CyberPeace
www.cyberpeace.org

DELNET
Developing Library Network
www.delnet.in

AI Skills for Enhanced Cybersecurity Resilience

CyberPeace | DELNET Developing Library Network

AI Skills for Enhanced Cybersecurity Resilience

CyberPeace is a global non-profit organization headquartered in India, working at the intersection of cybersecurity, policy, and peacebuilding. It envisions a safe, resilient, and inclusive cyberspace for all.

Through its global initiatives, CyberPeace drives capacity building, policy research, incident response, and public awareness to advance the vision of “CyberPeace and Trust in Technology.” From grassroots digital literacy programs to high-level policy and research collaborations, CyberPeace integrates innovation, education, and advocacy to strengthen digital ecosystems worldwide.

Championing the future of responsible technology, CyberPeace is building the next generation of Cyber Defenders and Responsible Digital Citizens, aligning its mission with the United Nations Sustainable Development Goals (SDGs) and India’s Viksit Bharat 2047 vision

Title: AI Skills for Enhanced Cybersecurity Resilience

Editor: Maj Vineet Kumar

https://www.cyberpeace.org/

Acknowledgments

AI Skills for Enhanced Cybersecurity Resilience has been developed under the esteemed guidance of **Major Vineet Kumar, Founder and Global President of CyberPeace,** by Sqn Ldr Parul Tiwari (R) and Ayndri. His continued commitment to a secure and digitally inclusive India inspires and anchors our work.

We are deeply grateful to **Dr. Sangeeta Kaul, Director, DELNET,** for her strategic partnership and encouragement in making this joint initiative possible. Her institutional support was key to driving this collaboration forward.

We sincerely thank the wider **teams at CyberPeace and DELNET** for their operational support and commitment to furthering the national skilling and cybersecurity agenda.

This white paper is being released as part of the **Cyber First Responder Initiative** undertaken by CyberPeace and DELNET with support from Google.org.

.

ABBREVIATIONS

Abbreviation	Full Form
AI	Artificial Intelligence
AICTE	All India Council for Technical Education
AiSP	Association of Information Security Professionals (Singapore)
BBA	Bachelor of Business Administration
BCA	Bachelor of Computer Applications
CDAC	Centre for Development of Advanced Computing
CERT-In	Indian Computer Emergency Response Team
CISO	Chief Information Security Officer
CYSREN	Cybersecurity Strategic Research and Education Network (NTU)
DSCI	Data Security Council of India
DPI	Digital Public Infrastructure
EC-Council	International Council of E-Commerce Consultants
ENISA	European Union Agency for Cybersecurity
GCC	Global Capability Centre
GCSCC	Global Cyber Security Capacity Centre
IDRBT	Institute for Development and Research in Banking Technology

ABBREVIATIONS

Abbreviation	Full Form
IIT	Indian Institute of Technology
IIIT	Indian Institute of Information Technology
ISACA	Information Systems Audit and Control Association
ITI	Industrial Training Institute
MeitY	Ministry of Electronics and Information Technology
ML	Machine Learning
NCERT	National Council of Educational Research and Training
NCVET	National Council for Vocational Education and Training
NEP	National Education Policy
NICE	National Initiative for Cybersecurity Education (NIST, U.S.)
NIC	National Informatics Centre
NCIIPC	National Critical Information Infrastructure Protection Centre
NEP 2020	National Education Policy 2020
NIELIT	National Institute of Electronics and Information Technology
NIST	National Institute of Standards and Technology (U.S.)
NSDC	National Skill Development Corporation

ABBREVIATIONS

Abbreviation	Full Form
NSQF	National Skills Qualification Framework
NUS	National University of Singapore
NUS-ISS	Institute of Systems Science, National University of Singapore
NTU	Nanyang Technological University
NTUC	National Trades Union Congress (Singapore)
PMKVY	Pradhan Mantri Kaushal Vikas Yojana
SOC	Security Operations Center
STQC	Standardisation Testing and Quality Certification Directorate
SUTD	Singapore University of Technology and Design
TCS	Tata Consultancy Services
TTAB	Tech Talent Assembly (Singapore)
UGC	University Grants Commission
UPI	Unified Payments Interface
USD	United States Dollar
Yojana	Government scheme or plan (in Hindi)

GLOSSARY OF KEY TERMS

Term	Plain-Language Definition
Artificial Intelligence (AI)	Technology that enables machines to mimic human thinking, like recognizing patterns, making decisions, or learning from data.
Cybersecurity	The protection of computers, networks, and data from theft, damage, or attacks through a convergence of people, processes, and tools.
AI-powered cyberattacks	Cyberattacks that use AI tools to make them faster, harder to detect, or more personalized.
Adversarial AI	A type of AI attack where hackers trick AI systems by feeding them misleading or harmful information.
Generative AI	AI that can create content—like text, images, or code—on its own, such as ChatGPT or DALL·E.
Digital Public Infrastructure (DPI)	Government-supported digital platforms that provide services to the public, such as Aadhaar (ID), UPI (payments), and DigiLocker (documents).
Cybersecurity Simulation Labs	Training centers where people can practice defending against real-world cyber threats in a controlled environment.
Stackable Micro-Credentials	Short, focused learning programs that can be combined over time to build up to full qualifications or certifications.
Regulatory Sandbox	A safe testing space where new technologies (like AI tools for cybersecurity) can be tried out under supervision before full rollout.
SOC (Security Operations Center)	A team or facility that monitors and responds to cyber threats in real time.

Executive Summary

As India undergoes rapid digital transformation across both public infrastructure and private enterprise, it is witnessing a sharp increase in cyberattacks in sectors like banking and finance, healthcare, government, and critical infrastructure. Simultaneously, artificial intelligence (AI) is being increasingly embedded into digital systems to enhance operations, including cybersecurity.

While AI can be leveraged to enhance threat mitigation, detection and response to cyberattacks, it also poses sophisticated risks that can present in the form of AI- generated breaches and evolving threat surfaces that require advanced technical protections. India's cybersecurity workforce, however, remains underprepared to meet these emerging challenges.

Against this backdrop, this white paper assesses global and national policy initiatives to integrate AI into cybersecurity skilling practices. It maps the current policy landscape, highlights key institutional gaps, and offers a roadmap for building a resilient, inclusive, and future-ready AI–cyber talent pipeline in India. It draws on international models like Singapore to provide practical recommendations for Indian legislators, educational institutions, and industrial stakeholders.

Introduction

Organisations globally are facing the impact of geopolitical pressures, supply chain disruptions, resource scarcity, and AI-driven technological advancement, along with increasing incidents of cybersecurity breaches.[1] AI has massive benefits for optimizing processes, but it also empowers threat actors to carry out attacks faster and at scale. Governments, businesses, and cybersecurity professionals need to keep upskilling to face and deter these attacks. But world over, a critical skills gap exists, with technology development outpacing security expertise growth. Nearly 4.8 million cybersecurity roles remain unfilled globally,[2] and a third of IT professionals report insufficient AI-security skills to counter this new wave of threats.[3]

India is actively pursuing the digitalisation of its economy by[1] expanding digital networks and infrastructure under the Digital India program. The India Stack is widely hailed as a global benchmark for digital services.[4] But the country also faces the challenge of persistent cyber threats from rapidly digitising institutions. In 2023-2024, the country saw over 369 million malware attacks, with an average of 702 detections per minute.[5] The country has seen massive data breaches, like the AIIMS Ransomware Attack (2023),[6] compromising 40 million patient records, and the Star Health Data Leak (2024), with 31 million records leaked. Energy, power, and utilities have also become prime targets in the recent past.[7]

Concomitantly, the demand for cybersecurity professionals to counter these threats is increasing. But there remains a critical talent shortage in the country, especially in specialised roles[8] such as AI security, cloud and network security, and data privacy. It is estimated that the year-on-year demand for cybersecurity professionals with interdisciplinary skills is only set to increase. India has among the largest youth populations in the world and over 31 % of the world's science, technology, engineering and mathematics (STEM) graduates, yet 30% of cybersecurity vacancies could not be filled in 2023 due to talent shortages.[9] The under-supply of critical cybersecurity expertise and the evolving nature of cyber attacks, including AI-powered attacks, threaten public and private sector resilience in the country. As cybersecurity threats grow in speed and complexity, so must the country's talent pipeline.

REFERENCES

1. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study
2. https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/
3. https://cybermagazine.com/articles/global-survey-reveals-critical-ai-security-skills-shortage
4. https://www.ey.com/en_in/insights/india-at-100/digitalizing-india-a-force-to-reckon-with
5. https://www.dsci.in/resource/content/india-cyber-threat-report-2025
6. https://thelegalschool.in/blog/recent-data-breaches
7. https://www.fortuneindia.com/macro/from-financial-services-to-healthcare-top-sectors-that-faced-highest-cybersecurity-threats-in-2024/119749 '
8. https://www.cnbctv18.com/education/india-cybersecurity-jobs-hiring-market-rising-demand-talent-shortage-vacancies-indeed-19497404.htm
9. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf

AI-Cybersecurity Convergence

In the AI-cybersecurity domain, two key competency areas emerge:

1. AI-integrated cybersecurity: This includes knowledge of techniques and tools to enhance threat detection, security operations, and risk prediction. Skills here fall under both existing cybersecurity roles (e.g., SOC Analyst) and emerging roles (e.g., AI-augmented Threat Intelligence Specialist).[10]

2. Cybersecurity of AI systems: This includes ensuring the security and integrity of AI models themselves, for defending against adversarial ML attacks, securing model pipelines, and auditing AI behaviour. New roles such as “Adversarial AI Researcher” or “AI Security Auditor” are evolving in response.[11]

As AI-driven threats and defense mechanisms become more intricate, the demand for structured, scalable training models grows. This requires institutional recognition of the same, curriculum development, and workforce alignment. In this regard, workforce and skill frameworks become essential to standardise skill requirements, define new job roles, and direct industry certifications and educational programs.[12] Attempts to train India's cybersecurity workforce for AI-centric roles run the risk of remaining fragmented and reactive in the absence of such frameworks.

REFERENCES

10. https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity#:~:text=What%20is%20AI%20in%20Cybersecurity,defense%20and%20safeguarding%20sensitive%20data

11. https://www.cybersecuritytribe.com/articles/cybersecurity-careers-and-ais-impact?

12. https://www.giac.org/blog/why-workforce-frameworks-certifications-matter-cybersecurity/

International & National Policy Landscape

Understanding India's approach to AI-cybersecurity requires situating it within broader global trends and the country's evolving policy ecosystem.

2.1 Global Frameworks

NIST NICE Framework (U.S.A)

The U.S. National Institute of Standards and Technology (NIST) maintains the NICE Workforce Framework for Cybersecurity, which articulates standardized roles, tasks and competencies to inform education and workforce development. An ongoing 2025 update incorporates AI-focused roles and skills, allowing institutions to adapt curricula to evolving technologies[13].

EU Artificial Intelligence Act (AI Act)

Effective August 2024, the EU's AI Act introduces a risk-based legal framework, mandating robust cybersecurity measures, particularly for "high-risk" AI systems deployed in critical sectors. It promotes secure design, auditability, and resilience against adversarial threats[14].

UK CyberFirst Initiative

The United Kingdom's CyberFirst program targets youth and school-age learners, providing pathways into cybersecurity through education and practical exposure. While not exclusively AI-focused, it illustrates how national skilling can begin at pre-university levels.

REFERENCES

13. https://www.nist.gov/blogs/cybersecurity-insights/impact-artificial-intelligence-cybersecurity-workforce

14. https://www.bsigroup.com/en-GB/insights-and-media/insights/blogs/the-eu-ai-act-and-its-interactions-with-cybersecurity-legislation/

15. https://government.economictimes.indiatimes.com/news/governance/national-cybersecurity-strategy-2023-to-be-introduced-soon-rajesh-pant/98116674

16. https://www.futureskillsprime.in/about-us/

2.2 India's Key Initiatives

National Cyber Security Policy (NCSP), 2013 & The National Cybersecurity Strategy

India's foundational 2013 policy aimed to protect critical information infrastructure and build national cyber capabilities. In line with technological evolution, a 2023 draft update, drafted by the DSCI and led by the erstwhile National Cybersecurity Coordinator, proposes enhanced frameworks to address threats from emerging technologies like AI, among others[15]. The final strategy is yet to be released.

MeitY–NASSCOM FutureSkills Prime

An initiative led by the Ministry of Electronics & IT (MeitY) in partnership with NASSCOM, FutureSkills Prime aims to train India's workforce in emerging technologies, including AI and cybersecurity. Strategic collaborations, such as with EC-Council, have integrated industry-standard security courses into its curriculum[16]. While over 13 lakh professionals enrolled in 2023[17] , these numbers provide limited insight into real-world post-training outcomes such as employability, skill application, or career advancement.

All India Council for Technical Education (AICTE) Curriculum Modernization

Since the 2020–21 academic year, AICTE has revamped its outcome-based model curricula across diploma, undergraduate, and postgraduate technical programs to include emerging fields like AI, Cybersecurity and Data Science. It even rolled out tools like the AICTE Translation Automation to regionalize learning content[18].In April 2025, AICTE established an expert panel aiming to integrate AI broadly across disciplines such as BBA, BCA, Electrical Engineering as part of its declaration of 2025 as the "Year of Artificial Intelligence", spanning 14,000+ institutions and targeting around 40 million students[19].

Industry-Led Skilling (NASSCOM–DSCI)

Initiatives by industry bodies, such as the Data Security Council of India (DSCI) and NASSCOM, support programs like CyberShikshaa[20] and host CISO forums[21]. These focus on enhancing awareness and practice, but data on implementation across states, especially in Tier-II/III areas, is scant.

REFERENCES

17. https://sansad.in/getFile/loksabhaquestions/annex/1711/AU4827.pdf?source=pqals#:~:text=(a)%20the%20total%20number%20of,FutureSkills%20PRIME%2C%20as%20on%2023.03.

18. https://rsdebate.nic.in/bitstream/123456789/735401/1/PQ_258_07122022_U26_p139_p139.pdf

19. https://apacnewsnetwork.com/2025/04/aicte-forms-expert-panel-to-mainstream-ai-across-all-technical-education-streams/

20. https://www.dsci.in/cyber-shikshaa/

21. https://www.dsci.in/event/aiss-2024/#:~:text=04%2C%2005%20&%2006%20December%2C,of%20Cyber%20Security%20&%20Data%20Protection.

Key Challenges Faced by India

While India has made commendable strides in digital skilling, **systemic gaps** continue to undermine the impact of its cybersecurity and AI-readiness agenda. The following challenges, such as AI-driven threat escalation to education–industry misalignment and uneven institutional capacity, must be urgently addressed to ensure India can build a secure, inclusive, and future-ready talent pipeline:

Weaponisation of AI in Cyber Attacks:

Generative AI is rapidly transforming the cyber threat landscape by creating new attack vectors and lowering the barrier of entry for cybercriminals. Further, AI is increasingly used in malware creation, phishing, and misinformation campaigns. A 2024 Axios and Arkose Labs survey found that 56% of organizations experienced an increase in the frequency and sophistication of cyberattacks attributed to AI tools, while only 1 in 5 felt adequately prepared to defend against them[22].

India is one of the Most Attacked Nations Globally:

According to CloudSEK's ThreatLandscape Report 2024, India was the second most targeted country worldwide, with 95 Indian entities experiencing data theft attacks in 2024, only behind the United States, which had 140 such incidents. The most impacted sectors included Finance & Banking, Government, Telecommunications, Healthcare & Pharma, and Education[23]. This emphasizes that rapid digitization does not imply resilience.

REFERENCES

22. https://www.axios.com/newsletters/axios-codebook-4c6813f0-a5ce-11ef-ad2a-91f707f80b70

23. https://www.business-standard.com/technology/tech-news/india-second-most-targeted-nation-in-terms-of-cyberattacks-cloudsek-125010200905_1.html

24. https://www.thehindu.com/business/Industry/india-facing-huge-shortage-of-cybersecurity-professionals-teamlease/article66994515.ece

25. https://www.thehindubusinessline.com/on-campus/bridging-the-skill-gap-in-cybersecurity/article68289195.ece

Education Misalignment:

Despite India's reputation as a global IT talent hub, its formal education system remains poorly aligned with the demands of the cybersecurity industry. As of May 2023, India had approximately 40,000 open cybersecurity positions, but nearly 30% remained unfilled due to a lack of qualified candidates, according to TeamLease Digital[24]. ISACA's *2023 State of Cybersecurity* report revealed that around 40% of Indian cybersecurity teams identified an industry–academia skills gap, particularly in cloud, AI, and advanced security controls[25].

Cybersecurity Talent Shortfall Predicted to Continue:

According to a NASSCOM–Zinnov report, India is projected to have 75–78 lakh tech professionals by 2026, while demand will reach 93–96 lakh, leading to a shortfall of 14–19 lakh tech workers[26]. Despite producing millions of STEM graduates, in 2021-22, only a fraction were trained in AI, cybersecurity, and cloud, creating a severe skills gap just as AI becomes central to both cyber threats and solutions[27].

Gender and Regional Gaps in Access to Cybersecurity Skilling:

Women continue to be underrepresented in cybersecurity and AI training pipelines despite flagship initiatives like CyberShikshaa, which has trained over 800+ women engineering graduates from 90+ cities/districts across 22 states/UTs. Though women's workforce participation rate in cybersecurity is expected to rise from 10.8% in 2022 to 14.9% by 2027[28] in India. This digital divide risks entrenching inequalities and limiting India's ability to cultivate a diverse and inclusive cybersecurity workforce at scale.

Fragmented Institutional Ownership of Skilling:

Cybersecurity skilling in India is governed by a patchwork of agencies like AICTE, UGC, MeitY, NCVET, and various industry consortia. A 2023 analysis of India's cybersecurity architecture highlighted fragmented regulatory frameworks, coordinating bodies like CERT-In and NCIIPC operate under different mandates, with inadequate central oversight and poor inter-governmental coordination between central and state agencies[29]. This fragmentation hampers consistent curricula enforcement, emerging tech integration, and national standardization of AI-cybersecurity training programs.

REFERENCES

26. https://www.businesstoday.in/big-story/story/india-could-face-a-shortage-of-14-19-lakh-techies-by-2026-nasscom-zinnov-report-323019-2022-02-17

27. Ibid.

28. https://www.dsci.in/dsci-blog/content/passive-leaners-leaders-growing-role-women-cyber-security-and-privacy

29. https://ijrpr.com/uploads/V5ISSUE12/IJRPR36240.pdf

Limited Public Sector Capacity & Awareness:

India's expansive digital footprint and increased reliance on interconnected networks are undermined by cybersecurity awareness and protection gaps in public-sector institutions[30]. Many public departments, especially in rural and tier-II/III districts vulnerable to ransomware, phishing, and AI-led misinformation campaigns[31].

REFERENCES

30. https://www.journalofpoliticalscience.com/uploads/archives/7-5-21-949.pdf

31. https://jaankari.csccloud.in/blog/cyberfraud.html

Case Study: Singapore's AI-Cybersecurity Convergence

Recognized as a regional cybersecurity hub, Singapore identifies robust cybersecurity as a **foundation for business growth and attracting global talent.** Accordingly, it prioritizes **coordination** within the ecosystem, robust innovation through **research and development**, and an **intellectual property protection** framework[32]. This offers valuable lessons on harmonizing policy, skilling, and innovation to secure a digital-first nation. *For a comparative overview of India and Singapore's AI-cyber readiness across skilling, policy, and infrastructure, see Appendix A.*

4.1 Holistic National Strategy – CyberSG Ecosystem

Under the CyberSG umbrella, Singapore's Cyber Security Agency (CSA) launched the Cybersecurity Talent, Innovation & Growth (Cyber TIG) Plan in 2023. This initiative[33]:

- Offers STEM-to-cyber conversion programs for experienced professionals
- Develops a professionalisation framework to certify and standardise cybersecurity roles
- Incorporates AI topics into its annual innovation challenge (*CyberCall*)
- Establishes talent and innovation hubs, including one at NUS, and provides SGD 110 million in funding through 2026.

REFERENCES

32. https://www.csa.gov.sg/news-events/speeches/speech-by-minister-for-comm-and-info-josephine-teo-at-csa-cybersecurity-innovation-day-on-29-september-2023

33. Ibid.

34. https://www.csa.gov.sg/resources/publications/guidelines-and-companion-guide-on-securing-ai-systems?utm_

35. https://www.ntu.edu.sg/cysren/professional-courses/ai---cybersecurity-innovation-camp-series?utm_

4.2 Targeted AI-Security Education & Certifications

A. CSA released the "Guidelines & Companion Guide on Securing AI Systems" (Oct 2024), recommending an AI lifecycle approach including design, development, deployment, operations, and end-of-life security to mitigate adversarial and supply chain risks[34].

B. Academic institutions are embedding AI-cybersecurity blends such as :

- NTU's AI & Cybersecurity Innovation Camp, via CYSREN, immerses participants in hands-on labs[35].
- SUTD, NTUC, AiSP & TTAB launched the "Design × AI × Tech (Cybersecurity)" certification to reskill non-IT professionals with mandatory internships[36].
- NUS-ISS's "AI and Cybersecurity" executive certificate blends AI-policing and attack modeling[37].

4.3 International Collaboration & Capacity Building

In March 2025, Singapore co-hosted the AI Cybersecurity Readiness Workshop with the UK's Global Cyber Security Capacity Centre (GCSCC), concentrating on AI cyber-risk metrics and secure AI deployment across governments and industry[38].

REFERENCES

36. https://www.sutd.edu.sg/course/design-ai-tech-cybersecurity/

37. https://www.iss.nus.edu.sg/blended-learning-programme/programmes/course-bl/detail/ai-and-cybersecurity/cybersecurity?utm_

38. https://gcscc.ox.ac.uk/article/gcscc-co-hosts-ai-cybersecurity-readiness-workshop-singapore?utm_

Opportunities for India: Why Act Now

If India can quickly bridge the AI skills gap, it presents a unique chance to integrate cybersecurity by design. According to a Quess IT Staffing report, by 2030, emerging technologies like artificial intelligence (AI), cybersecurity, cloud computing, data science and blockchain are expected to generate about one million new jobs in India, attracting about USD 150 billion and increasing the country's IT workforce from 5.4 million to 7.5 million[39]. India's AI-skilled workforce is expected to nearly double from roughly 6,00,000–6,50,000 in 2022 to over 1.25 million by 2027, according to a Deloitte–NASSCOM study. However, market demand is growing at a faster rate of 25–35% CAGR, indicating a persistent skills gap[40]. These trends underscore that while demand for digital talent is rising rapidly, the supply of skilled professionals, especially those with combined AI and cybersecurity expertise, is lagging.

India's world-leading Digital Public Infrastructure (DPI), including Aadhaar, UPI, and DigiLocker, offers a massive deployment canvas for secure, AI-enabled services. The international interest in India's DPI model and upcoming improvements like National Broadband Mission 2.0, which aims to reach rural and Tier-II/III areas by 2030, presents a once-in-a-lifetime chance to secure next-generation digital delivery systems. But capitalizing on this opportunity requires investing in an AI-fluent cybersecurity workforce immediately and laying the foundations for a quantum-trained cybersecurity workforce in the future.

Both the public and private sectors are already taking action. State government programs like Uttar Pradesh's AI Pragya Yojana, in partnership with Microsoft, Amazon, and HCL, aim to train one million people in AI, ML, data analytics, and cybersecurity[41].

REFERENCES

39. https://www.business-standard.com/technology/tech-news/ai-cybersecurity-to-drive-1-mn-jobs-by-2030-quess-it-staffing-report-124123000670_1.html?utm_

40. https://www.deloitte.com/in/en/about/press-room/bridging-the-ai-talent-gap-to-boost-indias-tech-and-economic-impact-deloitte-nasscom-report.html?utm_

41. https://wadhwanifoundation.org/press/ai-pragya-up-govt-to-launch-digital-literacy-campaign-train-citizens-in-ai-data-analytics-and-more-details/

Meanwhile, industry titans like Cisco have confirmed India's position as a strategic hub for cybersecurity and AI innovation[42]. These programs highlight India's readiness to leverage emerging private-sector momentum for co-created training solutions.

Finally, India's leadership in the Global Capability Centre (GCC) sector, operating over 1,700 high-value centers focused on tech roles, positions the country to evolve from a service outsourcing hub to a global innovation and export engine[43]. Strengthening AI-cyberskills across this ecosystem will help accelerate India's shift from low-code execution to AI-native product design and secure systems development.

REFERENCES

42. https://www.expresscomputer.in/features/ciscos-big-india-bet-powering-the-nations-ai-and-data-center-future/126210/

43. https://bwsecurityworld.com/technology/quess-corp-highlights-resilience-emerging-trends-in-indias-it-staffing-sector/?utm_

Policy Recommendations

Develop a National AI-Cybersecurity Skills Framework

India should lead the creation of a national framework defining the core competencies needed to work at the intersection of AI, cybersecurity and other emerging technologies in quantum. This can build on efforts by the National Skill Development Corporation (NSDC), AICTE, and NASSCOM and align with global initiatives like NIST's NICE Framework and ENISA's cybersecurity skills strategy. MeitY, NSDC, and NASSCOM could be established as lead agencies.

Integrate AI and Cyber Risk into Technical and Higher Education

Universities, engineering colleges, and ITIs must embed AI-cybersecurity convergence topics into core curricula, not just as electives. AICTE's ongoing curriculum modernization must go beyond AI theory to include real-world cyber risk scenarios, ethical AI, bias detection, and adversarial attacks. UGC and AICTE should jointly notify integrated AI-Cyber electives under NEP 2020 guidelines.

Set Up Zonal Cyber Labs and National Training Grounds

India can build a network of AI-Cybersecurity Simulation Labs across zones (North, South, East, West, Northeast) under MeitY's Digital India Centres of Excellence, with collaboration between CERT-In, NIELIT, CDAC, and State IT Departments, where public and private institutions train on real-world AI-led threat simulations.

Strengthen Public–Private Skilling Partnerships

To scale quickly, India must expand platforms like FutureSkills PRIME and CyberShikshaa to include AI-security co-certifications, paid apprenticeships and micro-internships. These should be co-designed by firms such as TCS, Wipro, Microsoft, Cisco and be open to Tier II/III learners and underrepresented groups.

Enable Lifelong Learning through Stackable Micro-Credentials

With cybersecurity threats evolving fast, professionals need to keep upskilling and exhibit transferable skills. India should formally recognize modular, stackable credentials under the National Skills Qualification Framework (NSQF). This will allow professionals to upgrade without pausing careers and build toward advanced certifications across AI for cybersecurity, privacy engineering, and cloud forensics.

Create a Regulatory Sandbox for AI in Cybersecurity

To balance innovation and safety, India should create a regulatory sandbox for AI-based cybersecurity tools, especially those used in governance, education, health, and financial infrastructure. CERT-In, in collaboration with NCIIPC and STQC, can pilot this model with support from MeitY

Launch an Indian Cybersecurity Readiness Index with AI Metrics

DSCI or NIC can be tasked to upgrade India's cybersecurity maturity index to include AI indicators such as:

- Integration of AI in national/state SOCs
- Use of AI in cyber threat detection
- AI-skilling penetration in the workforce

Fund Deep Research on Adversarial AI and Autonomous Threats

India should launch a National Research Mission on AI and Cybersecurity, supporting interdisciplinary R&D in adversarial attacks, synthetic media detection, and autonomous cyber defense. It should involve IITs, IIITs, CDAC, IDRBT and leading private labs

Measuring Impact: Tracking Progress on AI-Cybersecurity Skilling

Monitoring results is just as crucial to the success of India's AI-cybersecurity skill development initiatives as growing them. Although enrolment has been the main focus of initiatives like FutureSkills Prime and CyberShikshaa, little information about skill application, employability or public-sector integration is available to the public. India should implement a **transparent, goal-oriented monitoring system** to evaluate whether present and upcoming skilling initiatives are actually closing the AI-cybersecurity gap in order to maintain accountability. This paper suggests impact indicators across four domains: **industry alignment, innovation output, institutional capacity and workforce readiness** to make sure skilling initiatives are not just statistically impressive but also actually effective. The objectives of national skilling initiatives as well as the recognised problems in India's cybersecurity ecosystem are reflected in these domains. The following proposed indicators offer a basis for institutions, ministries and industry consortia to measure progress across workforce readiness, institutional capacity, industry alignment and research innovation:

Workforce Readiness

Metric	Purpose
% of engineering/technical graduates exposed to AI-cybersecurity modules	Measures integration into formal education
Number of professionals certified in AI-cyber convergence	Tracks the national scale of upskilling
Ratio of women in AI-cyber skilling programs	Assesses gender equity
Representation from Tier II/III towns	Promotes regional inclusion

Institutional & Public Sector Capacity

Metric	Purpose
Number of AI cybersecurity simulation labs established	Assesses infrastructure readiness. 1 per region (North, South, East, West, Northeast)
Public-sector adoption of AI-threat modules in training	Evaluates the preparedness of public institutions
Number of government agencies piloting AI cybersecurity tools	Measures the adoption of safe innovation

Industry Alignment & Hiring Outcomes

Metric	Purpose
Industry satisfaction score (via NASSCOM/DSCI surveys)	Measures alignment with workforce needs
Placement rate post AI-cyber skilling programs	Tracks employability
Industry-co-developed skilling programs	Ensures curriculum relevance

Research & Innovation Ecosystem

Metric	Purpose
Number of funded research projects on AI-cybersecurity	Measures academic engagement
Collaborative publications or patents in AI-cybersecurity	Tracks innovation output

Institutional Ownership for Monitoring

To implement these metrics effectively, India can leverage existing institutions:

- **MeitY, NSDC, and NASSCOM** to monitor training, credentials and employer engagement.
- **AICTE and UGC** to track curriculum implementation across technical education.
- **CERT-In and NCIIPC** to report on AI adoption in threat intelligence.
- **NITI Aayog and CAG** to audit performance and alignment with national skilling goals.

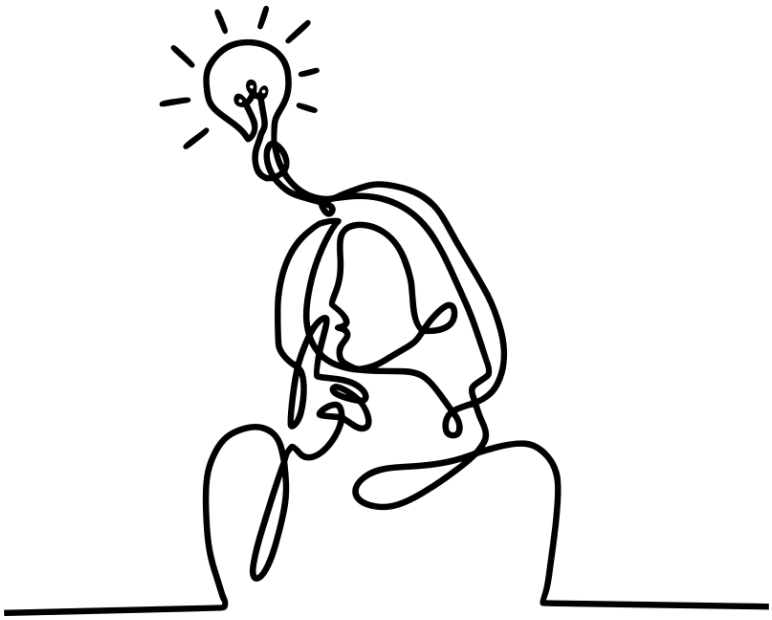
Developing an integrated public dashboard or annual AI–Cybersecurity Skilling Report can further enhance transparency and enable data-driven course correction.

Conclusion

The combination of AI and cybersecurity will determine how resilient India's digital public infrastructure, economic competitiveness and national security are as the country rapidly advances towards a digitally empowered future. However, these goals run the risk of being jeopardised by new threats and enduring skill shortages if the workforce is not both cyber-aware and AI-capable.

The urgency of creating an integrated skilling ecosystem that equips students from all backgrounds and locations, institutionalises AI-cybersecurity in national policy and matches technical education with changing industry demands has been emphasised in this white paper. It is past time for a new national cybersecurity policy that places sufficient emphasis on skilling. Models from nations such as Singapore demonstrate that leadership in this crucial area is achievable through early investment in innovation and training, cross-sector collaboration and strategic coherence.

India must act swiftly to institutionalize AI-cybersecurity readiness as a national priority. This calls for not just more programs, but smarter ones that are developed in collaboration with industry, delivered in simulation labs, tracked by open metrics and available to everyone. By doing this, India can secure the future for future generations and transform today's challenge into tomorrow's competitive advantage.



Appendix A: *Comparative Readiness Matrix – India vs. Singapore in AI-Cybersecurity Skilling & Policy*

This matrix offers a side-by-side comparison of India and Singapore's readiness in integrating AI into cybersecurity skilling and policy. It draws on national strategies, institutional coordination, industry-academia partnerships, and innovation capacity. While India has scaled initiatives across its vast geography, Singapore offers lessons in strategic coherence, certification ecosystems, and AI-specific policy integration.

Dimension	India	Singapore
National Strategy	Draft National Cybersecurity Strategy (2023, not yet released); fragmented ownership across agencies.	CyberSG Ecosystem with unified Cyber TIG Plan under Cyber Security Agency (CSA).
Integration of AI in Cyber Policy	AI mentioned in strategy drafts and skilling platforms, but not yet institutionalized in cyber policy.	Dedicated AI cybersecurity guidelines (Oct 2024); embedded AI lifecycle risk in national cybersecurity.
Skilling Ecosystem	FutureSkills PRIME, AICTE reforms, and Cyber Shikshaa programs, but limited tracking of learning outcomes.	Centralized, outcome-driven efforts via NUS, NTU, and SUTD, with mandatory internships and certifications.
Simulation Labs & Infrastructure	Proposal for zonal cyber labs: limited real-world attack simulation environments.	Active cyber hubs with SGD 110 million funding; CyberCall innovation challenges, and CYSREN hands-on labs.
Workforce Professionalization	No formal national certification for AI–cyber professionals yet.	Professionalization framework in place with structured role certifications.
Industry-Academia Collaboration	Industry-led programs (NASSCOM, EC-Council), but uneven reach and coordination.	Strong academia–industry integration with co-created courses and applied R&D funding.

Dimension	India	Singapore
Public Sector Capacity	Limited AI-cyber training in government departments, esp. in Tier II/III areas.	Government agencies piloting AI cybersecurity tools; cross-agency readiness workshops.
International Engagement	Limited formal participation in global AI-cyber risk workshops.	Co-hosted global AI Cybersecurity Readiness Workshop with the UK's GCSCC in 2025.
Gender & Regional Inclusion	CyberShiksha aimproving access, but large gender gaps remain.	Targeted programs exist, though inclusion is less emphasized as a challenge due to a smaller population base.
Monitoring & Impact Assessment	No national AI-cyber skilling index or public dashboard.	Centralized tracking via CSA and annual reporting mechanisms.

CyberPeace

DELNET
Developing Library Network