WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Modern India's Internet Security

Mr. Nagendra R[1], Mr. Darshan M Patel [2], Mr. Sanjay P[3]

[1]Assistant Professor, Department of Computer Science and Engineering,
[2]Assistant Professor, Department of Computer Science and Engineering,
[3]Assistant Professor, Department of Computer Science and Engineering,
[1, 2, 3] Brindavan College of Engineering, Bangalore-560063, Karnataka, India.
Email: n12.nagendra@gmail.com[1],

A B S T R A C T

Cyber security has developed into a complicated and quickly changing security concern (ICT) in the era of information, communication, and technology. As ICT dependence spreads across the world, cyber threats appear destined to infiltrate every nook and cranny of national economies and infrastructure. In fact, an increase in computer and Internet-based networking use has been accompanied by an increase in cyber-attack incidents worldwide that target individuals, businesses, and governments. ICT is also increasingly being seen by certain nations as a battleground on which to wage strategic conflicts and as a tactical advantage to be employed for the purposes of national security. This paper examines the significance of cyber security in the present security debate and furthers the analysis by looking at cyber security from the perspective of India.

Keywords: Cyber security, Information Technology.

1. INTRODUCTION

Security is one of the key ideas in the study of international affairs. As a result of the severity of threats that states face from other states, as well as the manner and effectiveness of their responses, state security has historically and up until recently been the main focus of security analysis (Rather and Jose 2014). However, when the Cold War ended, scholars extended the concept of security to encompass the safety of the individual, turning their focus away from the state-centric viewpoint (Buzan 1991). Threats changed from external invasion to domestic conflicts brought on by civil wars, environmental degradation, economic hardship, and human rights violations around the same time.

As a result, issues including poverty, industrial competitiveness, educational obstacles, environmental dangers, human trafficking, and resource scarcity have been added to the list of concerns that fall under the umbrella of national security in addition to those related to territorial defense. The most recent information, communication, and technology (ICT) revolution has also created new difficulties for national security while transforming every element of human life. Internet, email, social media, and satellite communications are all examples of ICT.

In fact, the digital age has given rise to new national security challenges that aim to undermine a country's electronic infrastructure.

It should go without saying that in today's globalized society, the Internet and ICTs are essential for social and economic advancement. They create a vital digital infrastructure on which governments, economies, and society rely to perform their core functions. Due to its generally open nature, the Internet is a dangerous environment on many levels (Pillai 2012). Because of this, the field of cybersecurity has grown to encompass a range of problems, such as the defense of vital infrastructure, cyberterrorism, cyber threats, privacy issues, cybercrime, and cyberwarfare.

In the second decade of the twenty-first century, cyberthreats are rapidly evolving and expanding. They may not always be done for financial gain, but they may also originate from new locations like foreign states and political organizations. They are nevertheless launched by criminal actors. These latter efforts might include military operations, cyberespionage, sabotage using tools like Stuxnet, and political destabilization, similar to what happened in Estonia in 2007 (OECD 2012, 12). The sophistication of cybercriminals, the emergence of cyberespionage, as well as the widely reported actions of hacker collectives, all seem to be contributing to the perception that cyberattacks are becoming more organized and sophisticated, exhibiting evident indicators of professionalization.

Cybersecurity: Term and Definition

Network outages, computer viruses, data compromised by hackers, and other incidents have a significant impact on our lives in ways that range from troublesome to life-threatening. This is because the majority of government and financial institutions, military organizations, corporations, hospitals, and

other businesses store and process a great deal of confidential information on computers. Due to the frequency and sophistication of cyberattacks, there is a heightened need to secure sensitive data, personal information, and the security of the country.

As a result, "cybersecurity" refers to a collection of tools, rules, guidelines, training, actions, security concepts and safeguards, risk management strategies, assurance, and technologies that can be used to secure and protect user and organizational assets as well as the cyber environment.

In addition to securing computer programs, networks, and data, cybersecurity also focuses on stopping unauthorized individuals from accessing data, altering it unintentionally, or destroying it on purpose or unintentionally. Additionally, information technology security is a goal.

Cybersecurity is also necessary for the ongoing development of information technology and Internet services (UNODA 2011). Thus, the successful protection of vital information infrastructures is now even more essential for maintaining national security and fostering economic growth. In many countries, making the Internet as secure as possible is now crucial to the development of new services and public policy (Gercke 2009). The remainder of this article examines India's past and present responses to this new issue.

In addition to securing computer programs, networks, and data, cybersecurity also focuses on stopping unauthorized individuals from accessing data, altering it unintentionally, or destroying it on purpose or unintentionally. Additionally, information technology security is a goal.

Cybersecurity is also necessary for the ongoing development of information technology and Internet services (UNODA 2011). Thus, the successful protection of vital information infrastructures is now even more essential for maintaining national security and fostering economic growth. In many countries, making the Internet as secure as possible is now crucial to the development of new services and public policy (Gercke 2009). The remainder of this essay examines India's up to date response to this fresh issue.

Cybersecurity in India: Background

India is in need of a robust cybersecurity system, but officials haven't given the issue much thought. The government hasn't been able to meet this need as a result. The fact that India lacks access to crucial technologies for thwarting complex malware like Stuxnet, Flame, and Black Shadows makes its offensive and defensive cybersecurity skills worse (Kaushik 2014).

Additionally, India has a lot less cybersecurity initiatives and projects than other developed nations. Of the important projects that were first suggested, the Indian government has only partially implemented them. Two more initiatives that have been approved but haven't yet achieved commercial success are India's National Cyber Coordination Center (NCCC) and the National Critical Information Infrastructure Protection Center (NCIPC). At the same time, India needs to act quickly to protect its critical infrastructure, such as its banks, satellites, automated power grids, and thermal power plants, from cyberattacks. The Indian government has acknowledged that cyberattacks on organizations like the banking and financial services sector have significantly increased. Malicious online behavior in India has taken many forms, including viruses, hacking, identity theft, spam, email bombing, web defacing, and denial of service.

Cyber Security in India: In-Depth

India's IT sector is now a major force behind the country's economic growth and a vital sector of its economy and government. The sector is positively influencing the lives of Indian citizens by making direct or indirect contributions to the betterment of many socioeconomic factors, including the standard of living, employment, and diversity. In addition, IT has played a significant role in elevating India to the top of the international rankings for the delivery of first-rate business services and technological advancements (DEITY 2011).

With the expansion of the IT sector, the need to protect the computing environment and build appropriate confidence and trust in it has increased dramatically. For instance, the majority of financial institutions and the banking industry have incorporated IT into their operations, opening up a plethora of opportunities for growth while also making these institutions vulnerable to cyberattacks in their day-to-day operations, making the apparent lack of strategies to address these types of threats all the more worrisome.

The government sector, on the other hand, has promoted corporate participation while constructing a sizable IT infrastructure to facilitate the increased adoption of IT-enabled services and initiatives, such as the Unique Identification Development Authority of India (UIDAI) and the National e-Governance Programs (NeGP). Currently, computer networks are widely utilized as a source of information, a communication tool, and to relay data for commercial transactions in critical industries like defense, banking, energy, telecommunication, transport, and other public services. To enhance online connectivity, e-commerce services, and general IT communications use, the government has set lofty goals. According to Indian Prime Minister Narendra Modi, the ambitious "Digital India" program, which aims to connect every grame panchayat by broadband internet, promote e-governance, and transform India into a connected knowledge economy, has been approved by the cabinet (The Economic Times 2014). All of this government spending on cutting-edge technology stimulates the adoption of stringent laws that will guarantee the quality of services. Notably, a growing reliance on IT has exposed India's vital defense and intelligence systems to cyberattacks. In fact, there is a higher chance of state and military secrets being stolen when attacks on government infrastructure occur (Aiyengar 2010). In light of this, it is not surprising that several organizations under the control of the Indian Ministry of Defence have stepped up to manage cybersecurity.

An illustration would be , To protect the army's networks at the divisional level and to conduct secure cybersecurity assessments, the Indian Army established the Cyber Security Establishment in 2005 (Pandit 2005). The army established a cybersecurity laboratory at the Military College of Telecommunications Engineering in Madhya Pradesh in 2010 to provide commanders with specialized training in security.

Energy and Cybersecurity

An important non-traditional security worry is now India's access to energy. Despite having one of the lowest average per-person energy consumptions in the world, the country utilizes the fourth-most primary energy globally (TERI 2013). Due to weak regulation of information sharing and insufficient mechanisms to support it, information on cyberattacks and equipment vulnerabilities in the Indian energy sector is basically nonexistent. The industry, however, appears to be a target of sophisticated attacks more frequently, according to trends in global cybersecurity, especially now that India has begun connecting it to modern technologies to meet its burgeoning energy needs (Walstrom 2016).

In fact, a few issues began to surface as a result of the application of new technology in this area. For instance, after India conducted a nuclear test in May 1998, a group of hackers posted comments critical of India and the nuclear industry on the website of the Bhabha Atomic Research Center (BARC). (2013) Patil and Bhosale. Additionally, in retaliation for ongoing government activities in the occupied territory of Kashmir, an internet hacker going by the handle PhrOzenMyst broke into the BARC's official website and exposed some of its sensitive material (The Pioneer 2013).

Defence and Cybersecurity

According to KPMG (2010), India has the third-largest armed forces in the world as well as a considerable defense industrial base. As a result of its reliance on these technologies and the requirement to link networks, it has also merged its defense industry with modern technology, exposing the country to a multitude of continuously evolving threats. For example, in 2012 hackers conducted a cyberattack against the eastern command computer systems of the Indian Navy, which are in charge of overseeing maritime operations in the South China Sea and conducting tests on India's ballistic missile submarines. The naval computers were infiltrated by a malware that covertly captured and sent private files and documents to Chinese IP addresses.

Finance and Cybersecurity

India's massive growth has been accelerated by the usage of IT, making it one of the economies in the world with the fastest growth rates. But as our reliance on IT has increased, so have new vulnerabilities. As has typically been the case, it is claimed that the majority of cyberattacks are carried out for financial benefit (KPMG 2014). In reality, modern banking and financial institutions are vulnerable to cyberattacks from both state-sponsored and non-state actors due to their complexity (Singh 2013). The problem has gotten worse due to the interconnectedness of modern technologies, which has increased the likelihood of fraud, theft, and other forms of exploitation (Bamrara et al. 2013). Because of this, Kapil Sibal, a former minister of telecom in India, said that "cybersecurity is crucial for economic security, and any failure.

Telecommunications and Cybersecurity

Telecommunications in India are now a significant driver of social and economic development. With 943 million phone connections in February 2012 alone, India is currently regarded as one of the telecom markets that is growing the quickest worldwide

The country had 911 million mobile phone connections in the same month (NTP 2012), and about 160 million people were online, with nearly half of them using social media. By 2020, according to the Indian government, there will be 600 million broadband connections and a complete teledensity

Numerous cyberthreats and attacks have also been present with this industry's tremendous expansion. The telecoms business is said to be most at risk from information due to the surge in cyberfrauds. As an example, on August 7, 2013, malware was installed on the computers of the Indian business Bharat Sanchar Nigam Limited (BSNL) after hackers gained access to the company's database. The BSNL Office Domain was once again breached on October 12 of that year, and some significant data was seized (Dilipraj 2014). Similar to this, on June 9, 2013, several unidentified hackers broke into the website of Mahanagar Telephone Nigam Limited (MTNL) using the DDoS tactic. The hack was carried out in protest of alleged MTNL-supported Internet censorship.

2. CONCLUSION:

The pages that precede it make clear that cyberattacks aimed targeting India's crucial information infrastructure, including its energy, financial, defense, and telecommunications sectors, have the potential to negatively impact the nation's economy and public safety. The protection of the vital information infrastructure has been upgraded to a high priority from the perspective of national security, according to legislation already adopted by other digital nations (DSCI 2013). In fact, the emergence of cybersecurity as a crucial component of national security plans has been pushed by the growing cross-border interdependence of the digital world.India shouldn't hold off on adopting policies that have been adopted by other countries (Kumar and Mukherjee 2013).

REFERENCES

1. Aiyengar, S. R. R. (2010). National Strategy for Cyberspace Security. New Delhi: KW Publisher.
2. 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
3. Empirical Assessment of the Banking Sector.” International Journal of Cyber Criminology,
4. 7 (1): 49–61.
5. Buzan, B. (1991). People, States, and Fear: An Agenda for International Security Studies in the Post Cold War Era. London: Harvester Wheatsheaf.
6. 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.
7. Dilipraj, E. (2013). “India‟s Cyber Security 2013: A Review.” Centre for Air Power Studies, 97 (14): 1–4.
8. DSCI. (2013). Analysis of National Cyber Security Policy (NCSP–2013). New Delhi: Data Security Council of India.
9. Gercke. (2009). Understanding Cybercrime: A Guide for Developing Countries, Geneva: ITU publication.
10. Governance Now. (2010). Army Sets Up Cyber Security Lab. http://www.governancenow.com/news/regular-story/army-sets-cyber-security-lab.
11. Government of India. (2011). Discussion Draft on National Cyber Security Policy. New Delhi: DIETY.
12. Government of India. (2012). “National Telecom Policy (NTP) – 2012.” Ministry of Communication and Information Technology (NTP). New Delhi, June 13.
13. http://www.dot.gov.in/sites/default/files/NTP-06.06.2012-final_0.pdf. Government of India. (2012). National Cyber Security Strategy, India: DEITY.
14. IANS. (2014). “69 Percent of Cyberattacks Targeted at Large Companies in India: Report.” Business Standard, New Delhi, April 24.
15. IDSA. (2012). India's Cyber Security Challenges. New Delhi: Institute of Defence Studies and Analyses.
16. Indo-Asian News Services. (2014). “Large Firms Hit by 69 Percent of Targeted Cyberattacks in India: Symantec.” April 26. http://gadgets/ndtv.com/internet/news/large-firms-hit-by-69-percent-of- targeted-cyber-attacks-in-india-symantec-513975.
17. ITU. (2009). Series-X: Data Networks Open System Communication and Security, Overview of Cybersecurity ITU-T X.1205, Geneva: ITU.
18. Jain, S. (2014). Cyber Security: A Sine Qua Non. http://www.indiandefencereview.com/news/cyber- security-a-sine-qua-non/.
19. 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.”
20. http://cybersecurityforindia.blogspot.in/2014/09/cyber-security-needs-urgent-attention.html.
21. KPMG. (2010). Indian Defence Sector: The Improving Landscape for US Business and Indo-US Commercial, KPMG International, Swiss.
22. KPMG. (2014). Forensic Technology Services: Cyber Crime Survey Report – 2014. KPMG International, Swiss.
23. Kumar, A. V.; K. K. Pandey, and D. K. Punia (2013). Facing the Reality of Cyber-Threats in the Power Sector. Bangalore: Wipro Technologies.
24. Kumar, R. & N. Mukherjee. (2013). Cyber Security in India: A Skill-Development Perspective. New Delhi: Communication Multimedia and Infrastructure.
25. Madaan, N. (2013). “More in City Fall in Net Trap.” Times of India, Pune, September 8.
26. Manoharan, N. (2013). “India‟s Internal Security Situation: Threats and Responses.” India Quarterly:
27. A Journal of International Affairs 69 (4): 367–381.
28. OECD. (2012). “Cybersecurity Policy Making at a Turning Point.” http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.
29. Pandit, R. (2005). “Army Gearing Up for Cyberwarfare.” Times of India, New Delhi, July 7. Patil, P.

    R. and Bhosale, D. V. (2013). “Need to Understand Cyber Crime‟s Impact over National
30. Security in India: A Case Study.” Online International Interdisciplinary Research Journal 3 (4): 167– 171.
31. Pillai, P. (2012). “History of Internet Security.” http://www.buzzle.com/articles/history-of-internet- security.html.
32. Pubby, M. (2012). “China Hackers Enter Navy Computers, Plant Bug to Extract Sensitive Data.” The Indian Express, New Delhi, July 1.
33. Rather, M. A. & K. Jose (2014). “Human Security: Evolution and Conceptualization.” European Academic Research, 2 (5): 6766–6797.

34. Reddy, K. S. (2012). “Anonymous Takes Down MTNL Website.” The Hindu, New Delhi, June 6. Reich, P. C., ed. (2012). Law, Policy, and Technology: Cyberterrorism, Information Warfare, and

35. Internet Immobilization: Cyberterrorism, Information Warfare, and Internet Immobilization. IGI Global.

36. Ruggiero, P. & J. Foote (2011). Cyber Threats to Mobile Phones. United State: US Department of Homeland Security.

37. https://www.us-cert.gov/security-publications/cyber-threats-mobile-phones.

38. Shuran, L., D. Hui, and G. Su. (2013). “Analyses and Discussions of the Blackout in Indian Power Grid.” Energy Science and Technology 6 (1): 61–66.

39. Singh, A. (2012). “Over 10,000 Email IDs Hit in „Worst‟ Cyberattack.” The Indian Express. New Delhi, December 18.

40. Singh, H. and J. T. Philip (2010). “Spy Game: India Readies Cyber Army to Hack into Hostile Nations Computer Systems.” Economic Times, New Delhi, August 6.

41. Singh, S. (2013). “Cyber Security Plan to Cover Strategic, Military, Government and Business Assets.” The Hindu, New Delhi, July 2.

42. TERI. (2013). TERI Energy Data Directory & Yearbook (TEDDY) 2012/13. New Delhi: TERI Press. The Economic Times. (2012). “Indian OS Developed by DRDO Likely to Be Ready in Three Years.”

43. Hyderabad, December 20.

44. The Economic Times. (2014). “Government Mulls Digital India Programme to Connect All Villages.” New Delhi, August 21.

45. The Economic Times. (2014). “Most Cyberattacks on India Show Chinese IP Address: NTRO.” New Delhi, November 13.

46. The Hindu (2013). “Cyber Frauds Cost India $4 Billion in 2013: Symantec.” New Delhi, October 22. The Indian Express (2014). “Modi to Visit Australia after G-20 Summit.” New Delhi, September 6. The Pioneer. (2013). “ECIL Website Hacked, Sensitive Data Leaked.” New Delhi, August 27.

47. UNIDIR. (2013). The Cyber Index: International Security Trends and Realities. New York and Geneva: United Nations Institute for Disarmament Research.

48. Unnithan, S. (2012). “Enter the Cyber Dragon: India to Walk an Extra Mile to Match China's Achievement in Cyberspace.” India Today, October 26.

49. UNODA. (2011). Developments in the Field of Information and Telecommunications in the Context of International Security. New York: United Nations Office for Disarmament Affairs.

50. Verma, A. K. and A. K. Sharma. (2014). “Cyber Security Issues and Recommendations.” International Journal of Advanced Research in Computer Science and Software Engineering 4 (4): 629–634.

51. Walstrom, M. (2016). “India‟s Electrical Smart Grid: Institutional and Regulatory Cyber security Challenges.” Seattle: Henry M. Jackson School of International Studies.

[1] [9] C. Bekara, “Security issues and challenges for the IoT-based smart grid”, Procedia Computer Science 34, pp. 532–537, 2014.

[2] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges”, Ad HocNetworks, vol. 10, no. 7, pp. 1497–1516 , 2012

[3] F. A. Alaba, M. Othman, I. A. T Hashem, F. Alotaibi, "Internet of Things security: A survey." Journal of Network and Computer Applications 88 , pp. 10-28, 2017.

[4] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the Internet of Things: perspectives and challenges. Wirel. Netw. 20 (8), pp. 2481–2501, 2014.

[5] N. Agarwal, A. Rana, J.P. Pandey, A. Agarwal, “Secured sharing of data in cloud via dual authentication, dynamic unidirectional PRE, and CPABE" in International Journal of Information Security and Privacy, Vol 14, Issue 1, pp 44-66, 2020.

[6] K. Zhao and L. Ge, “A survey on the internet of things security,” in Computational Intelligence and Security (CIS), 2013 9th International Conference on, pp. 663–667, IEEE, 2013.

[7] https://blog.smartbear.com/iot-2/how-to-protect-iot-gateways-from-securityvulnerabilities/ (Online; accessed on 04 May 2018)