Ghosts in the Machine: The Past, Present, and Future of India's Cyber Security

Shashank Yadav

ABSTRACT

The article "Ghosts in the Machine: The Past, Present, and Future of India's Cyber Security" by Shashank Yadav provides a comprehensive review of India's cybersecurity journey, from its early days of electronic communications under British rule to the present-day challenges. It traces the evolution of cybersecurity policies, highlighting key historical milestones and policy gaps. The article critically examines the 2013 National Cybersecurity Policy, identifying its shortcomings in addressing modern threats, such as advanced persistent threats (APTs) and the role of AI and automation. The paper emphasizes the need for a robust, forward-looking cybersecurity strategy that integrates human factors, operational constructs, and technological advancements to ensure national resilience in cyberspace. The article also delves into the human dimension of cybersecurity, emphasizing the importance of situational awareness and the vulnerabilities posed by reliance on technology. It argues that the current cybersecurity policy framework in India lacks the necessary depth and foresight to tackle emerging threats, particularly in the context of international cyber operations and the evolving landscape of cyber warfare. The author calls for a more integrated and proactive approach to cybersecurity, one that aligns with national security objectives and addresses the challenges of the digital age.

Key words: Cybersecurity policy, National Cybersecurity Strategy, Communication

When the National Cybersecurity Policy was released in 2013, the response from experts was rather underwhelming [1], [2]. A reaction to a string of unpalatable incidents, from Snowden's revelations [3] and massive compromise of India's civilian and military infrastructure [4] to the growing international pressure on Indian IT companies to fix their frequent data breaches [5], the 2013 policy was a macro example of weak structures finding refuge in a haphazard post-incident response. The next iteration of the policy is in formulation under the National Cybersecurity Coordinator. However, before we embark upon solving our cyber-physical domain's future threat environment, it is perhaps wise to look back upon the perilous path that has brought us here.

Early History of Electronic Communications in India

The institutional "cybersecurity thinking" of post-independence Indian government structures can be traced to 1839 when the East India Company's then Governor-General of India, Lord Dalhousie, had asked a telegraph system to be built in Kolkata, the then capital of the British Raj. By 1851, the British had deployed the first trans-India telegraph line, and by 1854, the first Telegraph Act had been passed. Similar to the 2008 amendment to the IT Act which allowed the government to intercept, monitor and

decrypt any information on any computer, the 1860 amendment to the Telegraph Act too granted the British to take over any leased telegraph lines to access any of the telegraphs transmitted. After all, the new wired communication technology of the day had become an unforeseen flashpoint during the 1857 rebellion.

Post-independence, under the socialist fervour of Nehruvian politics, the government further nationalised all foreign telecommunications companies and continued the British policy of total control over telecommunications under its own civil service structure, which too came pre-packaged from the British.

Historians note that the telegraph operators working for the British quickly became targets of intrigues and lethal violence during the mutiny [6], somewhat akin to today's Sysadmins being a top social engineering priority for cyber threat actors [7]. One of the sepoy mutineers of 1857, while on his way to the hangman's halter, famously cried out at a telegraph line calling it the cursed string that had strangled the Indians [8]. On the other side of affairs, after having successfully suppressed the mutiny, Robert Montgomery famously remarked that the telegraph had just saved India [9]. Within the telegraph system, the problems of information security popped up fairly quickly after its introduction in India. Scholars note that commercial intelligence was frequently peddled in underground Indian markets by government telegraph clerks [10], in what can perhaps be described as one of the first "data breaches" that bureaucrats in India had to deal with.

British had formulated different rules for telecommunications in India and England. While they did not have the total monopoly and access rights over all transmissions in Britain, for the purpose of maintaining political control, in India they did [11]. Post-independence, under the socialist fervour of Nehruvian politics, the government further nationalised all foreign telecommunications companies and continued the British policy of total control over telecommunications under its own civil service structure, which too came pre-packaged from the British.

The Computer and "The System"

Major reforms are often preceded by major failures. The government imported its first computer in 1955 but did not show any interest in any policy regarding these new machines. That only changed in 1963, when the government under the pressure to reform after a shameful military defeat and the loss of significant territory to China, instituted a Committee on Electronics under Homi Jehangir

Bhabha to assess the strategic utilities that computers might provide to the military [12].

In 1965, as punitive sanctions for the war with Pakistan, the US cut off India's supply of all electronics, including computers. This forced the government to set up the Electronics Committee of India which worked alongside the Electronics Corporation of India (ECIL), mandated to build indigenous design and electronic manufacturing capabilities. But their approach was considered highly restrictive and discretionary, which instead of facilitating, further constrained the development of computers, related electronics, and correspondingly useful policies in India [13]. Moreover, no one was even writing commercial software in India, while at the same the demand for export-quality software was rising. The situation was such that ECIL had to publish full-page advertisements for the development of export-quality software [12]. Consequently, in the early 1970s, Mumbai-based Tata Consultancy Services managed to become the first company to export software from India. As the 1970s progressed and India moved into the 1980s, it gradually became clearer to more and more people in the government that their socialist policies were not working [14].

In 1984, the same year when the word 'Cyberspace' appeared in a sci-fi novel called Neuromancer, a policy shift towards computing and communications technologies was seen in the newly formed government under Rajiv Gandhi [12]. The new computer policy, shaped largely by N. Sheshagiri who was the Director General of the National Informatics Centre, significantly simplified procedures for private actors and was released within twenty days of the prime minister taking the oath. Owing to this liberalisation, the software industry in India took off and in 1988, 38 leading software companies in India came together to establish the National Association of Software and Service Companies (NASSCOM) with the intent to shape the government's cyber policy agendas. As we are mostly concerned about cybersecurity, it should be noted that in 1990, it was NASSCOM that carried out probably the first IT security-related public awareness campaign in India where it called for reducing software piracy and increasing the lawful use of IT [5].

Unfortunately, India's 1990s were mired by coalition governments and a lack of coherent policy focus. In 1998, when Atal Bihari Vajpayee became the Prime Minister, the cyber policy took the most defining turn with the development of the National IT Policy. The IT Act, thus released in 2000 and amended further in 2008, became the first document explicitly dealing with cybercrime. Interestingly, the spokesman and a key member of the task force behind the national IT policy was Dewang Mehta, the then president of NASSCOM. Nevertheless, while computer network operations had become regular in international affairs [15], there was still no cyber policy framework or doctrine to deal with

the risks from sophisticated (and state- backed) APT actors that were residing outside the jurisdiction of Indian authorities. There still is not.

In 2008, NASSCOM established the Data Security Council of India (DSCI), which along with its parent body took it upon itself to run cybersecurity awareness campaigns for law enforcement and other public sector organisations in India. However, the "awareness campaign" centric model of cybersecurity strategy does not really work against APT actors, as became apparent soon when researchers at the University of Toronto discovered the most massive infiltration of India's civilian and military computers by APT actors [4]. In 2013, the Snowden revelations about unrestrained US spying on India also ruffled domestic feathers for lack of any defensive measures or policies [3]. Coupled with these surprise(?) and unpalatable revelations, there was also the increasing and recurring international pressure on Indian IT to put an end to the rising cases of data theft where sensitive data of their overseas customers was regularly found in online underground markets [16].

Therefore, with the government facing growing domestic and international pressure to revamp its approach towards cybersecurity, MeitY released India's first National Cybersecurity Policy in 2013 [17]. Ministry of Home Affairs (MHA) also released detailed guidelines "in the wake of persistent threats" [18]. However, the government admitted to not having the required expertise in the matter, and thus the preparation of the MHA document was outsourced to DSCI. Notwithstanding that, MHA's document was largely an extension of the Manual on Departmental Security Instructions released in 1994 which had addressed the security of paper-based information. Consequently, the MHA document produced less of a national policy and more of a set of instructions to departments about sanitising their computer networks and resources, including a section on instructions to personnel over social media usage.

The 2013 National Cybersecurity Policy proposed certain goals and "5-year objectives" towards building national resilience in cyberspace. At the end of a long list of aims, the 2013 policy suggested adopting a "prioritised approach" for implementation which will be operationalised in future by a detailed guide and plan of action at national, sectoral, state, ministry, department and enterprise levels. However, as of this writing the promised implementation details, or any teeth, are still missing from the National Cybersecurity Policy. As continued APT activities [19] show, the measures towards creating situation awareness have also not permeated beyond the technical/collection layer.

In 2014, the National Cyber Coordination Centre (NCCC) was established, with the primary aim of building situational awareness of cyber threats in India. Given the underwhelming response to the

2013 policy [1], [2], the National Cybersecurity Policy was surmised to be updated in 2020, but as of this writing, the update is still being formulated by the National Cybersecurity Coordinator who heads the NCCC. The present policy gap makes it an opportune subject to discuss certain fundamental issues with cyber situation awareness and the future of cyber defences in the context of the trends in APT activities.

Much to Catch Up

Recently, the Government of India's Kavach (an employee authentication app for anyone using a 'gov.in' or 'nic.in' emails-id) was besieged by APT26 [20]. APT26 is a Pak- affiliated actor and what one might call a tier-3 APT i.e., what they lack in technical sophistication, they try to make up for that with passion and perseverance. What makes it interesting is that the malicious activity went on for over a year, before a third-party threat observer flagged it. Post-pandemic, APT activities have not just increased but also shown an inclination towards integrating online disinformation into the malware capabilities [21]. APT actors (and bots), who have increasingly gotten better at hiding in plain sight over social networks, have now a variety of AI techniques to integrate into their command and control - we've seen the use of GANs to mimic traffic of popular social media sites for hiding command and control traffic [22], an loT botnet that had a machine-learning component which the attacker could switch on/off depending upon people's responses in online social networks [21], as well as malware that can "autonomously" locate its command and control node over public communication platforms without having any hard-coded information about the attacker [23].

Post-pandemic, APT activities have not just increased but also shown an inclination towards integrating online disinformation into the malware capabilities.

This is an offence-persistent environment. In this "space", there always exists an information asymmetry where the defender generally knows less about the attacker than the opposite being true. Wargaming results have shown that unlike conventional conflicts, where an attack induces the fear of death and destruction, a cyber-attack generally induces anxiety [24], and consequently, people dealing with cyber attacks act to offset those anxieties and not their primal fears. Thus, in response to cyber-attacks, their policies reflect risk aversion, not courage, physical or moral. It need not be the

case if policymakers recognise this and integrate it into their decision-making heuristics. Unfortunately, the National Cybersecurity Policy released in 2013 stands out to be a fairly risk-averse and a placeholder document. Among many other, key issues are:

- The policy makes zero references to automation and AI capabilities. This would have been understandable in other domains, like poultry perhaps, but is not even comprehensible in present-day cybersecurity.
- The policy makes zero references to hardware attacks. Consequently, developing any capability for assessing insecurity at hardware/firmware levels, which is a difficult job, is also overlooked at the national level itself.
- There are several organisations within the state, civilian and military, that have stakes and roles of varying degrees in a robust National Cybersecurity Policy. However, the policy makes zero attempts at recognising and addressing these specific roles and responsibilities, or any areas of overlap therein.
- The policy does not approach cyber activity as an overarching operational construct which permeates all domains, but rather as activity in a specific domain called "cyberspace". Consequently, it lacks the doctrinal thinking that would integrate cyber capabilities with the use of force. A good example of this is outer space, where cyber capabilities are emerging as a potent destabiliser [25] and cybersecurity constitutes the operational foundation of space security, again completely missing from the National Cybersecurity Policy.
- The policy is also light on subjects critical to cybersecurity implementation, such as the approach towards internet governance, platform regulation, national encryption regime, and the governance of underlying technologies.

A Note on the Human Dimension of Cybersecurity

There exist two very broad types of malicious behaviour online, one that is rapid and superficial, and another that are deep and persistent. The present approaches to building situation awareness in cyberspace are geared towards the former, leading to spatiotemporally "localised and prioritised" assessments [26], matters pertaining to the immediate law and order situations and not stealthy year-long campaigns. Thus, while situation awareness itself is a psychological construct dealing with decision-making, in cybersecurity operations it overwhelmingly has turned into software-based visualisation of the incoming situational data. This is a growing gap which must also

be addressed by the National Cybersecurity Policy.

In technology-mediated environments, people have to share the actual situation awareness with the technology artefacts [27]. Complete dependence on technology for cyber situation awareness has proven to be problematic, for example in the case of Stuxnet, where the operators at the targeted plant saw on their computer screens that the centrifuges were running normally, and simply believed that to be true. The 2016 US election interference only became clearer at the institutional level after several

The use of computational tools and techniques to automate and optimise the social interactions of a software agent presents itself as a significant force multiplier for cyber threat actors.

months of active social messaging and doxing operations had already been underway [28], and the story of Telebots' attack on Ukrainian electricity grids is even more telling - a powerplant employee whose computer was being remotely manipulated, sat making a video of this activity, asking his colleague if it could be their own organisation's, IT staff "doing their thing" [29].

This lack of emphasis on human factors has been a key gap in cybersecurity, which APTs never fail to exploit. Further, such actors rely upon considerable social engineering in initial access phases, a process which is also getting automated faster than policymakers can play catchup to [30]. The use of computational tools and techniques to automate and optimise the social interactions of a software agent presents itself as a significant force multiplier for cyber threat actors. Therefore, it is also paramount to develop precise policy guidelines that implement the specific institutional structures, processes, and technological affordances required to mitigate the risks of malicious social automation on the unsuspecting population, as well as on government institutions.

Concluding Remarks

There is a running joke that India's strategic planning is overseen by accountants and reading through the document of National Cybersecurity Policy 2013, that does not seem surprising. We have had a troubling policy history when it comes to electronics and communications and are still in the process of shedding our colonial burden. A poorly framed National Cybersecurity Policy will only take us away from self-reliance in cyberspace and towards an alliance with principal offenders themselves. Notwithstanding, an information- abundant organisation like NCCC has undoubtedly to make some choices about where and what to concentrate its attentional resources upon, however, the present National Cybersecurity Policy appears neither to be a component of any broader national security

strategy nor effective or comprehensive enough for practical implementation in responding to the emerging threat environment.

References

[1] N. Alawadhi, “Cyber security policy must be practical: Experts,” The Economic Times, Oct. 22, 2014. Accessed: CSep. 14, 2022. [Online]. Available: https://economictimes.indiatimes.com/tech/internet/cyber-security-policy-must-be-practical-experts/articleshow/44904596.cms[2] A. Saksena, “India Scrambles on Cyber Security,” The Diplomat, Jun. 18, 2014. https://thediplomat.com/2014/06/india-scrambles-on-cyber-security/ (accessed Sep. 18, 2022). [3] C. R. Mohan, “Snowden Effect,” Carnegie India, 2013. https://carnegieindia.org/2013/06/19/snowden-effect-pub-52148 (accessed Sep. 18, 2022).

[4] R. Dharmakumar and S. Prasad, “Hackers’ Haven,” Forbes India, Sep. 19, 2011. https://www.forbesindia.com/printcontent/28462 (accessed Sep. 18, 2022).

[5] D. Karthik and R. S. Upadhyayula, “NASSCOM: Is it time to retrospect and reinvent,” Indian Inst. Manag. Ahmedabad, 2014.

[6] H. C. Fanshawe, Delhi past and present. J. Murray, 1902.

[7] C. Simms, “Is Social Engineering the Easy Way in?,” Itnow, vol. 58, no. 2, pp. 24-25, 2016.

[8] J. Lienhard, “No. 1380: Indian telegraph,” Engines Our Ingen., 1998.

[9] A. Vatsa, “When telegraph saved the empire - Indian Express,” Nov. 18, 2012. http://archive.indianexpress.eom/news/when-telegraph-saved-the-empire/1032618/0 (accessed Sep. 17, 2022).

[10] L. Hoskins, BRITISH ROUTES TO INDIA. ROUTLEDGE, 2020.

[11] D. R. Headrick, The invisible weapon: Telecommunications and international politics, 1851-1945. Oxford University Press on Demand, 1991.

[12] B. Parthasarathy, “Globalizing information technology: The domestic policy context for India’s software production and exports,” Iterations Interdiscip. J. Softw. Hist., vol. 3, pp. 1-38, 2004.

[13] I. J. Ahluwalia, “Industrial Growth in India: Stagnation Since the Mid-Sixties,” J. Asian Stud., vol. 48, pp. 413-414, 1989.

[14] R. Subramanian, “Historical Consciousness of Cyber Security in India,” IEEE Ann. Hist. Comput., vol. 42, no. 4, pp. 71-93, 2020.

[15] C. Wiener, “Penetrate, Exploit, Disrupt, Destroy: The Rise of Computer Network Operations as a Major Military Innovation,” PhD Thesis, 2016.

[16] N. Kshetri, “Cybersecurity in India: Regulations, governance, institutional capacity and market mechanisms,” Asian Res. Policy, vol. 8, no. 1, pp. 64-76, 2017.

[17] MeitY, “National Cybersecurity Policy.” Government of India, 2013.

[18] MHA, “NATIONAL INFORMATION SECURITY POLICY AND GUIDELINES.” Government of India, 2014.

[19] S. Patil, “Cyber Attacks, Pakistan emerges as China’s proxy against India,” Obs. Res. Found., 2022.

[20] A. Malhotra, V. Svajcer, and J. Thattil, "Operation 'Armor Piercer:' Targeted attacks in the Indian subcontinent using commercial RATs," Sep. 23, 2021. http://blog.talosintelligence.com/2021/09/operation-armor-piercer.html (accessed Sep. 02, 2022).

[21] NISOS, "Fronton: A Botnet for Creation, Command, and Control of Coordinated Inauthentic Behavior." May 2022.

[22] M. Rigaki, "Arming Malware with GANs," presented at the Stratosphere IPS, Apr. 2018. Accessed: Oct. 19, 2021. [Online]. Available: https://www.stratosphereips.org/publications/2018/5/5/arming-malware-with-gans

[23] Z. Wang et al., "DeepC2: AI-Powered Covert Command and Control on OSNs," in Information and Communications Security, vol. 13407, C. Alcaraz, L. Chen, S. Li, and P. Samarati, Eds. Cham: Springer International Publishing, 2022, pp. 394-414. doi: 10.1007/978- 3-031-15777-6_22.

[24] J. Schneider, "Cyber and crisis escalation: insights from wargaming," 2017.

[25] J. Pavur, "Securing new space: on satellite cyber-security," PhD Thesis, University of Oxford, 2021.

[26] U. Franke and J. Brynielsson, "Cyber situational awareness - A systematic review of the literature," Comput. Secur., vol. 46, pp. 18-31, Oct. 2014, doi: 10.1016/j.cose.2014.06.008.

[27] N. A. Stanton, P. M. Salmon, G. H. Walker, E. Salas, and P. A. Hancock, "State-of- science: situation awareness in individuals, teams and systems," Ergonomics, vol. 60, no. 4, pp. 449-466, Apr. 2017, doi: 10.1080/00140139.2017.1278796.

[28] "Open Hearing On The Intelligence Community's Assessment on Russian Activities and Intentions in the 2016 U.S. Elections." Jan. 10, 2017. Accessed: Dec. 22, 2021. [Online]. Available: https://www.intelligence.senate.gov/hearings/open-hearing-intelligence-communitys-assessment-russian-activities-and-intentions-2016-us#

[29] R. Lipovsky, "Tactics, Techniques, and Procedures of the World's Most Dangerous Attackers," presented at the Microsoft BlueHat 2020, 2020. [Online]. Available: https://www.youtube.com/watch?v=9LAFV6XDctY

[30] D. Ariu, E. Frumento, and G. Fumera, "Social engineering 2.0: A foundational work," in Proceedings of the Computing Frontiers Conference, 2017, pp. 319-325.

ABOUT THE AUTHOR

Shashank Yadav is currently pursuing his PhD at IIT Mumbai. His area of research relates to social botnets, AI governance and security.