MeitY Startup Hub
Delivering Innovation!

FICCI

The Dialogue™
INFORM ENGAGE IDEATE

WHITE PAPER

INDIA'S DIGITAL REVOLUTION: CHARTING THE FUTURE OF SECURE DIGITAL INFRASTRUCTURE

India's Digital Revolution: Charting the Future of Secure Digital Infrastructure

"Cybersecurity is no longer limited to just the digital world and has now become a matter of national security."

- **Prime Minister Narendra Modi**

Authors: Bhoomika Agarwal, Garima Saxena and Vaishnavi Sharma

Copyeditor and Designer: Akriti Jayant

About MeitY Start-up Hub (MSH)

To give wings to MeitY's vision of promoting technology innovation, start-ups and creation of Intellectual Properties, a nodal entity called MeitY Start-up Hub (MSH) has been setup under its aegis. MSH is a dynamic, singular and collaborative platform for tech startup community towards building meaningful synergies in the Indian start-up space. MSH's quick value additions to domestic tech startups in terms of improving scalability, market outreach and domestic value addition and setting up innovative partnerships with various stakeholders has been a key differentiator in MSH's efforts to catapult the tech startup ecosystem in the country.

MSH is acting as a hub and ensuring synergies among all the TIDE 2.0 Centres, theme-based incubation centres, domain specific Centre of Excellences on Emerging Technologies and other existing platforms for facilitating criss-crossing of technology resources, sharing best practices and ideas across the entire gamut of innovation and startup ecosystem.

About the Federation of Indian Chambers of Commerce & Industry (FICCI)

A non-government, not-for-profit organisation, FICCI is the voice of India's business and industry. FICCI encourages debate, engages with policy makers and civil society, and articulates the views and concerns of industry. It serves its members from the Indian private and public corporate sectors and multinational companies, drawing its strength from diverse regional chambers of commerce and industry across states, reaching out to over 2,50,000 companies.

About The Dialogue™

The Dialogue™ is a public policy think tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues. The Dialogue™ has been ranked as the world's Top 10 think tanks to watch out for, by the Think Tank and Civil Societies Programme (TTCSP), University of Pennsylvania in their 2020 and 2021 rankings.

For more information, visit

https://www.meitystartuphub.in/ | https://www.ficci.in/ | https://www.thedialogue.co/

Suggested Citation

Agarwal, B., Saxena, G. and Sharma, V. (2023, August). India's Digital Revolution: Charting the Future of Secure Digital Infrastructure. Meity Start-up Hub, FICCI & The Dialogue™.

Publication Date

August 17, 2023

Disclaimer

CONTENTS

1. INTRODUCTION

India's journey towards digital transformation has gained immense momentum over the past years, further accelerated by the challenges and opportunities presented by the COVID-19 pandemic. A significant shift to remote working and online communications has resulted in a remarkable surge in internet users. Mobile broadband subscribers have nearly doubled in five years, from 345 million to 765 million.[1] Notably, an impressive 69% of organisations in India now position themselves as "Digital Businesses" armed with robust digital strategies and capabilities.[2] The health and human services sector leads the pack, showcasing the nation's highest digital technology adoption rate.[3]

1.1 The Cybersecurity Challenge

However, this remarkable digital evolution has its challenges. We have seen an alarming increase in cybercrimes, from identity thefts to vast data breaches. With our global supply chains intricately intertwined, a single vulnerability can jeopardise multiple stakeholders. A staggering 40% of cyber threats exploit these vulnerabilities through indirect supply chain attacks. The World Economic Forum's annual report, The Global Cybersecurity Outlook 2022, accentuates the gravity of the situation – 80% of cyber leaders view ransomware as a considerable threat to public safety.[4] Per the cybercrime report of 2022, the cost of cybercrime is predicted to hit US $8 trillion in 2023 and will grow to US $10.5 trillion by 2025.[5] Even emerging technologies like IoT devices, including GPS trackers and smart wearables, are not spared from these cyber threats.[6] The fallout from these cyber onslaughts is multifaceted,

[1] EY India. (2023, February 7). *Digitaliasing India: A force to reckon with*. https://www.ey.com/en_in/india-at-100/digitalizing-india-a-force-to-reckon-with

[2] International Data Corporation. (2023, June 1). *69% of Organizations in India Identify as "Digital Businesses" With a Clear Digital Strategy and Technology Integration, Finds IDC*. https://www.idc.com/getdoc.jsp?containerId=prAP50777523

Gupta, N., Ponnala, R., & Srinivasamurthy, S. (2023). *Digital Transformation Adoption — Industry Priorities and Focus Areas*. International Data Corporation. https://www.idc.com/getdoc.jsp?containerId=AP50372423

[3] EY India. (2021, March 18). *India has among the highest adoptions of digital technologies by health and human services organizations: EY Imperial College London Survey*. https://www.ey.com/en_in/news/2021/03/india-has-among-the-highest-adoptions-of-digital-technologies-by-health-and-human-services-organizations

[4] World Economic Forum. (2022). *Global Cybersecurity Outlook 2022*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

[5] Morgan, SC. 2022 Official Cybercrime Report. *Cybersecurity Ventures* https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

[6] Griffiths, C. (2023, August 4). *The Latest Cyber Crime Statistics*. AAG IT Services. https://aag-it.com/the-latest-cyber-crime-statistics/

ranging from data destruction, financial losses, operational disruptions, to significant reputational damage.[7] The gravitas of the situation is underscored by the fact that cybersecurity has now become a matter of national security.

1.2 Government Initiatives and Investment in Cybersecurity

Governments worldwide have shifted their policy focus accordingly, recognising the pressing need for a fortified cybersecurity framework. India, in particular, has demonstrated a proactive approach. The government has embarked on several measures, ranging from regulatory reforms, strengthening institutional mechanisms, and awareness drives, to cross-industry alliances. Between 2019 and 2022, the government allocated a substantial Rs. 809.58 crores to various cybersecurity initiatives. The 2023-24 budget has further earmarked Rs. 400 crores under the Ministry of Electronics and Information Technology (MeitY) for Cyber Security projects and Rs. 225 crores for the Indian Computer Emergency Response Team (CERT-In).[8]

1.3 India's Growing Footprint in the Global Cybersecurity Landscape

This proactive governmental approach has significantly empowered the private sector, fostering innovation and bolstering cybersecurity practices. The fruits of these efforts are evident – India has proudly secured a position in the top 10 of the International Telecommunication Union-Global Cybersecurity Index amongst 180 countries.[9] India's digital journey, characterised by its remarkable accomplishments, spans across IT services, e-commerce, digital payments, and software development.

While the global IoT market is projected to escalate to US $1,854.76 billion by 2028, India's share is expected to witness a growth rate of 17.05%, culminating in a market size of US$60 billion in 2028.[10] The cybersecurity segment, a critical component of the IoT industry, is

[7] Cybersecurity Ventures. (2022). *2022 Official Cybercrime Report*. https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf?utm_medium=email&utm_source=pardot&utm_campaign=autoresponder

[8] Yadav, P. (2023, February 2). Government allots Rs 225 crores to cybersecurity response team and Rs 400 to cybersecurity projects. *CNBC TV18*. https://www.cnbctv18.com/finance/budget-2023-government-allots-rs-225-crores-to-cybersecurity-response-team-and-rs-400-crores-to-cybersecurity-projects-15791861.htm

[9] International Telecommunication Union, Global Cybersecurity index, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[10] Statista. *The Internet of Things- India*. https://www.statista.com/outlook/tmo/internet-of-things/india#:~:text=Revenue%20in%20the%20IoT%20market,US%2460bn%20by%202028.

forecasted to expand at a CAGR of 12.87%, achieving a market size of US$4.57bn by 2028.[11] The flourishing cybersecurity landscape in India is further propelled by the integration of AI and ML technologies, augmented focus from regulators, increased budgetary allocations, and the demographic dividend of a young population eager to engage with digital platforms. In this era of global interconnectivity, cybersecurity's significance is paramount, especially in a nation as diverse and dynamic as India.

1.4 India's Digital Rise and the Imperative for Cybersecurity

With unwavering government support, innovation, and resilience, Indian cybersecurity startups are poised for global leadership. Their groundwork positions India as a forthcoming global cybersecurity titan.

India's rapid digitalisation has transformed its socio-economic framework, introducing many opportunities. However, this digital ascent is shadowed by looming cyber threats that could impede our progress. The demand for rigorous cybersecurity intensifies as technology permeates sectors like e-governance, finance, healthcare, and education. It is a technological necessity and a national imperative intertwined with India's holistic progress.

Digital proliferation, while enhancing transparency in governance, cashless economies, and accessibility in sectors like health and education, also underscores the pivotal role of cybersecurity. Balancing the promise of digitalisation while shielding against cyber threats is crucial. A multifaceted strategy integrating governmental regulations, public awareness, technology, and global alliances, is critical to navigating this digital era safely.

India's commitment to cybersecurity is evident in its strategic approach, positioning the nation not only as a protector of its present digital assets but also as a guarantor for a secure digital future. As we strengthen our global digital footprint, the emphasis on cybersecurity is paramount. With concerted efforts from all sectors, India is charting a course towards being a global cybersecurity exemplar, ensuring a safe and impactful digital journey.

[11] Statista. *Cyber Security-India*. https://www.statista.com/outlook/tmo/cybersecurity/india#:~:text=Revenue%20in%20the%20Cybersecurity%20market,US%244.57bn%20by%202028.

2. INDIA'S CYBERSECURITY INITIATIVES

In the dynamic digital landscape, cybersecurity stands as a bulwark against potential threats, aiming to shield crucial data and systems from unauthorised access and potential harm. Defined by Section 2(1)(nb) of the Information Technology Act, 2000, "cybersecurity" in India focuses on safeguarding *"information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction."*[12] With rapid technological advancements, the imperative is to ensure swift recovery from electronic communication networks, information systems, or industrial process control systems following any cyber anomalies or attacks.[13]

2.1 Foundational Regulatory and Policy Frameworks

Delving into the fabric of India's cybersecurity framework, we traverse through its robust regulatory pillars and strategic vision. At the heart of this ecosystem lies a nexus of legislative acts, policies, and dedicated regulators, each driving the nation's agenda of fortified cyberspace. It is indeed a testament to India's commitment to safeguarding its cyber frontiers against emerging challenges.

INFORMATION TECHNOLOGY ACT, 2000

India, prior to the advent of the Information Technology Act, 2000 (IT Act), lacked a comprehensive legal framework addressing cybersecurity.[14] This seminal Act laid the groundwork for safeguarding critical information infrastructure (CII), marking distinct areas warranting cybersecurity focus. Section 70 distinctly identifies CII as resources whose "incapacitation or destruction would severely impede national security, economy, public health or safety."[15] Further bolstering this, the Act facilitated the establishment of the National Critical Information Infrastructure Protection Centre (NCIIPC) in 2014,[16] designed to shield CIIs from

[12] The Information technology Act, 2000, S. 2(1)(nb). https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[13] Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for People and Organizations. *Journal of Library Administration*, 54(1), 46–56. https://doi.org/10.1080/01930826.2014.893116

[14] Joshi, D. *A comparison of legal and regulatory approaches to cyber security in India and the United Kingdom*. The Centre for Internet & Society. https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf

[15] The Information technology Act, 2000, S. 70. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[16] National Critical Information Infrastructure Protection Centre https://www.nciipc.gov.in/.

myriad threats. In tandem, the CERT-In was set up to manage 'cybersecurity incidents' in non-critical sectors.[17] Since its inception in 2004, CERT-In has been at the forefront of India's cybersecurity efforts.

NATIONAL CYBERSECURITY POLICY, 2013

A testament to India's proactive stance, the Ministry of Communication and Information Technology unveiled the National Cybersecurity Policy in 2013,[18] accentuating a secure online space, enhancing cyberattack alert systems, and synchronising with global best practices. Recognising the evolving digital threats, a revision of this policy is currently underway, spearheaded by a dedicated task force.[19] Adding to this, the National Security Council Secretariat (NSCS) earlier declared the drafting of a National cybersecurity Strategy, aiming for a comprehensive approach towards safeguarding India's cyberspace.[20]

INDIAN CYBER SECURITY REGULATORS

While multiple governmental institutions oversee various facets of cybersecurity,[21] no singular central authority holds the mandate for its overarching policy formulation. Nevertheless, several pivotal ministries and institutions have emerged as torchbearers in sculpting India's cybersecurity blueprint.

Table 1: Regulators in the Indian Cybersecurity landscape

MEITY	MeitY is the leading government institution in shaping cybersecurity policies in India. Beyond policy blueprinting and regulatory supervision, MeitY fervently drives research and innovation. Collaborating closely with academia and R&D labs, it spearheads pioneering research tailored to address intricate cybersecurity challenges.[22]

[17] The Information technology Act, 2000. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[18] Ministry of Electronics and Information Technology. *National Cyber Security Policy-2013*. https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf

[19] (2023, February 20). National Cybersecurity Strategy 2023 may come out soon: Pant. *The Economic Times*. https://telecom.economictimes.indiatimes.com/news/national-cybersecurity-strategy-2023-may-come-out-soon-pant/98093316

[20] Pandey, D.K. (2022, December 14). Draft cybersecurity strategy has been formulated: Centre. *The Hindu*. https://www.thehindu.com/news/national/national-security-council-secretariat-formulated-draft-national-cyber-security-strategy-centre/article66262515.ece

[21] Ranganathan, N. (2021, March 21). *Watchtower: An interactive map of cybersecurity institutions in the Government of India*. Internet Democracy Project. https://internetdemocracy.in/2016/03/an-interactive-map-of-cybersecurity-institutions-in-the-government-of-india

[22] Ministry of Electronics & Information Technology. *R & D in Cyber Security*. https://www.meity.gov.in/content/cyber-security-r-d

CERT-in	CERT-In, established under the IT Act in 2004, has remained an influential entity in fortifying India's cyber defences. Growing instances of cyber-terrorism both globally and domestically in the last decade catalysed the crystallisation of robust cybersecurity protocols.[23] Consequently, in 2008, the IT Act underwent amendments to specify CERT-In's responsibilities, broadening its scope to counter diverse cyber threats, including cyber-terrorism, identity theft, and data protection.[24]
NCIIPC	Established via a Gazette of India notification in 2014, the National Critical Information Infrastructure Protection Centre (NCIIPC) operates under a clearly defined charter. Its mission is to adopt comprehensive measures to ensure the protection of Critical Information Infrastructure against myriad threats, thereby fostering coordination, synergy, and raising awareness on information security among all stakeholders.[25] In this interconnected framework, CERT-In holds the responsibility to report significant cybersecurity incidents from critical sectors to NCIIPC.

2.2 Innovative Endeavours in Cybersecurity within India

In an era of swift digital transformation, India's proactive stance towards establishing and bolstering its cybersecurity framework is notably prominent. Recognising the escalating threats to its vast digital domain, the Indian government has channelled its resources and expertise into fostering innovative endeavours in cybersecurity. India's dedication to cybersecurity mirrors a comprehensive vision of a safe digital future, from enhancing the nation's resilience against botnet infections to fortifying its criminal justice IT systems. The table below highlights some pioneering initiatives, emphasising the country's commitment to a secure digital realm.

Table 2: Key Initiatives in the in the Indian Cybersecurity landscape

Cyber Swachhta Kendra	A critical part of MeitY's Digital India campaign, the Cyber Swachhta Kendra aims to create a fortified cyber ecosystem in India.[26] Under CERT-In, mandated by Section 70B of the IT Act, 2000, this center focuses on identifying and resolving botnet infections nationwide. The end goal is a digital environment resilient against cyber threats, reflecting the ethos of the National Cybersecurity Policy.

[23] Ministry of Electronics and Information Technology, *Guidelines on Information Security Practices" for Government Entities for Safe & Trusted Internet*. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1936470

[24] Joshi, D. *A comparison of legal and regulatory approaches to cyber security in India and the United Kingdom*. The Centre for Internet & Society. https://cis-india.org/internet-governance/files/india-uk-legal-regulatory-approaches.pdf

[25] National Critical Information Infrastructure Protection Centre (https://www.nciipc.gov.in/).

[26] Ministry of Electronics and Information Technology, *Cyber Swacchta Kendra*. https://www.csk.gov.in/

Inter-operable Criminal Justice System	The ICJS, envisioned by the Supreme Court's e-Committee and run by the Ministry of Home Affairs vide National Crime Records Bureau and National Informatics Centre, offers an integrated platform that unifies IT systems pivotal to India's Criminal Justice.[27] ICJS facilitates seamless data exchange across the gamut of the criminal justice spectrum—spanning courts, enforcement agencies, correctional entities, and forensic labs—under a unified integrated framework. With objectives such as streamlining data sharing, devising a centralised crime-related repository, orchestrating comprehensive reporting mechanisms, and fostering a robust network for secure data interchange and video conferencing, the ICJS embodies innovation.
Indian Cyber Crime Coordination Centre	Initiated in 2018 under the Ministry of Home Affairs, the I4C signifies a consolidated approach to combat cybercrime.[28] Designed to foster synergy among law enforcement agencies and stakeholders, its mission is to boost India's capacity to address cybercrimes and enhance citizens' trust in the digital realm.
Information Security Education and Awareness Project	Launched in 2014 by MeitY, the ISEA Project Phase II strives to elevate Information Security competence.[29] It focuses on upskilling, training government personnel, and enhancing public awareness. The initiative aims for comprehensive Information Security education, creating an informed workforce and widespread understanding of its principles.

[27] Centre approves project to connect pillars of Criminal Justice System. *The Indian Express*. (2022, February 19). https://indianexpress.com/article/india/govt-approves-project-to-connect-pillars-of-criminal-justice-system-7780642/

[28] Indian Cybercrime Coordination Centre (I4C) I4C, Ministry of Home Affairs, Government of India. https://i4c.mha.gov.in/about.aspx

[29] Information Security Education and Awareness (ISEA) Project Phase-II, MeitY, Government of India. https://isea.gov.in/aboutus.php

3. CYBERSECURITY INDUSTRY IN INDIA

India's cybersecurity industry is on an unprecedented growth trajectory, spurred by rapid digital transformation and the increasing fusion of physical and digital realms. The nation, famous for its IT prowess and innovative capabilities, is addressing the mounting cybersecurity challenges with a multifaceted approach. From the evolution of its digital landscape, marked by pioneering tech initiatives, to the surge of visionary cybersecurity startups, India is fortifying its digital defenses. The commendable achievements of National Start-up Award winners further attest to India's innovative spirit in this domain. Moreover, Indian-origin entrepreneurs are making significant inroads in the global cybersecurity scene, showcasing the nation's expanding influence and potential as a global leader in ensuring digital safety and resilience. This chapter delves into these facets, painting a picture of the current state and promising future of the cybersecurity industry in India.

3.1 The Evolution of India's Digital Landscape

The lines between the physical and digital worlds are becoming increasingly indistinct. As businesses and individuals navigate this transformation, the need for a robust digital infrastructure is paramount. India has established itself as a global technology powerhouse, recognised for its thriving IT services and digital innovation. This rapid growth is propelled by a fusion of skilled tech professionals, an innovation-centric environment, and a relentless pursuit of cutting-edge technologies. Moreover, pioneering initiatives, from 5G rollouts to diverse digital platforms, further boost India's digital prowess.

However, these technological advancements come with inherent risks, presenting opportunities for malicious cyber activities. The 3.63 million cybersecurity incidents recorded by CERT-IN between January 2019 and June 2022 highlight the pressing concerns.[30] Hence, robust cybersecurity is no longer optional—it's indispensable.

Indeed, cybersecurity is the cornerstone of the digital economy. Every technological advance adds complexity to the cyber landscape, posing threats that could endanger businesses,

[30] *Rising focus on cybersecurity in India | IBEF*. India Brand Equity Foundation. https://www.ibef.org/blogs/rising-focus-on-cybersecurity-in-india

compromise data, and undermine public trust. With interconnected systems and the proliferation of digital platforms, cybersecurity remains a central component of any progressive digital strategy.

3.2 Startup-Driven Transformation of India's Secure Digital Infrastructure

The booming cybersecurity sector underscores its pivotal role. In just four years (2021-2025), revenue from cybersecurity solutions is projected to surge from $9.85 billion to a remarkable $13.6 billion.[31] This growth exemplifies the increasing demand for comprehensive cybersecurity measures in response to escalating threats. As our lives become increasingly digital, the need for cutting-edge cybersecurity measures becomes paramount, driving the development of tailored solutions.

India's vibrant startup ecosystem is responding with agility and innovation. As a hub for tech advancements, India provides a conducive environment for cybersecurity startups. The Cyber Security Task Force (CSTF), a venture by DSCI and NASSCOM, envisions a $35 billion valuation for the cybersecurity sector by 2025. Moreover, the CSTF aims to facilitate the emergence of a million cybersecurity roles and foster the growth of 1,000 startups by 2025.[32] Given this momentum, India's cybersecurity market is set to experience robust growth over the next five years.

The ascent of Indian cybersecurity startups reflects the nation's technological prowess and entrepreneurial spirit. Not only are these startups competing on a global scale, but they are also shaping the future of cybersecurity. Through continuous innovation and adaptation, they are committed to ensuring a secure digital future for all.

[31] International Trade Administration. (n.d.), *India - Information and Communication Technology*, International Trade Administration | Trade.gov. Retrieved August 10, 2023, from https://www.trade.gov/country-commercial-guides/india-information-and-communication-technology#:~:text=Revenues%20in%20India's%20cybersecurity%20services,infrastructure%20sectors%20continue%20to%20expand.

[32] Growing Cybersecurity Industry, Roadmap for India, DSCI, NASSCOM, 2016.

3.3 Incentivising growth

In recent years, India has witnessed a dynamic shift in the cybersecurity landscape, driven by an array of innovative start-ups that have risen to global prominence. Recognising this burgeoning potential, the National Start-up Awards stands as a beacon, honouring those at the forefront of this revolution.

In 2020, Staqu Technologies made waves with its groundbreaking approach to analysing crime data, setting new standards in speaker identification.[33] They have carved a niche by aiding police forces across India in digitising and managing criminal records efficiently. Meanwhile, Lucideus Tech embarked on a mission to simplify cybersecurity.[34] Their flagship product, SAFE, offers an objective assessment of an organisation's cyber risk, marking a transformative step in the realm of cybersecurity.

As 2021 rolled in, the brilliance of Pivotchain Solutions came to the fore.[35] This start-up stands as a testament to the power of AI-driven video surveillance, redefining real-time video intelligence and surveillance. On the other side of the spectrum, Sequretek IT Solutions took a holistic approach.[36] Their comprehensive cybersecurity solutions span from device security to user behaviour, showcasing the depth of their innovation.

By 2022, the spotlight was on Qunu Labs, a start-up championing quantum-safe data encryption.[37] Their suite of solutions promises robust protection against current and future threats, reinforcing India's position on the global cybersecurity map. Complementing this quantum leap, Atom Alloys emerged with its patented explosion prevention technology,

[33] *National Startup Awards, 2020*. Department for Promotion of Industry and Internal Trade, Ministry of Commerce and Industry, Government of India. https://www.startupindia.gov.in/content/dam/invest-india/nsa/National%20Startup%20Awards%202020.pdf

[34] *National Startup Awards, 2020*. Department for Promotion of Industry and Internal Trade, Ministry of Commerce and Industry, Government of India. https://www.startupindia.gov.in/content/dam/invest-india/nsa/National%20Startup%20Awards%202020.pdf

[35] *National Startup Awards, 2021.* Department for Promotion of Industry and Internal Trade, Ministry of Commerce and Industry, Government of India.
https://www.startupindia.gov.in/content/dam/invest-india/CTB-12th%20Jan%2022.pdf

[36] *National Startup Awards, 2021.* Department for Promotion of Industry and Internal Trade, Ministry of Commerce and Industry, Government of India.
https://www.startupindia.gov.in/content/dam/invest-india/CTB-12th%20Jan%2022.pdf

[37] *National Startup Awards, 2022*. Department for Promotion of Industry and Internal Trade, Ministry of Commerce and Industry, Government of India. https://www.startupindia.gov.in/nsa2022results/assets/File/NSA%202022%20Report%20Final.pdf

ensuring safety from fuel and gas tank explosions and underscoring the importance of integrating safety with innovation.[38]

Collectively, these trailblazing start-ups signify the prowess of the Indian cybersecurity ecosystem. Their achievements, accentuated by the National Start-up Awards, epitomise the promising journey ahead for the Indian cybersecurity industry. With unwavering governmental support and a thriving innovative spirit, the future holds immense promise for India's digital security landscape.

3.4 India's Steady Growth in Cybersecurity Innovation

The global cybersecurity landscape is witnessing a subtle yet significant imprint of startups led by Indian-origin entrepreneurs. Among the many making waves are ventures like US-based Securonix, Singapore-based CloudSEK,[39] and UK-based Zyber 365.[40] While their headquarters may be overseas, their operational and leadership core resonates with India's ethos. A shining example is Zyber 365, which recently raised US $100 million in its Series A round. Co-founded by Indian-origin innovators Pearl Kapur and Sunny Vaghela in 2023, the company seamlessly integrates advanced cybersecurity with a dedication to environmental sustainability.

This upward trajectory illustrates the potential that Indian talent holds in the cybersecurity realm. With digital threats on the rise, the global appetite for innovative cybersecurity solutions is growing. Positioned with an extensive reservoir of tech professionals and a thriving startup environment, India is gradually marking its territory. The nation is not just adapting but is also making headway as an influencer in the global cybersecurity arena, channeling its innovation prowess and knowledge to pioneer the field.

[38] *National Startup Awards, 2022*. Department for Promotion of Industry and Internal Trade, Ministry of Commerce and Industry, Government of India. https://www.startupindia.gov.in/nsa2022results/assets/File/NSA%202022%20Report%20Final.pdf

[39] Sangwan, M. (2022, May 08). These 6 Indian origin cybersecurity startups are redefining digital security landscape. *YourStory*. https://yourstory.com/2022/05/indian-cybersecurity-startups-securonix-wijungle-securden-cloudsek-securethingsai

[40] (2023, July 26). Web3 Startup Zyber 365 Raises $100 Mn, Becomes India's First Unicorn In 2023. BW Business World. https://www.businessworld.in/article/Web3-Startup-Zyber-365-Raises-100-Mn-Becomes-India-s-First-Unicorn-In-2023/26-07-2023-485515/

4. GLOBAL SCALABILITY

India's emergence in the secured digital infrastructure ecosystem highlights the nation's steady growth in the digital safety domain. Building on its IT foundations and a growing start-up ecosystem, India is making its mark on the global stage. From government-led initiatives to harness the vast internal market to fostering international collaborations, this chapter delves deep into India's strategic moves to champion a secured digital infrastructure ecosystem. Through its visionary policies, India is not just navigating but pioneering the global cybersecurity realm, highlighting its unwavering commitment to a safer digital future for all.

4.1 Digital Dominance and India's Global Cybersecurity Evolution

India, with its rich IT heritage and a treasure trove of talent, is poised to pioneer cybersecurity innovation. The nation's ascent as a global IT powerhouse, spearheaded by tech stalwarts such as Infosys, Tata Consulting Service, and Wipro, exemplifies its technological acumen. This strong foundation not only attests to its past achievements but also sets the stage for India to specialise further in the realm of cybersecurity.

Over the past decade, India's start-up landscape has been a hotbed of innovation, particularly in cybersecurity. Leading this surge are cities like Bangalore, Hyderabad, and Pune, which are quickly establishing themselves as global hubs of cybersecurity innovation. Moreover, these burgeoning start-ups are not solely focused on domestic markets; they have captivated international audiences, securing clients from every corner of the world.

Acknowledging the paramount importance of cybersecurity in our increasingly digital world, the Indian government has undertaken a series of critical strategic alliances with countries such as the USA,[41] Australia,[42] and Japan[43]. These partnerships not only foster knowledge exchange

[41] United States and India Sign Cybersecurity Agreement, July 19, 2011, https://www.dhs.gov/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement

[42] Australian-India Cyber and Critical Technology Partnership: Grant Round 2, https://india.highcommission.gov.au/ndli/AICCTP.html

[43] India-Japan sign Memorandum of Cooperation in the field of Cybersecurity, October 7, 2020, https://indbiz.gov.in/india-japan-sign-memorandum-of-cooperation-in-the-field-of-

but also provide India with the dual opportunity to assimilate global best practices and showcase its pioneering advancements.

India's digital evolution, propelled by its status as the world's second-most populous nation, indicates a vast internal market brimming with opportunities. Government-led digital drives, encompassing Aadhaar, digital payments, and e-governance, underscore the nation's intrinsic need for impeccable cybersecurity measures. Each year, India moulds millions of IT graduates. By redirecting this prodigious talent towards cybersecurity and fortifying it with specialised training, India can create a vanguard poised to tackle global cyber challenges.

The thriving ecosystems of Bangalore, Hyderabad, and Pune can very well be the cradle for avant-garde cybersecurity solutions. Furthermore, government campaigns like 'Make in India' and 'Start-up India', bolstered by incentives for tech enterprises, are powerful catalysts that can spur cybersecurity product innovation.

Harnessing global partnerships, spanning academia and business sectors, can be a conduit for invaluable knowledge exchange. These synergistic collaborations can amplify research, attract foreign investment, and pave the way for Indian cybersecurity products to capture the global market. One of India's distinctive strengths lies in delivering premium solutions at competitive price points. This ability equips Indian cybersecurity products to cater to a diverse clientele, ranging from small enterprises to global conglomerates, thus enhancing their appeal on the international platform.

Furthermore, India's geopolitical stance gives it a unique insight into regional cyber threats, enabling it to craft bespoke solutions addressing specific regional cyber challenges.

4.2 Catalysts to Change through Government-led Initiatives

The Indian government, ever cognizant of the crucial role of cybersecurity in our digital age, has been at the forefront of advocacy and action in this domain. Highlighted below are some stellar initiatives:

cybersecurity/#:~:text=India%20and%20Japan%20recently%20signed,mutual%20interest%20regarding%20the%20same.&text=The%20Indo%2DJapan%20MoC%20is,5G%2C%20IoT%2C%20AI%20etc.

Table 3: Government-led Initiatives in India

Cyber Surakshit Bharat Initiative	A joint venture between the MeitY and industry trailblazers, this initiative is geared towards enhancing cybersecurity awareness and upskilling professionals.[44]
Digital India Campaign	While its primary aim is digital empowerment of citizens, a cornerstone of this initiative is 'Secure Cyberspace', underscoring cybersecurity's pivotal role in India's digital odyssey.[45]
Cybersecurity Skill Development	Realising the domain's skill gap, the government has forged ties with academia to usher in specialised cybersecurity courses and training regimens.
Collaborative Framework	India has fortified its cybersecurity capabilities through global partnerships, facilitating knowledge transfers and joint ventures.
Promotion of R&D	The government, through assorted schemes and grants, is fuelling research and innovation in cybersecurity, ensuring indigenous solutions for distinct challenges.
Public-Private Partnerships	The government's collaboration with the private sector, tapping into their expertise, epitomises its holistic approach towards devising and deploying formidable cybersecurity solutions.[46]
BharatNet Project	In tandem with its mission to provide high-speed internet to rural precincts, the government is zealously ensuring these connections are fortified against cyber threats.
Data Protection and Privacy	The Digital Personal Data Protection Act, 2023, enshrines the protection of individual data, setting stringent cybersecurity benchmarks for all entities handling personal data.

These concerted efforts and visionary policies bear witness to the Indian government's dual commitment to fostering digital solutions and ensuring that they are resilient, secure, and beneficial for its citizenry and institutions. The future beckons with promise, and India is unequivocally charting its path towards a secure and innovative digital infrastructure.

[44] Cyber Surakshit Bharat Initiative, Ministry of Electronics and Information Technology, https://www.meity.gov.in/writereaddata/files/Cyber%20Surakshit%20Brochure_.pdf

[45] Digital India: A programme to transform India into a digitally empowered society and knowledge economy, Ministry of Electronics and Information Technology, https://www.meity.gov.in/sites/upload_files/dit/files/Digital%20India.pdf

[46] Microsoft joins forces with Ministry of Skill Development and Entrepreneurship to train youth in digital and cybersecurity skills, June 1st, 2023, https://news.microsoft.com/en-in/microsoft-joins-forces-with-ministry-of-skill-development-and-entrepreneurship-to-train-youth-in-digital-and-cybersecurity-skills/

4.3 Investing in India's Secure Digital Infrastructure

India's burgeoning cybersecurity sector stands on the brink of a transformative evolution, brimming with abundant opportunities for growth. With unwavering support from the government, pioneering contributions by Indian-origin founders, and insights gleaned from global cybersecurity ventures, the sector is well-equipped to overcome challenges and achieve commendable progress. To establish India as a vanguard in the secured digital infrastructure domain, a collaborative approach is paramount amongst all stakeholders. The focal areas of opportunity include:

ENHANCING AWARENESS AND CULTURAL PARADIGM SHIFT

The nexus of opportunity lies in amplifying robust awareness campaigns targeted at businesses, particularly small to medium-sized enterprises. Illuminating the paramount significance of cybersecurity can empower startups to establish their solutions as quintessential, fostering enhanced uptake of products and services. Additionally, hosting enlightening workshops and seminars can pivot the perception of cybersecurity from being solely an IT concern to a pivotal business imperative, reinforcing its essence across all organisational echelons.

TALENT DEVELOPMENT

India's teeming reservoir of tech-adept professionals presents a golden opportunity. Through symbiotic collaborations with academic institutions and proffering skill-centric training[47],startups can bridge the existing talent chasm, cultivating a proficient cybersecurity workforce in the process.

INVESTMENT INITIATIVES

By accentuating the indispensable role of cybersecurity in the contemporary digital arena, startups can magnetise concentrated investments. Aligning with industry luminaries and presenting cybersecurity as an elemental technological cornerstone can captivate investor interest. The government's recent promulgation of the Digital Personal Data Protection Act, 2023[48] reinforces the imperative for a fortified digital infrastructure, emphasising user privacy and elevating cybersecurity as a sine qua non for entities operating within India.

[47] Singh, A. (2023, June 29). Why there is still shortage of cybersecurity professionals in India?. The Week. https://www.theweek.in/news/sci-tech/2023/06/29/why-there-is-still-shortage-of-cybersecurity-professionals-in-the-country.html#:~:text=As%20per%20a%20recent%20report,by%20the%20end%20of%202023.

[48] Digital Personal Data Protection Act, 2023

INFRASTRUCTURE AUGMENTATION

Leveraging India's swiftly advancing digital infrastructure enables startups to avail themselves of essential tools and seamless connectivity. Forging public-private partnerships can exponentially amplify accessibility to critical infrastructure facets.

AGILE THREAT MITIGATION

By instituting dedicated research and development wings and partnering with international cybersecurity centres of excellence, startups can consistently remain at the forefront of the ever-mutating threat milieu, ensuring their solutions are perennially avant-garde.

Through these amalgamated endeavours of the government, private sector, and academic institutions, India is poised to champion cybersecurity education, awareness, and entrepreneurial ventures. Guided by the acumen of Indian entrepreneurial luminaries and the nation's intrinsic technological prowess, the cybersecurity sector is primed for unparalleled growth and international acclaim.

5. STRENGTHENING GLOBAL CYBER ALLIANCES

Under the stewardship of its G20 presidency, India has emphatically solidified its position as a frontrunner in the ever-evolving world of cybersecurity. The nation's leadership during the G20 presidency has been transformative, underpinning the critical role of cybersecurity and offering a robust platform for global stakeholders.

A poignant G20 meeting on security and AI saw the Hon'ble Home Minister, Amit Shah, highlighting the need for an integrated approach to cybersecurity policies.[49] Such a strategy, he suggested, would fortify information exchange, streamline protocols, and optimise resource allocation.

As the era of digitalisation unfolds, bringing unparalleled transformations in our engagement with the world, India's rising stature in the digital realm showcases its potential as a technological innovator and a pivotal player in global cybersecurity alliances. India, with its rich IT legacy and dynamic start-up ecosystem, is strategically positioning itself as a beacon in the development of a secure digital infrastructure ecosystem. Recognizing the criticality of cybersecurity and the benefits of global cooperation, the Indian government is proactively nurturing international alliances, further strengthening its cybersecurity framework to mitigate cyber threats and tap into the nation's technological expertise.

India understands that addressing cyber threats is not just a national concern but a global imperative. By championing international cybersecurity collaborations, India resonates with the G20's ethos of '*Vasudhaiva Kutumbaka*m - One Earth, One Family, One Future'. The formation of the Digital Innovation Alliance exemplifies India's dedication to a collective approach towards a safer digital world. As India progresses in the digital age, it is not just leveraging its indigenous capabilities but also emphasizing the significance of fostering and nurturing global cyber alliances to ensure a fortified and resilient digital future for all.

[49] Jain, B. (2023, July 14). 'Integrated move must for cyber security.' *The Times of India*. https://timesofindia.indiatimes.com/india/integrated-move-must-for-cyber-security/articleshow/101742044.cms?from=mdr