International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cybersecurity in Digital India

Koyel Ghosh

Student, Brainware University in Kolkata
ghoshkoyel2025@gmail.com

Abstract

In the age of information, communication, and technology, cybersecurity has evolved into a complex and rapidly evolving security concern (ICT). Cyber threats seem likely to infiltrate every nook and cranny of national economies and infrastructure as ICT dependence spreads across the globe; in fact, the increased use of computers and Internet-based networking has been accompanied by an increase in cyberattack incidents worldwide that target people, companies, and governments. ICT is also increasingly being viewed by certain countries as a battlefield where strategic wars can be fought as well as a strategic asset to be used for the reasons of national security. The importance of cybersecurity in the current security discussion is examined in this study, which deepens the analysis by considering the cybersecurity field from the standpoint of India.

Keywords: Cybersecurity, Information Technology.

Introduction

One of the most important concepts in the study of international relations is security. Security analysis has historically, and up until recently, been primarily concerned with state security, considering it as a result of the degree of threats that states confront from other states, as well as the style and efficacy of their responses (Rather and Jose 2014). But following the end of the Cold War, researchers broadened the definition of security to include the protection of the individual, shifting their attention away from the state-centric perspective (Buzan 1991). Around the same period, dangers shifted from external invasion to internal conflicts caused by civil wars, environmental degradation, economic hardship, and human rights abuses.

Because of this, national security has expanded to include concerns beyond territorial defence, such as poverty, industrial competitiveness, educational challenges, environmental risks, human trafficking, and resource shortages. Finally, the recent Information, Communication, and Technology (ICT) revolution has transformed every aspect of human life and presented fresh challenges to national security. ICT includes the Internet, email, social media, and satellite communications.

In fact, new threats to national security are being introduced by the digital era that aim to destroy a nation's technological infrastructure.

It goes without saying that the Internet and ICTs are crucial for economic and social development in the globalised world. They form a crucial digital infrastructure on which societies, economies, and governments rely to carry out their fundamental duties. The Internet is a risky environment on many levels due to its relatively open nature (Pillai 2012). As a result, cybersecurity has expanded to include a variety of issues, including the protection of critical infrastructure, cyberterrorism, cyber threats, privacy concerns, cybercrime, and cyber warfare.

Cyber threats are developing and growing quickly in the second decade of the twenty-first century. They are still started by criminal actors, but they also emerge from new places like foreign states and political organisations, and they might not just be done for financial gain. These latter activities could involve political destabilisation (such as what occurred in Estonia in 2007), cyberespionage, sabotage (such as Stuxnet), and even military actions (OECD 2012, 12). Cyberattacks appear to be growing more organised and sophisticated, showing obvious symptoms of professionalisation, as a result of the sophistication of cybercriminals, the advent of cyberespionage, as well as the widely publicised actions of hacker collectives.

Cybersecurity: Term and Definition

Because the majority of government and financial institutions, military organisations, corporations, hospitals, and other businesses store and process a great deal of confidential information on computers, network outages, computer viruses, data conceded by hackers, and other incidents have a significant impact on our lives in ways that range from troublesome to life-threatening. As a result, there is a greater need to secure sensitive data, personal information, and the nation's security due to the frequency and sophistication of cyberattacks.

As a result, "cybersecurity" refers to a group of technologies, policies, guidelines, training, actions, security concepts and safeguards, risk management techniques, assurance, and tools that can be used to secure and protect both organisation and user assets as well as the cyber environment.

Cybersecurity also focuses on protecting computer programmes, networks, and data, along with preventing access to information by unauthorised users, as well as preventing unintended change or intended/unintended destruction. It also aims to secure information technology.

Additionally, the continued advancement of information technology and Internet services depends on cybersecurity (UNODA 2011). The successful safeguarding of crucial information infrastructures has thus become more crucial to national security and nations' economic prosperity. Making the Internet as secure as feasible is now essential to the creation of both new services and government policy in many nations (Gercke 2009). The remainder of this article looks at how well India has, up until now, handled this new problem.

Cybersecurity also focuses on protecting computer programmes, networks, and data, along with preventing access to information by unauthorised users, as well as preventing unintended change or intended/unintended destruction. It also aims to secure information technology.

Additionally, the continued advancement of information technology and Internet services depends on cybersecurity (UNODA 2011). The successful safeguarding of crucial information infrastructures has thus become more crucial to national security and nations' economic prosperity. Making the Internet as secure as feasible is now essential to the creation of both new services and government policy in many nations (Gercke 2009). The remainder of this paper looks at how well India has, up to now, handled this new problem.

Cybersecurity in India: Background

The need for a strong cybersecurity apparatus in India is growing, but policymakers haven't given the problem much attention. As a result, the government hasn't been able to address this need. India has both

offensive and defensive cybersecurity capabilities, which is made worse by its inability to access key tools for fending off sophisticated malware like Stuxnet, Flame, and Black shades (Kaushik 2014).

Additionally, compared to other wealthy countries, India has much less cybersecurity projects and activities. The Indian government has only implemented a small number of the pertinent projects that had originally suggested. The National Critical Information Infrastructure Protection Center (NCIPC) and the National Cyber Coordination Center (NCCC) of India are two other projects that have been approved but have so far failed to metarialize. At the same time, India must urgently safeguard crucial infrastructure from cyberattacks, including banks, satellites, automated power grids, and thermal power plants. The Indian government has acknowledged that there has been a significant increase in cyberattacks targeting organisations like the banking and financial services industry. In India, malicious online behaviour has included everything from viruses to hacking to identity theft to spamming to email bombing to web defacing to denial of service.

Cyber Security in India: In-Depth

India's IT industry has become a key driver of the nation's economic expansion as well as an essential component of its commerce and government. Through direct or indirect contributions to the improvement of numerous socioeconomic criteria, such as the standard of living, employment, and diversity, the sector is favourably affecting the lives of Indian inhabitants. Additionally, IT has been crucial in making India a worldwide leader in the provision of top-notch business services and technological solutions (DEITY 2011).

The requirement to safeguard the computing environment and to establish sufficient confidence and trust in it has grown significantly along with the development of the IT industry. For instance, the majority of financial institutions and the banking sector have integrated IT into their operations, creating countless opportunities for growth while also making these institutions vulnerable to cyberattacks in their daily operations, making the apparent lack of strategies to deal with these types of threats particularly concerning.

For its part, the government sector has facilitated the increased adoption of IT-enabled services and programs, such as the National e-Governance Programs (NeGP) and the Unique Identification Development Authority of India (UIDAI), by building a sizable IT infrastructure and encouraging corporate participation. Computer networks are currently heavily used in crucial sectors like defence, banking, energy, telecommunication, transport, and other public services to relay data for business transactions, as well as a source of information and for communication. The government currently has ambitious goals to increase cyber connectivity, e-commerce services, and overall IT communications use. The ambitious "Digital India" programme, which aims to connect every gramme panchayats by broadband internet, promote e-governance, and turn India into a connected knowledge economy, has been approved by the cabinet, according to Indian Prime Minister Narendra Modi, is typical in this respect (The Economic Times 2014b). All of this public investment in emerging technology encourages the implementation of strict regulations that will deliver reliable services. Notably, a growing reliance on IT has left the crucial defence and intelligence systems underpinning India vulnerable to cyberattacks. Attacks on government infrastructure do, in fact, raise the risk of state and military secrets being stolen (Aiyengar 2010). Therefore, it is not unexpected that a number of organisations under the purview of the Indian Ministry of Defence have taken on the task of managing cybersecurity. As an illustration, the

Indian Army established the Cyber Security Establishment in 2005 to safeguard the army's networks at the divisional level and to carry out secure cybersecurity audits (Pandit 2005). In order to give commanders specialised training in security, the army has created a cybersecurity laboratory at the Military College of Telecommunications Engineering in Madhya Pradesh in 2010.

Energy and Cybersecurity

India's energy security has become a crucial non-traditional security concern. The nation consumes the fourth-most primary energy in the world, although its average per-person consumption is quite low (TERI 2013). Information on cyberattacks and equipment vulnerabilities in the Indian energy sector is essentially nonexistent due to inadequate regulation of information sharing and inadequate structures to promote it. However, trends in global cybersecurity lead us to believe that the industry is increasingly the target of sophisticated assaults, particularly now that India has started connecting it to contemporary technologies to fulfil its expanding energy needs (Walstrom 2016).

Indeed, a number of difficulties started to emerge as a result of the introduction of new technology in this field. For instance, a gang of hackers placed anti-India and anti-nuclear remarks on the Bhabha Atomic Research Center (BARC) website following India's nuclear test in May 1998. (Patil and Bhosale 2013). Additionally, an internet hacker by the name of PhrOzenMyst compromised the BARC's official website and released some of its sensitive data in retaliation for ongoing government activities in the occupied region of Kashmir (The Pioneer 2013).

Defence and Cybersecurity

India has the third-largest armed forces in the world and has a sizable defence industrial base (KPMG 2010). At the same time, it has integrated its defence industry with modern technology, exposing the nation to a number of constantly changing threats as a result of its reliance on these technologies and the need to integrate networks. For instance, in 2012 hackers launched a cyberattack against the Indian Navy's eastern command computer systems, which are in charge of managing maritime operations in the South China Sea and testing of India's ballistic missile submarines. A virus that secretly collected and transmitted private files and documents to Chinese IP addresses infected the naval computers.

Finance and Cybersecurity

The use of IT has acted as a catalyst for India's enormous growth, making it one of the economies in the world with the quickest growth rates. However, new vulnerabilities have been created as a result of growing reliance on IT. Most cyberattacks are said to be motivated by money or financial gain, which has generally been the case (KPMG 2014). Actually, due to their complexity, modern banking and financial institutions are open to cyberattacks from both state-sponsored and non-state entities (Singh 2013). The issue has been made worse by the interconnected nature of contemporary technologies, which has given rise to numerous chances for theft, fraud, and other types of exploitation (Bamrara et al. 2013). As a result, the former Indian Minister of Telecom, KapilSibal, has stated that "cybersecurity is important for economic security, and any failure.

Telecommunications and Cybersecurity

In India, telecommunications has become a major force for social and economic advancement. India is currently considered to be one of the fastest expanding telecom markets in the world, with 943 million telephone connections in February 2012 alone.

In the same month, the nation had 911 million mobile phone connections (NTP 2012), and there were almost 160 million Internet users, with nearly half of them using social media. The Indian government has declared that it will have 600 million broadband connections and 100 percent teledensity by 2020.

The significant expansion of this industry has also been accompanied by a number of cyberthreats and attacks. Due to the rise in cyberfrauds, it is stated that information poses the greatest risk to the telecommunications industry. As an illustration, on August 7, 2013, malware was put into the systems of Bharat Sanchar Nigam Limited (BSNL), an Indian company, after hackers broke into its database. On October 12 of that year, BSNL's Office Domain was once again compromised, and some crucial data was taken (Dilipraj 2014). Similar to this, on June 9, 2013, some unidentified hackers used the DDoS technique to infiltrate the website of Mahanagar Telephone Nigam Limited (MTNL). The attack's motivation was to protest alleged Internet censorship supported by MTNL.

Conclusion

As is evident from the pages that precede it, cyberattacks aimed at India's important information infrastructure, including its energy, financial, defence, and telecommunications sectors, have the potential to have a negative effect on the country's economy and public safety. According to regulations already taken by other digital nations, the protection of the essential information infrastructure has been elevated to a high priority from the standpoint of national security (DSCI 2013). In fact, the increasing cross-border interdependence of the digital sphere has prompted the development of cybersecurity as a key element of national security strategies.India should not wait to emulate the policies that have been implemented in nations around the world (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 Cybersecurity Challenges." Seattle: Henry M. Jackson School of International Studies.