain by hacking data and/or sensitive, private, or classified records. India's population comes from a diverse spectrum of social and economic origins. Depending on their financial situation, people employ a variety of technology, from expensive, highly secure electronic gadgets to low-cost mobile phones. This makes it difficult to establish a single set of legislative and technological standards controlling data protection. Additionally, there is a low level of digital literacy and familiarity among the general populace. Governments, companies, and individuals are all concerned about cyber security, which is becoming more and more of a problem. Maintaining the security of our personal data has become a top priority as more and more aspects of our life are being captured online, including our credit card details, vacation journals, and cute kitten videos. Ransomware, phishing, virus attacks, and other dangers are only a few of the many that exist for cyber security. With 2,299,682 instances of local cyberattacks already in Q1 2020, India is placed 11th globally.

Cyber attacks and India's response

In order to reach a $5 trillion economy, it is rumoured that the Indian government will announce its cybersecurity strategy policy in January 2020. A recent analysis by Recorded Future, a U.S. business that studies worldwide cyber threats, detailed RedEcho's attack on India's power infrastructure. From the middle of 2020 onward, ten organisations in the power industry and two Indian seaports were planned as targets. At an SKOCH event, Rajesh Pant, the national cybersecurity coordinator for India, said: "India's cybersecurity strategy policy would enable the government to secure all of India." This endeavour will help the government achieve its $5 trillion economic growth goal. Few efforts have been made to advance the Indian economy. In September 2020, Minister Sanjay Dhotre will inform the legislature that ZTE and Huawei provide the mobile network equipment for BSNL. Huawei was being looked at in 2014 over allegations that it had hacked BSNL. In this sense, the electric power industry is akin to other sectors of the economy. China supplied 21,000 crore of the 71,000 crore worth of power sector equipment that India imported in 2018–19. The government has taken major decisions since the year's beginning. Indian businesses would need government authorisation to import Chinese power supply equipment from July 2020. Before using any equipment other than approved equipment for network updates, telecom businesses must obtain Department of Telecommunications approval.

In order to strengthen our cyberdefenses and safeguard us against cyberattacks, a deterrence plan must be put into place. Some claim it's difficult to prevent cyberattacks. The United States is under attack from China, Russia, Iran, and North Korea despite having the strongest military and cyber capabilities in the world. We have nuclear and conventional deterrence because we are aware of the capabilities and financial burden of our enemies. Cyberwarfare's precise nature is yet uncertain. It is challenging to link cyberattacks to a state actor since we have no way of knowing what the other side is capable of. Deterrence will therefore be challenging to implement. According to a Business Standard analysis, one of the nation's most frequently targeted by cyberattacks in 2021 would be India. It was anticipated that every year, the number of cyberattacks will rise by a factor of two. India is expected to see 1.16 million cyber breaches in 2020, a threefold increase over 2019. This prediction is made by the Computer Emergency Response Team (CERT). 2021 and 2022 are expected to see more breaches. As of June 2021, official sources had identified 6,07,220 cybersecurity weaknesses in total. Is this a condition that the Indian government is aware of? The amount of money spent on cybersecurity is the subject of a wealth of information. Business Standard reports that in 2021–2022 the government overspent on cyber security for the first time in eight years. Recently, the government budgeted 515 crore rupees for cyber security for the years 2022–2023.

The steps India has taken and the progress it has made in creating its cybersecurity plan for 2020.

- **CERT-In** The Indian Computer Emergency Response Team (CERT-In) has made major strides in thwarting cyberattacks on government networks. The Indian government faces a serious problem with cybercrime, but anti-phishing and cybersecurity training have made a difference. CERT-In also releases alerts and advisories to let the public know about the most recent cyberthreats and countermeasures.
- **Cyber Surakshit Bharat** A initiative called Cyber Surakshit Bharat, created by MeitY, is intended to improve the cybersecurity landscape in India. This event was made possible by a grant from the National e-Government Division. (NeGD). Given the effects of digitization on government, good governance is more crucial than ever. Such a programme would increase awareness of cybercrime and make CISOs and frontline IT

personnel more secure. Officials will receive cybersecurity health toolkits and training on best practises as part of this first public-private partnership.

- **National Critical Information Infrastructure Protection Centre** The federal government established the National Center for Immunization and Immunization Programs (NCIIPC) to safeguard crucial data that impacts public health, economic development, and national security. This was modified by Section 70A of the Information Technology (IT) Act, 2000. This organisation has no issues conducting routine cybersecurity exercises to check on the state of readiness and posture of the government and other important sectors.
- **Appointment of Chief Information Security Officers** Greater digitization calls for greater safety considerations. If even the slightest error is found, the entire federal system might collapse. Every government organisation should have a Chief Information Security Officer (CISO) who can determine and record the security needs for every technology innovation. The Indian government has provided CISOs with instructions on how to safeguard apps, infrastructure, and compliance from online attacks.
- Training & Mock Drills The government has also evaluated the cybersecurity of businesses by running mock drills. MeitY reports that 44 drills have been held by CERT-In this year. Reliable sources report that 265 organisations representing various states and industry participated. Attacks will be made against telecommunications, finance, defence, and energy. Cyberattack readiness is a perennial worry for CISOs and network or system administrators. 515 persons had participated in 19 of these trainings as of October 2019.
- Malware Protection The central government has also introduced a malware analysis and detection tool called Cyber Swachh Kendra. Additionally, you can utilize the free tools provided to delete or omit them from your website or online application. As part of the Cyber Swachh initiative, the government has established a department in addition to the National Cyber Coordination Centre to educate the public about existing and potential cybersecurity hazards (NCCC).
- Personal Data Protection Bill Last but not least, the union government of India has approved the Personal Data Protection (PDP) Bill, which aims to localize data and protect Indian users from breaches that may occur anywhere in the globe. According to the bill, all personal data must be processed and maintained in India. Private and confidential information about an individual must be kept locally, however processing abroad is permitted under certain circumstances. The measure also makes an effort to make social media companies more accountable and to compel them to address issues with the dissemination of objectionable content. And they will.

Conclusion

Cyberattacks against India's critical infrastructure, which includes the energy, financial, defence, and telecommunications sectors, have the potential to have a detrimental impact on the country's economy as well as public safety. In accordance with the procedures used by other digital nations, the safeguarding of crucial informational infrastructure has been elevated to a position of great importance in the context of the nation's overall security (DSCI 2013). Indians shouldn't wait to build a national security plan that incorporates cybersecurity as a substantial component of the plan, as has been done by other nations across the world. Other nations have done this successfully.

Acknowledgement

We'd like to thank everyone who contributed to this article. We'd want to express our gratitude to everyone whose suggestions and inspiration helped us create this piece. The authors and specialists who have written on similar issues are also to be thanked for their citations, which helped us to correctly conclude our work.

Conflict of interest and funding

The authors declare no conflict of interest

References

Aiyengar, S. R. R. (2010). National Strategy for Cyberspace Security. New Delhi: KW Publisher

Alık, N. A. H. A. (2022). Emerging Cyber Security Threats: India's Concerns and Options. International Journal of Politics and Security, 4(1), 170-200.

Alsaibai, H., Waheed, S., Alaali, F., & Wadi, R. A. (2020, June). Online fraud and money laundry in E-Commerce. In ECCWS 2020 20th European Conference on Cyber Warfare and Security (p. 13). Academic Conferences and publishing limited.

Bagga, R. (2018). The National Cyber Security Policy of India 2013: An Analytical Study. Indian JL & Just., 9, 164.

Bajwa, L. G. J., George, M. G. N., & Sinha, B. D. (2016). Makeover of Rainbow Country.

Bamrara, D., Singh, G., & Bhatt, M. (2013). Cyber attacks and defense strategies in India: An empirical assessment of banking sector. Gajendra and Bhatt, Mamta, Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector (January 1, 2013).

Buzan, B. (2008). People, states & fear: an agenda for international security studies in the post-cold war era. ECPR press

Devi, S. (2019). Cyber Security In The National Security Discourse. World Affairs: The Journal of International Issues, 23(2), 146-159.

Dilipraj, E. (2013). India's Cyber Security 2013: A Review. Centre for Air Power Studies, 97(14), 1-4.

Dunn Cavelty, M. (2012). The militarisation of cyber security as a source of global tension. Center for Security Studies.

Ebert, H. (2020). Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. India Review, 19(4), 376-413

Ghate, S., & Agrawal, P. K. (2017). A literature review on cyber security in indian context. J. Comput. Inf. Technol, 8(5), 30-36.

Kovacs, A. (2021). Cybersecurity and Data Protection Regulation in India: An Uneven Patchwork. In CyberBRICS (pp. 133-181). Springer, Cham

Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. Crime, Law and Social Change, 66(3), 313-338.

Kshetri, N. (2016). Cybersecurity in India. In The Quest to Cyber Superiority (pp. 145-157). Springer, Cham.

Kumar, A. (2020). Securing digital sovereignty: In context to present day challenges of cyber space (Doctoral dissertation, Full Text-IIPA, New Delhi).

KUMAR, G. Cyber Security System and Policy of India: Challenges and Prospects. Soc. Sci, 6(7), 1937-1943

Pandey, S. (2020). Cyber Peace and Security.

Pandey, S. (2020). New Emerging Security Threats and Global Cyber Security Index.

Parmar, S. D. (2018). Cybersecurity in India: An evolving concern for national

Patil, S. (2022). India's Cyber Security Landscape. In Varying Dimensions of India's National Security (pp. 75-90). Springer, Singapore

Poornima, B. (2022). Cyber Threats and Nuclear Security in India. Journal of Asian Security and International Affairs, 23477970221099748.

Prasad, S., & Kumar, A. (2022). Cyber Terrorism: A Growing Threat to India's Cyber Security. In Nontraditional Security Concerns in India (pp. 53-73). Palgrave Macmillan, Singapore

Relia, S. (2016). Cyber warfare: its implications on national security. Vij Books India Pvt Ltd.

Selby, J. (2017). Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? International Journal of Law and Information Technology, 25(3), 213-232.

Shackelford, S. J., & Craig, A. N. (2014). Beyond the new digital divide: Analyzing the evolving role of national governments in internet governance and enhancing cybersecurity. Stan. J. Int'l L., 50, 119.

Venkatraman, B., & Gupta, K. (2016). Cybersecurity-Its Effects on National Security and International Relations. Indian JL & Pub. Pol'y, 3, 75..