KAUTILYA
SCHOOL OF
PUBLIC POLICY

Issue Brief Series

Paradox of Digital Literacy and Cybercrime in the Education Sector

Submitted by: Tanya Gupta (MPP Cohort 2025-27)

Under the Supervision of: Dr. Jandhyala B. G. Tilak, Visiting Faculty, Kautilya School of Public Policy

Cite this report as: Gupta, T. (2026) "Paradox of Digital Literacy and Cybercrime in the Education Sector" [online]. Available at: https://www.kspp.edu.in/issue-brief/paradox-of-digital-literacy-and-cybercrime-in-education-sector

Paradox of Digital Literacy and Cybercrime in the Education Sector

Abstract

This paper argues that India's digital turn in education has produced a paradox: the same expansion of digital literacy and infrastructure that democratises learning has also amplified the scale, sophistication and frequency of cybercrime against and from within the education sector. It points out the cyber deficiencies in the education sector to understand why the sector is one of the most attacked ones in India. Further, it analyses the paradoxical impact by drawing on anecdotal incidents and proposes practical and aspirational solutions.

Methodology

The paper uses a qualitative, interpretive methodology grounded in secondary data analysis and illustrative case-based reasoning. Due to the dearth of literature, it synthesises existing empirical studies, policy documents, official statistics and media reports to theorise the paradoxical relationship between digital literacy, technical education and cybercrime in India's education sector.

Introduction

In the digital era, the integration of technology into education is both indispensable and fraught with challenges. The environment of interactive learning enhances information accessibility, and endeavours to create a level-playing field to ensure equitable educational outcomes across socio-economic and neurodiverse strata. However, this technological integration renders educational institutions vulnerable to cybersecurity threats, including data breaches, hoax bomb alerts, and other cybercrimes, for which many lack adequate preparedness.

Consider, for instance, a classroom in rural Rajasthan, where a student logs into a government-backed website to access e-learning resources, unlocking interactive modules on quantum physics that were historically the privilege of the urban elite institutions. This scene, emblematic of India's digital transformation in education through the National Education Policy 2020, embodies hope. The surge in digital literacy through e-learning modules, virtual classrooms and artificial intelligence learning tools, has democratised education by making it reach the last mile. Yet, the same digital ecosystem serves as a conduit for malicious cyber activities.

The Threat Intelligence Report for India by the Check Point Software Technologies, a partner organisation of the World Economic Forum, revealed that the education sector in India is the most targeted industry. It faces 7,095 attacks per week, per educational institution, which is higher than the national average of 3,233 per week, and the global average of 2,002 per organisation.[1] Thus, digital transformation has magnified sector-specific vulnerabilities, stemming from an expanded digital footprint that generates a large number of data repositories for exploitation, and a weak cyber defence.

A closer examination reveals a paradoxical situation. The digital literacy, intended to empower, inadvertently fuels cybercrime. The sophisticated nature of the crime requires advanced technical skills. Thus, the proliferation of technology-focused education has unintentionally expanded the cadre of potential cyber-offenders in India, making India one of the top exporters of cybercrime in the world (Ebert, 2020).

Therefore, digital literacy and cybercrime share a symbiotic relationship where one fosters a conducive environment for the other to prosper. This has a direct impact on the digital ecosystem of the country, making digitalisation a wicked problem, rather than a solution. Further, it questions the credibility of education itself. Does this mean we limit technical education or the process of digitalisation? Neither. The solution lies in breaking this cycle through socio-economic empowerment of the education sector to build a strong cyber defence, and a workforce that accredits this cyber defence.

Literature Review

Cybersecurity Deficiencies in the Education Sector

In order to understand the impact of cybercrime on the education sector, it is important to understand the cybersecurity deficiencies which render the sector vulnerable. These deficiencies can be broadly classified as follows:

Proliferation of digital learning endpoints: The adoption of new technologies in the education sector has increased the endpoints manifold, creating a complex education network. These endpoints are determined by the teledensity and internet penetration in the country. Teledensity is defined as the number of telephone connections per 100 people in a specific area, and internet penetration is defined as the percentage of a country's or region's

[1] ETCISO Desk (2025), 'India's education sector faces 7,095 weekly cyberattacks: Check point,' The Economic Times https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/indias-education-sector-faces-7095-weekly-cyberattacks-check-point/124448887

total population that has access to or uses the internet. As per the Telecom Regulatory Authority of India, the teledensity in India is 84.85 per cent as of January 2025.[2] Meanwhile, as per the Comprehensive Modular Survey 2025 under the 80th National Sample Survey, around 86.3 percent households in India have access to the internet within the household premises.[3] Thus, the exposure of the society to infrastructural advancements has amplified the number of digital endpoints, thereby enhancing vulnerability.

When we come to the digital learning endpoints, we observe a distinction between pre-pandemic and post-pandemic levels in terms of digital accessibility. In 2020, Smile Foundation, a child rights NGO conducted a study called 'Scenario amidst COVID 19 – Onground Situations and Possible Solutions' to understand access to technology. As per their survey, 56.01 per cent of children had no access to smartphones during the pandemic, showcasing the digital divide that became apparent when digital education was being promoted in the country.[4] However, as per the Annual Status of Education Report (ASER) 2024, 90 per cent of the surveyed children reported to have access to smartphones at home, with 57 per cent of them utilising them for educational purposes.[5] These statistics show that the number of endpoints in digital education have increased when compared to pre-pandemic levels. This can be attributed to the emergence and adoption of new learning technologies like remote learning through pre-stored content on devices, online learning through real-time classes, and AI-based applications for easy comprehension and structured learning. While these technologies enhanced last mile academic connectivity during the pandemic, it birthed a population unprepared to interact with digital devices, making them vulnerable to

---

[2] 'Highlights of Telecom Subscription Data as on 28th February 2025,' Telecom Regulatory Authority of India https://www.pib.gov.in/PressReleasePage.aspx?PRID=2124081&reg=3&lang=2

[3] 'Results of Comprehensive Modular Survey: Telecom, 2025' https://www.pib.gov.in/PressReleasePage.aspx?PRID=2132330&reg=3&lang=2

[4] 'About 56% of children have no access to smartphones for e-learning: Study,' (2020) Smile Foundation https://www.smilefoundationindia.org/about-56-of-children-have-no-access-to-smartphones-for-e-learning-study/

[5] Mufti, I. (2025), 'Only 57% teens use smartphones for study: ASER,' The New Indian Express https://www.newindianexpress.com/nation/2025/Jan/29/only-57-teens-use-smartphones-for-study-aser

cybercrime.

Fiscal and infrastructural constraints: Budgetary constraints within the education sector engender vulnerabilities creating 'soft targets' that cybercriminals prefer. The institutions digitize and generate data faster than their capacity to implement robust security measures. As Vineet Kumar, founder of CyberPeace, says, "Digitisation without cybersecurity is like building a house without doors or locks" (Pandey, 2025). Just like doors and windows are considered as discretionary extras rather than core infrastructural elements of a house, expenditure on cybersecurity is categorised as an accessory, facilitating cybercrimes like data theft, denial of service and phishing which become easy to execute.

In India, government expenditure on education constitutes 1.02 per cent of its Gross Domestic Product, out of which technical education accounts for 4.76 per cent only.[6] Consequently, many schools and universities function on obsolete hardware and software. The budgetary priorities emphasize foundational elements like connectivity, personnel salaries, and physical infrastructure over security enhancements or vulnerability assessments. Although the 'Union Budget 2025' has allocated Rs 19,000 crore for national cybersecurity initiatives,[7] the proportion allocated to the education sector remains indeterminate. Moreover, the absence of empirical data on the amount spent by educational institutions on cybersecurity tools like anti-virus software underscores the marginal prioritisation of cybersecurity within sector budgets.

With the advent of artificial intelligence as a supplementary teaching tool in classrooms, the lack of investment in building cyber-resilience through training and software updates would exacerbate the problems of cybercrime. According to the UDISE report for 2023-24, only 26.77 per cent of India's school teachers have been trained in computer-based teaching. On reading this in conjunction with a survey conducted by the Centre for Teacher Accreditation (CENTA), which says that in India, while 90 per cent of the teachers use AI tools in the classroom, only 57 per cent can identify an AI misconception , we can understand

---

[6] Analysis of Budget Expenditure on Education 2019-20 to 2021-22 (2024), Ministry of Education, Government of India https://www.education.gov.in/sites/upload_files/mhrd/files/statistics-new/budget_exp_2020_22.pdf

[7] Dhar, R. (2025), 'Union Budget 2025 Prioritizes Cybersecurity Amid Rising Threats,' Frost & Sullivan https://www.frost.com/uncategorized/union-budget-2025-prioritizes-cybersecurity-amid-rising-threats/

the dire need for investment in the digital as well as AI literacy of the guardians.

Gaps in policy frameworks: India has a policy framework for cybersecurity known as the National Cybersecurity Policy 2013 which not only recognises education as an important sector for digital expansion, but also aims to create a trust-based digital ecosystem. However, these guidelines are generic and normative in nature, making implementation and evaluation challenging. The lack of cyber safety standards in the educational institutions and the lack of penalties in case of non-enforcement of advisories provided by CERT-In, NCERT and Cyber Swachhta Kendra, reveal fissures in the policy cycle.

Further, there is an absence of policy-driven national structure for real-time threat intelligence sharing between educational institutions and the government department, leaving gaps in coordinated responses to cyber threats. In 2025, the government of the National Capital Territory of Delhi, rolled out a comprehensive 'Standard of Procedure (SOP) for managing bomb threats in schools.'[8] While the policy addresses the significance of inter-departmental coordination during the evacuation, it fails to address its significance in the identification of threat itself. Therefore, India's policy focus remains on a risk-based and curative approach to cybercrime, rather than a preventive one.

Inherent structural fragmentations: As per the 'Unified District Information System for Education (UDISE) Plus,' a data platform functioning within the Ministry of Education, 'only 57.2 per cent of schools in the country have functional computers and 53.9 per cent have Internet access.'[9] This often compels students and teachers to use their personal devices to avoid latency caused by obsolete hardware and software. These external devices could carry malware, making the organisation as a whole vulnerable to large-scale ransomware attack.

Further, large educational institutions have departments which function autonomously, making centralisation of the security system difficult. Decentralised structures

---

[8] ET Education (2025) Delhi govt issues SOP for handling bomb threats in schools, The Economic Times https://education.economictimes.indiatimes.com/news/school-education/delhi-govt-issues-sop-for-handling-bomb-threats-in-schools/121266961

[9] The Hindu Bureau (2025), '57% schools have functional computers, 53% have Internet access: Education ministry,' The Hindu https://www.thehindu.com/education/57-schools-have-functional-computers-53-have-internet-access-education-ministry/article69053427.ece

often create traceability issues, lack of implementation of standardised protocols and information asymmetry. It also fosters an environment of weak passwords due to the unavailability of the password-holding entity at times. This makes it easy for AI systems to study the patterns of password changes and predict them, providing easy access to cybercriminals. As a part of the e-Kawach Project, CyberPeace conducted a study which found that the most used passwords were '123', '1234', '12345', '123456', '1234567', and '12345678' (Kumar, 2024).

Findings & Analyses

Impact of Cybercrime on Education Sector

Cybercrime has socio-economic and psychological impact on the policy actors involved in the education sector directly and indirectly. Such cybercrime activities precipitate data breaches, financial exigencies, disruptions to educational activities, diminished educational outcomes and loss of trust in the educational institutions.

*Impact on psychological vulnerability of students***:** In the contemporary digital era, students' interaction with cyberspace has a profound impact on their psychological well-being. Being a victim to cybercrime can lead to deteriorated mental and emotional health, potentially culminating into suicidal thoughts and Post Traumatic Stress Disorder (PTSD) (Pant & Chaubey, 2024). Given the emotional naivety of children compared to adults, cybercriminals prey on their emotions of fear, anger, guilt, embarrassment and excitement with relative ease, thereby elevating susceptibility to targeted cyberattacks.

For example, in 2023, educational institutions in the border villages, including the chain of Army Public School, faced cyberattacks by Pakistan Intelligence Operatives (PIO). PIOs contacted the students through WhatsApp, masquerading as teachers to extract sensitive information about the students and their guardians, leveraging the proximity of these institutions to sensitive facilities as a 'strategic advantage' to gain access to critical infrastructure.[10] The children who engaged in these conversations were direct casualties of cybercrime of identity theft and privacy intrusion. Being closely linked to national security, the negative emotions caused by cybercrime get magnified fostering iterative and vicious cycles of self-blame, self-shame and self-harm. Consequently, the victims of such forms of

[10] 'How Pakistan is targeting students from army schools in India to seek sensitive info (2023),' Firstpost https://www.firstpost.com/explainers/how-pakistan-is-targeting-students-from-army-schools-in-india-to-seek-sensitive-info-12916342.html

cyberviolence may experience social disengagement, low self-esteem, perpetual feeling of fear, elevated tension, aversion to technology and constant anxiety (Pant & Chaubey, 2024), which have a direct impact on their academic performance. This vulnerability is further exacerbated by email-based bomb threat hoaxes targeting schools, where abrupt evacuations engender fear and a feeling of mistrust on their learning institutions. Frequent instances often cause PTSD, school avoidance or school-phobia and chronic anxiety among students.[11]

Moreover, psychological vulnerability of students, especially in primary and secondary levels of education, has been augmented in the post-pandemic period amid increased exposure to digital devices without adequate safeguards and cyber awareness. Concurrently, the emergent educational technologies, while transformative, may disrupt neurocognitive development of students, impeding attentional competence, processing speed, verbal intelligence, high-order thinking, long-term memory and sustained attention capabilities (Jha & Arora, 2020). The simultaneous occurrence of the two has a multiplication effect on psychological vulnerability of the students.

Quantification of education disruptions: It is well-known that cybercrime has an effect on the educational outcomes as it undermines students' cognitive efficacy and output. As we observed above, its role in advancing psychological vulnerabilities impacts the productivity and efficiency of the students. Over time, this trajectory may widen global learning gaps in terms of employability and socio-economic mobility.

In Delhi NCR, for instance, 2025 witnessed a surge in privacy-compromising bomb threat hoaxes. Through various news reports, the impact of these bomb threats on the number of school days lost can be calculated. In 2024, the Directorate of Education directed the schools in all districts to ensure a minimum of 220 working days for students for upper primary classes, in accordance with the Right to Education Act 2009.[12] In 2025, schools across Delhi NCR faced bomb threat emails hampering them to function on approximately 20

---

[11] Chauhan, P. (2025), 'Delhi schools face bomb threat scare, experts warn lasting impact: Say, 'Children may avoid classes, need counselling, resilience and better cyber safety',' Bhaskar English https://www.bhaskarenglish.in/local/new-delhi/news/experts-warn-bomb-threats-in-delhi-anxiety-schools-spark-lasting-135836956.html

[12] Mufti, I. (2024) 'Education department directs Delhi schools to adhere to 220 working days,' The New Indian Express https://www.newindianexpress.com/cities/delhi/2024/Dec/10/education-department-directs-delhi-schools-to-adhere-to-220-working-days

days of the year.[13] Mathematically, this accounts for a loss of 9.09 per cent of effective schooling days. This metric, however, understates ancillary losses like fear-induced absenteeism in the wake of repeated instances.

Impact on administrative efficiencies: Apart from data breach and ransomware, cybercrime includes distributed denial-of-service attacks and social engineering tactics which reduce the efficiency of educational institutions. These incursions not only signal security lacunae but also strategically impede public service provision. For example, in 2025, the Rajasthan Education Department's website was hacked, and messages were displayed to incite violence.[14] During those hours, the website was inaccessible for public delivery services. Further, it diverted the attention of the department on the crime, rather than engaging in education itself. It was also assumed that several other websites of the department were hacked into by cybercriminals to propagate vitriolic content targeted at students. Such instances divert administrative bandwidth from pedagogy to incident response.

Similar patterns have been observed in the edtech startups as well. The breach of data from Vedantu in 2019, Unacademy in 2020[15] and Byju's in 2021[16] point out the systemic frailties that lie in conventional and non-conventional forms of education services. Often hailed as a saviour of the students from the redundant conventional education, these platforms democratise education by ensuring access to all. Yet, the subsequent breach of data and privacy invasion led to acute reputational erosion and confidence among students and their guardians. Ultimately, such administrative inefficiencies and compromised security inflict a collateral toll on the digital transformation as well as the broader education ecosystem.

---

[13] Dates: January 8, January 9, February 5, February 7, May 1, July 14, July 15, July 16, July 18, August 18, August 20, September 20, September 28, October 17, October 24, November 13, November 18, November 20, December 10 and December 19

[14] Asnani, R. (2025) 'Rajasthan Education Department website hacked; message from 'Pakistan Cyber Force' displayed,' The New Indian Express https://www.newindianexpress.com/nation/2025/Apr/29/rajasthan-education-department-website-hacked-message-from-pakistan-cyber-force-displayed

[15] Ahaskar, A. (2020) 'Millions of Unacademy user accounts exposed in data breach: Report,' mint https://www.livemint.com/technology/tech-news/over-20-mn-unacademy-user-accounts-exposed-in-data-breach-report-11588775083410.html

[16] Singh, J. (2023) 'Byju's exposed sensitive student data, including loan details,' TechCrunch https://techcrunch.com/2023/08/25/byjus-student-data-exposed/

Erosion of institutional trust: With increasing instances of cybercrime in educational spaces, guardians are becoming averse to the idea of using digital tools in educational institutions. Guardians become hesitant in allowing the integration of technology in schools. With bomb hoax and data breach becoming a reality, guardians are 'torn between academic continuity and their child's safety.' Many schools in Delhi NCR have reported 10-15 per cent reduction in attendance as an aftermath of bomb threat hoax.[17] This erosion of institutional trust is worrisome as it questions the credibility of the education system itself.

In 2024, hidden cameras were found in the women's washrooms of the hostels of an engineering college in Andhra Pradesh, yielding deepfake pornography for commercial exploitation.[18] Such incidents have a gendered impact on the education system, making it difficult for women to pursue higher education. These events act as discouraging instances for guardians to consider while 'allowing' their children to pursue tertiary education. The absence of choice and mobility in education perpetuates a cycle of lost opportunities and low-income employability for women in the country. A similar incident occurred in 2025, where CCTV footage of approximately 80 dashboards from schools and other critical institutions were hacked and sold to a pornographic website.[19] Such instances reflect poor security stewardship to the guardians. Moreover, with elevated media scrutiny, lawsuits and loss of social capital, the reputation of educational institutions is jeopardised.

Economic repercussions: Broadly, cybercrime exacts a macroeconomic toll. According to the Indian Cyber Crime Coordination Centre (I4C), an organisation within the Union Ministry of Home Affairs (MHA), cyberfrauds could amount to 0.7 per cent of the

---

[17] 'Low attendance in Delhi schools day after bomb scare; principals revisit evacuation plans for future' (2025), The Hindu https://www.thehindu.com/news/cities/Delhi/low-attendance-in-delhi-schools-day-after-bomb-scare-principals-revisit-evacuation-plans-for-future/article68131285.ece

[18] 'Hidden Camera Scandal In Andhra Engineering College, Minister Orders Inquiry' (2024) NDTV https://www.ndtv.com/india-news/hidden-camera-found-in-andhra-college-videos-were-sold-to-students-6450297

[19] 'Inside India's voyeur web: 80 CCTV dashboards hacked across 20 states; hospitals, schools, homes streamed to porn channels; 50,000 clips sold' (2025), The Times of India https://timesofindia.indiatimes.com/city/rajkot/inside-indias-voyeur-web-80-cctv-dashboards-hacked-across-20-states-hospitals-schools-homes-streamed-to-porn-channels-50000-clips-sold/articleshow/125073851.cms

country's GDP. Ironically, this figure is closer to the education outlays in India. Within the education sector, such depredations manifest as resource reallocation. There are no audits which determine the exact cost of cybercrime on the Indian educational institutions. Extrapolating from global benchmarks, 'lower-education organizations report a mean cost of USD 3.76 million to recover from a ransomware attack in 2024.'[20] Therefore, diversion of resources could have a negative impact on the operational efficiency of the institutions as well as the educational outcomes.

Impact of Advancement in Technical Education on Cybercrime

While cybercrime has a deleterious impact on the education system, the converse dynamic is equally salient. Advancement in technology as well as technical education, primarily aimed to build a skilled workforce and foster high-order thinking, creates a double-edged sword. On one hand, these advancements yield a cadre of cybersecurity professionals adept to mitigate the threats of cybercrimes. On the other hand, these advancements provide an opportunity as well as the knowledge to the people to weaponise these technologies for malicious purposes.

Routine Activity Theory (RAT) states that 'a crime occurs when three elements converge temporally and spatially: a motivated offender, a suitable target and the absence of a capable guardian' (Cohen & Felson, 1979). Rising unemployment motivates an offender to execute a cybercrime, digital expansion and low psycho-economic barriers create suitable targets, and the absence of robust security barriers in terms of awareness and policy aid in seamless execution of cybercrime. This theoretical lens illuminates the paradoxical relationship between digital literacy and cybercrime via two principal contentions. First, the 'Offender Argument' which says that higher education and employability gap equips people with the necessary tools to commit sophisticated crimes, corroborates the motivation aspect of the theory. Second, the 'Victim Argument', which says that a higher educated population tends to engage more with technology, creating target pools amid guardian deficits (Anthony, 2025).

Rising unemployment: Traditional crime models, like Merton's Strain Theory (1938), predict 'a positive relationship between unemployment and criminal activity, as economic hardships act as a motivation for individuals to seek illicit sources of income for themselves

[20] Gregory, J (2025) 'Reducing ransomware recovery costs in education,' IBM https://www.ibm.com/think/insights/reducing-ransomware-recovery-costs-in-education

and their families' (Anthony, 2025). When technical education fails to deliver anticipated employability, it inadvertently channels graduates toward cybercrime, a domain characterized by elevated profitability and negligible operational expenditures relative to its exploitable scale. In India, nearly 83 per cent of engineering graduates fail to secure employment or an internship after graduation. This is because of the rising employability gap. The students possess the required formal education, but do not possess dynamic skills that make them relevant in the contemporary job market. This communicates an outdated syllabus and irrelevant pedagogy of the education system in India. Therefore, 73 per cent companies today, prefer recruiting students with hands-on experience and relevant skills over college pedigree.[21]

There is a direct link between rising unemployment and cybercrime. The paradox of high Gross Domestic Product (GDP) growth and scarcity of jobs push cyber skilled individuals into the arena of cybercrime. Even if these individuals are employed, they remain underpaid.[22] In 2023, Sukhdev Vaid, 24, of Haryana pleaded guilty in a cyber fraud case tried at Montana, USA for targeting elderly people as a side hustle to earn more money.[23] This is not an isolated incident, but points to a broader employment malaise aggravated during the pandemic. According to a survey conducted by Centre for Monitoring Indian Economy, 41.2 per cent of the people surveyed were unemployed between December 2019 and April 2020. For the population between 15-24 years, this number rose up to 58.5 per cent.[24] Therefore,

---

[21] Sharma, N. (2025) 'Why are so many of India's 1.5 million fresh engineers every year unemployable?' Forbes India https://www.forbesindia.com/article/upfront/column/why-are-so-many-of-indias-1-5-million-fresh-engineers-every-year-unemployable/2988705/1

[22] Tewari, T (2025) 'Engineers are underpaid and unemployed: Is engineering obsession breaking its promise?', The Times of India https://timesofindia.indiatimes.com/education/news/engineers-are-underpaid-and-unemployed-is-engineering-obsession-breaking-its-promise/articleshow/122877637.cms

[23] 'India-based computer-hacking scam that targeted elderly across the country and stole $150,000 from a Kalispell woman sends Indian national to prison for more than four years' (2024), District of Montana, United States Attorney's Office https://www.justice.gov/usao-mt/pr/india-based-computer-hacking-scam-targeted-elderly-across-country-and-stole-150000

[24] Farcis, S. (2021) 'India's youth: Hit hard by the pandemic,' The UNESCO Courier https://courier.unesco.org/en/articles/indias-youth-hit-hard-

switching to cybercrime during a crisis is viewed as a survival strategy for the youth rather than an intentional venture.

Today, the youth of the country faces challenges of employability despite substantial educational investments. This employability gap professionalises cybercrime as an underground gig economy, an avenue for skilled graduates to earn disposable income, and in some cases pay off educational loans. It could also give rise to 'cyber slavery', where skilled individuals are initially coerced into the facilitation of cybercrime, but gradually start liking it due to the financial incentives, elevation of social status and standard of living, and perceived security provided by digital anonymity (Sarkar & Shukla, 2025). To put this into perspective, 'India lost Rs. 22,845.73 crore to cyber criminals in 2024 and Rs 7,465.18 crore in 2023', as reported by the Ministry of Home Affairs.[25] Such outcomes interrogate the socioeconomic returns of education: if formal qualifications yield neither employment nor stability, their instrumental value warrants re-evaluation.

Low psycho-economic barriers: Another reason why cybercrime is directly impacted by education is due to the low entry barriers in the former. The Government of India has taken several measures to enhance the quality of 'Science, Technology, Engineering & Mathematics (STEM) education' in India, which can be seen in the National Education Policy 2020 explicitly.[26] Financial benefits provided by the All India Council for Technical Education (AICTE) foster youth participation in the STEM fields, as historically as well, these fields perform better than humanities in terms of employment opportunities and labour market outcomes. Providence of technical education does not factor in the intention of the student behind pursuing the said form of education. With the advent of digitalisation and artificial intelligence tools, technical education has become universal, accessible, available and affordable. Digitalization and artificial intelligence (AI) render technical proficiency ubiquitous, cost-effective, and unmonitored—precluding panoptic surveillance of knowledge

---

pandemic#:~:text=Urban%20youth%20on%20the%20front%20line&text=According%20to%20a%20three%2Dyear,people%20aged%2015%20to%2024.

[25] Bhushan, K. (2025) 'India's Financial Fraud Risk Indicator Helps Prevent INR 660 Crore Cyber Fraud Losses in Just 6 Months,' India Entrepreneur https://www.entrepreneur.com/en-in/technology/indias-financial-fraud-risk-indicator-helps-prevent-inr/501227

[26] PIB (2025) 'Higher education institutions in the country in STEM,' Ministry of Education https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2114326&reg=3&lang=2

application. Thus, learners may harness AI utilities for password circumvention, data exfiltration, or privacy encroachments with impunity.

However, there exists a rural-urban digital divide, due to geographic and infrastructural disparities, which modulates cybercrime sophistication. Rural populations with lesser formal education than urban populations engage in low-skill offences like phishing and fake recruitment drives rather than high-skill cybercrimes like ransomware attacks (Anthony, 2025). The 'Jamtara Model' is the case in point. The modus operandi of the youth belonging to the village in Jharkhand was simple, in line with their minimal formal education and short informal training in impersonation and social engineering techniques.[27]

Further, the opportunity cost for cybercrime is low. Models like Cybercrime-as-a-Service (CaaS) available for rent, inexpensive infrastructure and automation allows even novice hackers to conduct high-impact attacks. The high return on investment with a low conviction rate (1.6 per cent)[28] makes cybercrime a lucrative career prospect for skilled individuals to escape the corporate drudgery and meagre salaries; additional factors include remote execution, recession-proof nature of the cybercrime industry and availability of recreation time. In fact, the Rational Choice Theory of Becker (1968) states that offenders weigh costs and benefits such that crime becomes a calculated choice, rather than an irrational decision. With rising inflation, unemployment and digital expansion that outpaces security, legitimate incomes fail to keep pace with living costs, making cybercrime a calculated choice (Anthony, 2025).

However, one of the most significant factors that attracts skilled individuals towards cybercrime is the identity of the cyberspace itself. Cyberspace is identified as a resource based on authority, accessibility and anonymity. Thus, the individuals are under the impression that they have perpetual control over their finances through cyberspace, can access or commit any crime, and simultaneously remain anonymous. Since most cybercriminals follow a decentralised approach to crime in spatial and temporal context, traceability becomes difficult, creating a perception of anonymity, obfuscating public

---

[27] Srivastava, A. (2016), 'Phish pond,' India Today https://www.indiatoday.in/amp/magazine/nation/story/20160808-cyber-crime-jamtara-jharkhand-829309-2016-07-27

[28] Singh, A. (2024) 'Only 1.6% conviction rate in 2 yrs amid surge in cybercrime cases,' The Tribune https://www.tribuneindia.com/news/delhi/only-1-6-conviction-rate-in-2-yrs-amid-surge-in-cybercrime-cases/

scrutiny.

Student opportunism: The low entry barriers to technical education has given rise to amateur cyber incursions by students for personal gains. Even though these threats appear harmless and disregarded as childish & mischief, they take a toll on the educational institutions and other students. For instance, in 2025, a school in Delhi NCR faced a threat email by a student who later confessed to have sent it in order to avoid examinations. The confession came after the authorities were informed and evacuation had been carried out.[29] Such instances surface the lack of interdepartmental threat identification and communication systems in India.

Moreover, education is a long process that requires patience. Students who feel stuck in this lengthy process look for instant gratification provided by education. This is coupled with glamorisation of an individual's monetary value and overnight success stories on social media platforms. Students are enticed to participate in these online scam-events, in order to elevate their social worth among peers. Such behaviours of seeking peer validation also lead to cyber slavery, where one individual follows another into the pothole of cybercrime.

Recommendations

As educational institutions increasingly integrate digital technologies, the imperative to fortify cybersecurity becomes paramount. The digital tools in the education sector are going to benefit all stakeholders, provided they are used in a judicious manner. While complete eradication of cybercrime remains unattainable in an interconnected era, strategic interventions can attenuate vulnerabilities within the education sector, hoping for cascading benefits across broader socioeconomic domains.

Allocation of dedicated budgets for cybersecurity infrastructure: The foremost requirement of the government should be to acknowledge the occurrence of cybercrime in educational institutions and factor in the cost borne by the institutions during such attacks, while allocating annual budget. It is proposed that the union budget should include sector-wise distribution of funds earmarked for cybersecurity. In 2025, the Federal Communications Commission initiated the 'Schools and Libraries Cybersecurity Pilot Program' which

[29] 'Student sends bomb threat to school to avoid exams, apprehended' (2025), The Hindu https://www.thehindu.com/news/cities/Delhi/student-sends-bomb-threat-to-school-to-avoid-exams-apprehended/article70175815.ece

'provides up to USD 200 million to selected institutions over a three-year term to purchase a wide variety of eligible cybersecurity services and equipment.' The aim of the program is to identify the cybersecurity services required by these institutions, and whether they can be funded universally.[30] The government of India can emulate the program by identifying institutions that are equipped to understand the nuances of cybercrime and taking their help in deploying basic cybersecurity equipment in schools. Such a pilot program would reduce economic wastage and frame scalable solutions for cybersecurity.

In scenarios of fiscal shortfall, public-private partnerships (PPPs), as exemplified by Finland's collaborative cyber defense initiatives, Israel's innovation-driven security consortia, and Germany's federal-industry alliances, offer viable augmentation[31] Beyond cost-sharing, such collaborations align with Sustainable Development Goal (SDG) 17, fostering strengthened global partnerships for sustainable development.

Investment in Curriculum Research and Ethical Integration: Anthony (2025) provides empirical evidence showing that 'broad public spending on education does not exert a direct, short-term mitigating effect on cybercrime.' This is contrary to the popular belief that more education would reduce cybercrime. Therefore, the focus of education for reducing cybercrime needs to be on content-revision rather than haywired expenditure. Courses on cybersecurity, digital ethics, ethical hacking and the legal consequences that follow cybercrime need to be highlighted to mitigate the creation of skilled offenders through education, as identified by the National Education Policy 2020. In addition to this, the institutions need to conduct post-crime counselling sessions for students and guardians to maintain institutional trust, reduce fear and stabilise academic performance. For effective optimisation, students need to be consulted as significant stakeholders while curriculum

---

[30] Consumer and Government Affairs Bureau (2025), 'Schools and Libraries Cybersecurity Pilot Program,' Federal Communications Commission https://www.fcc.gov/cybersecurity-pilot-program

[31] Radunović, V. & Rüfenacht, D. (2016) 'Cybersecurity Competence Building Trends,' Diplo Foundation https://www.diplomacy.edu/wp-content/uploads/2019/02/Cybersecurity20Full20Report.pdf#:~:text=%E2%80%A6%20in%20cybersecurity%20as,and%20%E2%80%A6&text=ten%20OECD%20countries%20which,and%20%E2%80%A6&text=have%20approached%20cybersecurity%20education.,and%20%E2%80%A6&text=cutting%2Dedge%20knowledge%2C%20best%20practices%2C,and%20%E2%80%A6

designing. This would illuminate ground-level exigencies and provide legitimacy to the curriculum, thereby ensuring a high level of acceptance.

In 2023, Australia, India, Japan and the USA initiated Quad Cyber Challenge, following a multi-stakeholder approach to collaborate with students, civil society and private players in order to educate students and teachers about cyberthreats, and at the same time, invite simple and implementable measures from them.[32] Such coordinated and inclusive response creates a sense of shared understanding of the challenge, providing motivational impetus for collective comprehension among students to formulate solutions. Amid geopolitical tensions, such initiatives might get lost. Thus, the Education Departments of the Indian states can collaborate to conduct hackathons and invite research papers to find the most practical solutions to cyberthreats tailor-made to their specific regions.

Deployment of Cost-Effective Technological Interventions: Understanding the cost restraint in India, any technological solution needs to be cost-effective. Therefore, schools and universities can go for multi-factor authentication, maintenance of firewall, spam-proofing email ids and account lockout policies in their digital devices. Using artificial intelligence and machine learning, predictive analysis could be done to recognise the patterns of the cyberattacks and categorise them as low-risk or high-risk for future action. The AICTE Cybersecurity Strategy for Higher Education Institutions furnishes a normative blueprint, advocating tailored policies for student and institutional fortification. Implementation should emphasize interoperability and scalability, ensuring equitable access across urban-rural divides.

Refinement of Policy Frameworks for Coordinated Governance: India's cybersecurity architecture evinces maturity, securing a Tier-1 (Role-modeling) ranking with a score of 98.49 out of 100 in the Global Cybersecurity Index 2024 by the International Telecommunications Union.[33] The country shows excellent performance across legal, technical, capacity and cooperation pillars, falling short in the organisational domain. The 'Handbook on Basics of Cyber Hygiene for Higher Education Institutions' by the University

[32] Klein, A. (2023), 'Four Countries Want Students to Help Their Schools Fight Cyber Threats,' EducationWeek https://www.edweek.org/technology/four-countries-want-students-to-help-their-schools-fight-cyber-threats/2023/02

[33] Country Profile, Global Cybersecurity Index (2024) International Telecommunication Union https://www.itu.int/epublications/zh/publication/global-cybersecurity-index-2024/en

Grants Commission (UGC), operationalizes this foundation, prescribing hygiene protocols to embed resilience at institutional levels. Anchoring the stable institutional framework of India like National Security Council Secretariat and National Critical Information Infrastructure Protection Centre, operating directly under the Prime Minister's Office. Organisations like CERT-In, National Cyber Coordination Centre, C-DAC under the Ministry of Electronics & Information Technology, and I4C under the Ministry of Home Affairs, various initiatives like Cyber Swachhta Kendra and M-Kavach have been successful.

Notwithstanding these strengths, fragmented agency mandates risk procedural inertia and bureaucratic delays, impeding resilient responsive mechanisms for cyberthreat mitigation. The promulgation of the Digital Personal Data Protection (DPDP) Rules, 2025, augurs enhanced accountability in data stewardship, mandating encryption, 72-hour breach notifications, and stringent verification for sensitive information. Thus, India is required to focus on the policy implementation stage to ensure enhanced accountability in the policy evaluation stage of the policy cycle.

In essence, these recommendations integrate fiscal prudence in budgeting, innovative curricular reforms, pragmatic technological deployments, and harmonized policy frameworks to safeguard educational institutions against cyber threats. By adapting international best practices to India's distinct socioeconomic landscape, technical education can be repositioned from a victim of cybercrime to a robust defensive asset, fostering long-term societal resilience.

Limitations

This study provides an overview of how technical education and cybercrime connect in complex ways, but it has some clear limits worth noting. It mostly draws from secondary sources, like books, reports, and articles, which pull together existing ideas. Hence, it might carry over some biases from those original sources. The paper is based on observations made during anecdotal incidents which are helpful for showing patterns, but they're not backed by any long-term studies. This places the observations exclusively in the Indian context, which might not be applicable globally. For example, the rural-urban divide that pertains in India while accounting for the victims and perpetrators of cybercrime in the education sector. More broadly, they point to a key gap in research: we need more hands-on studies linking school programs directly to cybercrime paths which would give us practical tools to handle the risks of digital skills in our connected world.

Conclusion

Cybercrime is a 'self-reinforcing crime,' driven by entrenched criminal networks, the emulation of successful fraud models and relaxed adoption of suitable preventive measures by the institutions. This underscores the requirement of having a sustained and long-term policy strategy which focuses on dismantling the criminal ecosystem while improving deterrence (Anthony, 2025). In the intricate paradox of cybercrime and digital education, where online learning's democratizing force sparks innovation yet exposes users to rampant threats like phishing and data breaches, resilient education stands as the cornerstone of sustainable development. This duality erodes trust in vulnerable communities, hindering equitable growth, but it also signals a pivotal opportunity: to forge education as a bulwark against exploitation.

Transformative curricula must prioritize cybersecurity literacy from early stages, weaving in practical skills like ethical hacking, privacy protocols, and critical media discernment. By nurturing adaptive, values-driven learners, we alchemize vulnerabilities into empowerment. Graduates emerge not as passive targets, but as ethical innovators driving economic resilience, social equity, and inclusive technological ecosystems. Thus, the paradox resolves: digital education evolves from a double-edged sword into a beacon of collective progress, illuminating pathways to good citizenship and human-centered prosperity.

Eleanor Roosevelt in 1930 described good citizenship as the foremost purpose of education.[34] In the contemporary age of technology, good citizenship needs to be manifested to the digital realm as well. This is where the idea of digital citizenship enters. Althibyani & Al-Zahrani (2023) say,

> "Digital citizenship refers to the competence to navigate digital environments in a responsible and safe manner, and to engage actively and respectfully in these spaces. It involves understanding how to use digital technology effectively and ethically, while also respecting the rights and privacy of others. The nine dimensions of digital citizenship are essential for promoting safe, respectful, and responsible use of digital technology. These dimensions include digital law, digital manners, digital communication, digital rights and duties, digital trade, digital health, digital access, digital security, and digital culture."

[34] Roosevelt, E. (1930) 'Good Citizenship: The Purpose of Education,' *Pictorial Review* https://socialwelfare.library.vcu.edu/programs/education/good-citizenship-purpose-education/

Therefore, using education as a tool to reduce cybercrime should focus on normative transformation of society in digital spaces. Though aspirational in scope, the idea should serve as the ideal we strive to achieve every time we formulate educational policies.

References

Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the Effect of Students' Knowledge, Beliefs, and Digital Citizenship Skills on the Prevention of Cybercrime. *Sustainability*, *15*(15), 11512. https://doi.org/10.3390/su151511512

Anthony B (2025;), "Economic determinants of cybercrime in India: a state-level panel data analysis". *Safer Communities* https://www.emerald.com/sc/article-abstract/doi/10.1108/SC-03-2025-0020/1328063/Economic-determinants-of-cybercrime-in-India-a?redirectedFrom=fulltext

Becker, G. S. (1968). Crime and Punishment: An Economic Approach. *Journal of Political Economy*, *76*(2), 169–217. http://www.jstor.org/stable/1830482

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4), 588–608. https://doi.org/10.2307/2094589

Digital Personal Data Protection Rules 2025, Ministry of Electronics and Information Technology, Government of India https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf

Ebert, H. (2020). Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. *India Review*, *19*(4), 376–413. https://doi.org/10.1080/14736489.2020.1797317

Jha, A. K., & Arora, A. (2020). The neuropsychological impact of E-learning on children. *Asian journal of psychiatry*, *54*, 102306. https://doi.org/10.1016/j.ajp.2020.102306

Kumar, M. V. (2024), Exploring Cyber Threats and Digital Risks in Indian Educational Institutions, CyberPeace https://delnet.in/pdf/cpfpub.pdf

Pandey, D. (2025) Critical gaps in Indian education sector's digital defences: CyberPeace report, The Hindu https://www.thehindu.com/news/national/critical-gaps-in-indian-education-sectors-digital-defences-cyberpeace-report/article69925218.ece

Pant, R. & Chaubey, U. (2024), Protecting Minds in the Digital Age: A Review Based Study on Psychological Impact of Cybercrime, The International Journal of Indian Psychology ISSN 2348-5396 (Online), ISSN: 2349-3429 (Print), Volume 12, Issue 3, July- September, 2024 https://ijip.in/wp-content/uploads/2024/09/18.01.220.20241203.pdf

Sarkar, G. & Shukla, S. (2025), Cyber Slavery Infrastructures: A Socio-Technical Study of Forced Criminality in Transnational Cybercrime, Cornell University https://arxiv.org/abs/2510.12814