AMCHAM INDIA

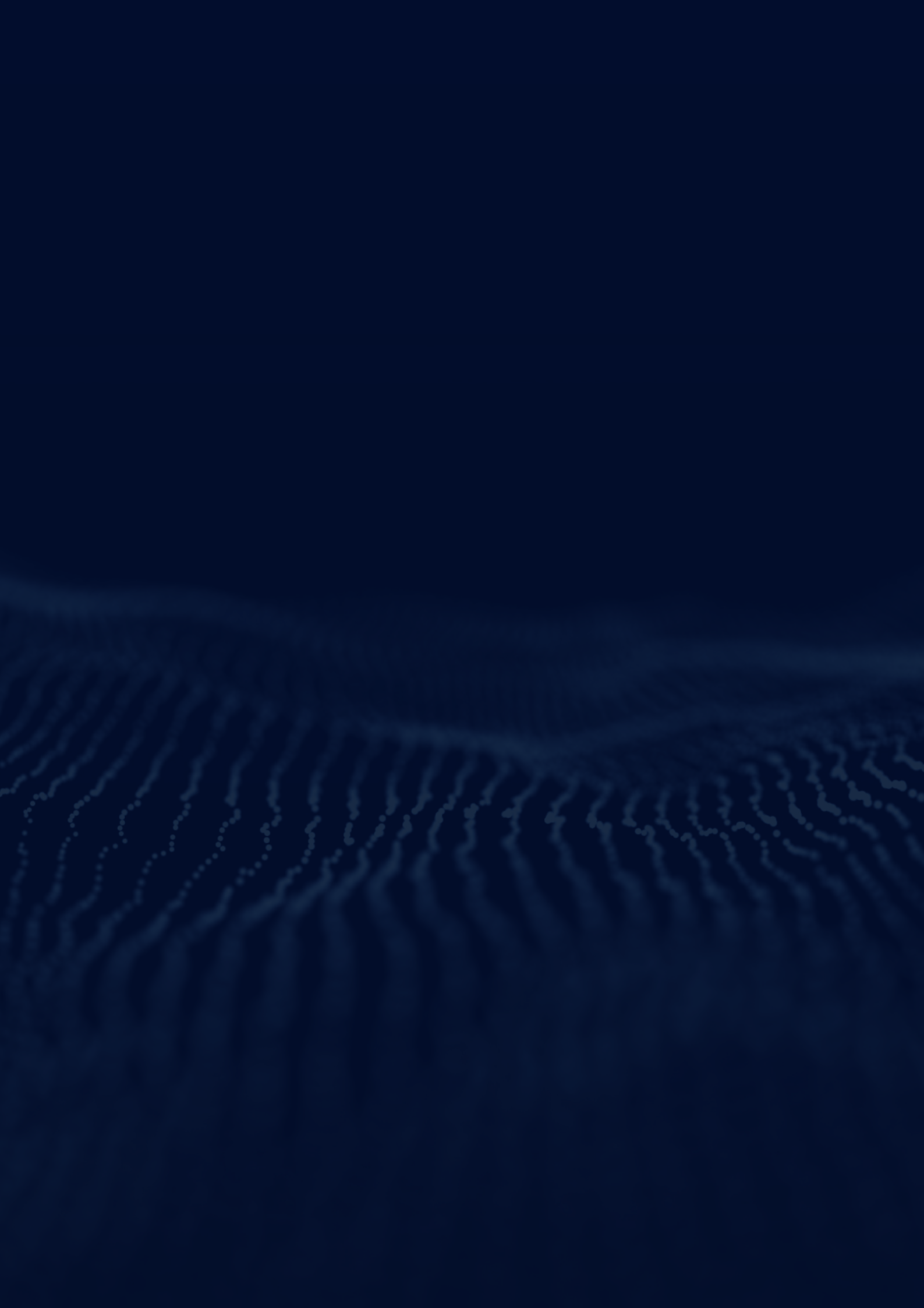
FORTINET

Securing the Digital Future:
Strengthening Cybersecurity in ICT US-India Partnership

January 2025

KOAN

Knowledge Partner



Securing the Digital Future: Strengthening Cybersecurity in ICT US-India Partnership

January 2025

About AMCHAM

The American Chamber of Commerce in India (AMCHAM) is the apex chamber of U.S. industry in India. Established in 1992, AMCHAM has over 400 members spread all over the country. The incumbent U.S. Ambassador to India is the Honorary President of AMCHAM. The chamber enjoys a close relationship with U.S. Embassy officials and receives tremendous support in fulfilling its objectives. Country Heads of leading U.S. companies constitute the elected National Executive Board. The chamber's mission is to assist member companies to succeed in India through advocacy, information, networking and business support services. AMCHAM is headquartered in New Delhi and has regional chapters in Bengaluru, Chennai, Hyderabad, Kolkata, Mumbai and Pune.

Foreword

The landscape of cybersecurity has evolved dramatically since our last white paper in 2020. As we enter 2025 with a new administration in the United States, AMCHAM recognises the crucial juncture that offers unprecedented opportunities to strengthen the U.S.-India strategic partnership, particularly in cybersecurity cooperation. Digital threats know no borders, and this reality has only been reinforced by the increasing sophistication and frequency of cyberattacks targeting both nations' critical infrastructure, businesses, and citizens.

With the advent of Generative AI, cybercriminals have gained powerful new tools to orchestrate sophisticated attacks, making traditional security measures increasingly vulnerable. This technological shift, alongside developments in quantum computing and cloud technologies, has fundamentally altered the cybersecurity landscape, bringing both unprecedented challenges and opportunities for our cyberdefence capabilities. AMCHAM, as the premier body representing U.S. business interests in India, has been at the forefront of facilitating bilateral cooperation in these emerging technology areas. As two of the world's largest digital economies, the United States and India must lead the way in establishing robust cybersecurity frameworks that can adapt to these emerging technologies while fostering innovation and growth.

Yet AI also brings powerful solutions, with advanced threat detection and automated defence mechanisms, emerging as critical tools in the cybersecurity arsenal. Representing 400+ U.S. companies, AMCHAM continues to serve as a vital bridge between these two great nations. Our member companies bring cutting-edge expertise in cybersecurity solutions, and this white paper reflects their collective wisdom and recommendations for strengthening India's cyber resilience. The timing of this report is particularly significant as it coincides with a new chapter in U.S.-India relations under the incoming U.S. administration, offering fresh opportunities for deeper collaboration in critical technology areas. AMCHAM remains committed to fostering this strategic technology partnership through various initiatives, committees and working groups.

Thanks to all stakeholders who contributed to this comprehensive analysis and support India's journey towards becoming a global leader in cybersecurity, while strengthening the U.S.-India strategic partnership. This white paper not only outlines the challenges we face but also provides actionable recommendations for building a secure digital future that benefits both nations.

Ranjana Khanna
Director General CEO, AMCHAM India

Foreword

The digital era has unlocked immense potential for innovation and growth, but it has also brought unprecedented cybersecurity challenges. As two of the world's largest digital economies, India and the United States stand at a pivotal crossroads. Both nations face a shared cybersecurity imperative: safeguarding critical infrastructure, securing emerging technologies, and defending against increasingly sophisticated threat actors in a rapidly evolving cyber threat landscape.

At Fortinet, we have a front-row seat to the dynamic and complex nature of these challenges. From the rise of AI-driven ransomware campaigns to state-sponsored espionage targeting vital industries, the cyber risks we face today are more interconnected than ever, transcending geographical and organizational boundaries. It is in this context that the India-US partnership becomes more significant, enabling the development of shared defensive strategies, fostering innovation, and setting global benchmarks for cybersecurity excellence.

This report highlights several urgent priorities that demand immediate attention: strengthening critical infrastructure in sectors like healthcare, energy, and finance; fostering international collaboration to enhance cybercrime investigations; and ensuring the security of transformative technologies such as AI and quantum computing. Addressing these challenges requires the combined efforts of public-private collaboration and cross-border partnerships to build the resilience needed to secure our digital future.

The insights and recommendations in this report provide a vital roadmap for policymakers, industry leaders, and cybersecurity professionals in both nations. The time to act is now. By turning these insights into tangible initiatives, we can fortify the security of our digital economies and create a safer, more resilient cyber landscape for all.

Vishak Raman
AMCHAM Cyber Security Commitee Chair &
VP Sales South Asia (India , SEA & ANZ), Fortinet

Table of Contents

Executive Summary

Tracing Commonalities in Threat Landscapes

The United States of America and India are faced with a shared urgency for collaboration in addressing emerging cyberthreats, as two of the world's largest economies and most frequent targets of cyberattacks. Both nations have embraced advanced technologies, enhancing their global influence, while also broadening their susceptibility to cyberattacks. There are also striking similarities in the two nations' cyberthreat landscapes in terms of the nature of incidents, the vectors through which these attacks are carried out, and the profiles of threat actors involved. Major trends in the shared threat landscapes of the countries include risks to critical infrastructure, supply chain vulnerabilities, a surge in ransomware incidents, the misuse of commercial spyware, and challenges arising from the malicious use of emerging technologies like AI, machine learning (ML), and the Internet of Things (IoT). Critical sectors such as healthcare, energy, education, banking and finance, manufacturing, IT services, defence, public utilities and telecommunications are among the most frequently targeted. These similarities underscore shared vulnerabilities and highlight the critical areas where collaborative measures could significantly bolster their cyber defences. In fact, the two nations have entered into strategic partnerships across domains, with cybersecurity being a common denominator across many such partnerships.

Shared Priorities and Challenges

An analysis of the shared goals between India and the US in cyberspace should start from a discussion of their strategies to secure their respective digital ecosystems. By examining the commonalities and divergences in their approaches to cybersecurity, we seek to identify the shared goals and policies that shape each nation's defence against the growing spectrum of cyber threats. Through this, we create a broad layout of not only potential areas of collaboration in protecting cyberspace, but also potential technological shortfalls in such collaboration.

Potential Avenues for Collaboration: Across Bilateral, Regional, and Multilateral Forums

The critical importance of cybersecurity in both nations, the emergence of common threat landscapes and priority areas, lead us to a discussion on collaborative efforts between the US and India across bilateral, regional, and multilateral fora to address the two nations' shared priorities. Over the past two decades, the US-India cybersecurity relationship has evolved significantly, transitioning from initial discussions to a strong and multifaceted strategic partnership. This growth has been shaped by changing priorities in response to emerging threats, strengthened mutual trust, and a more advanced recognition of shared challenges in the cyberspace domain. An analysis of the history of US-India bilateral cybersecurity cooperation and cooperation in regional and multilateral forums such as the QUAD, G20, IPEF, etc., reveals six priority areas which form the foundation for future collaborations in the field of cybersecurity. These are:

Critical Infrastructure/Critical Information Infrastructure	**Supply Chain Security**	**Strengthening Law Enforcement Capabilities**
Capacity Building	**Securing Emerging Technologies while Combating Evolving Cyberthreats**	**International Cooperation to build Resilience**

Recommendations for India's National Cybersecurity Strategy

Despite its robust participation in bilateral, regional, and multilateral cybersecurity dialogues, India's approach to cybersecurity remains relatively nascent, highlighting a significant gap in its strategic policy framework. It is imperative for India to craft a forward-looking cybersecurity strategy that not only catches up with global standards but also sets a proactive stance on cybersecurity governance. The above shared priority pillars for US-India are consistent with broader objectives of Indian Cybersecurity Strategy. Our recommendations are summarised as below:

Pillar 1 **Protection of critical infrastructure**	**Pillar 2** **Supply Chain Security**	**Pillar 3** **Strengthening Law Enforcement Capabilities**
Recommendation 1: Sectoral approach to critical infrastructure protection, through the establishment of sector-specific Information Sharing and Analysis Centres (ISACs) in each critical sector: power and energy, banking, financial services and insurance, telecom, transport, government, strategic and public enterprises. ISACs to be administered by NCPIIC.	**Recommendation 1:** Mutual Recognition Agreements (MRAs) to facilitate trusted supply chains, which classify imports from trusted traders as low security risks. MRAs would enable secure and predictable supply chains, while ensuring companies' access to markets of trusted trade partners.	**Recommendation 1:** Nationwide threat intelligence network that integrates government and private sector insights, coordinated by the NCIIPC, which would play a pivotal role in developing and enforcing standardised protocols for secure and efficient sharing of threat intelligence across relevant sectors.
Recommendation 2: Building robust deterrence capabilities by strengthening critical infrastructure defences to make successful attacks prohibitively costly and resource-intensive. Deterrence measures also ensure continued functioning of critical infrastructures during cyberattacks.	**Recommendation 2:** Standardisation of Indian markets in line with global standards.	**Recommendation 2:** Development of advanced threat-blocking technologies that utilise AI and ML to pre-emptively identify and mitigate cyber threats. **Recommendation 3:** Leveraging international threat intelligence sharing initiatives by formalizing partnerships and integrating these efforts into national frameworks.

Pillar 4
Capacity building

Recommendation 1:
Prioritise the development of a skilled, professional, and diverse cybersecurity workforce by expanding educational programs, establishing clear professional standards, and creating defined career pathways to enhance industry competence and readiness.

Recommendation 2:
Enhance cyber awareness by launching nationwide campaigns to educate and inform all citizens about the best practices in digital hygiene, thereby improving individual and collective cybersecurity across the country.

Pillar 5
Leveraging Emerging Tech

Recommendation 1:
Prioritise initiatives under the National AI Initiatives, such as the IndiaAI Mission, to develop AI-led cybersecurity solutions for priority sectors and expedite the establishment of an AI Safety Institute to ensure the safe development and deployment of AI technologies.

Pillar 6
Global cooperation/ International Cooperation

Recommendation 1:
Enhance India's representation at international forums and standard-setting organizations such as the International Standards Organization (ISO), International Electrotechnical Commission (IEC), and International Telecommunications Union (ITU) to actively contribute to and accelerate the development and implementation of global cybersecurity standards.

Recommendation 2:
Drive efforts to incorporate comprehensive cybersecurity clauses into bilateral and plurilateral trade and investment agreements, ensuring robust cybersecurity measures are integrated within international trade frameworks.

Chapter I: **Introduction**

The United States of America (US) and India, as two of the world's largest economies and most frequent targets of cyberattacks, face a shared urgency to collaborate on addressing escalating cyberthreats. In 2023, India accounted for 13.7 percent of global cyberattacks, the highest proportion worldwide, while the US followed closely at 9.6 percent. As significant actors on the global stage, both nations hold substantial influence in economic, geopolitical, and security realms. Both have embraced technology—with the US as an established leader and India rapidly advancing—to enhance their global positions. Their shared interests have led to strategic partnerships across these domains. Cybersecurity is a common denominator in all of these domains. The increasing utilisation of advanced technologies such as Artificial Intelligence (AI) by malicious state and non-state actors has significantly escalated both the scale and severity of cybersecurity threats. Additionally, the deeper integration of technologies with cloud services, along with the expansion of 5G and the emergence of 6G networks, has broadened the attack surface, making cybersecurity an increasingly central aspect of many relationships.[1]

Both countries have recognised cybersecurity as a critical national priority and have launched various initiatives domestically while actively participating in international forums. Given that cyber threats transcend national borders and are amplified by a diverse array of state and non-state actors and the malicious use of advanced technologies, addressing these challenges exceeds the capability of any single nation. Although existing international forums like the UN's Open-ended Working Group (OEWG) and the Group of Governmental Experts (GGE) have made important strides, substantial challenges remain due to the difficulty of achieving consensus on complex issues across different national approaches. The prioritisation of consensus often results in resolutions that do not fully address the complexities of modern cybersecurity challenges.[2] Moreover, the increasing politicisation of these forums has also impeded the development of enforceable international laws.

These factors point to an enhanced need for bilateral collaboration for cybersecurity between the two nations. The US-India government-to government relationship saw significant growth since 2016, with the signing of the Framework for the US-India Cyber Relationship. This framework emphasises joint efforts in cybersecurity information sharing, capacity building, and fostering innovation in secure technologies.[3] Most recently, India and the US also signed a Memorandum of Understanding (MOU) to enhance cooperation in cybercrime investigations.[4] It aims to step up the level of cooperation and training with respect to the use of cyber threat intelligence and digital forensics in criminal investigations. Such partnerships enable them to present a unified front, share best practices, build mutual capacities, and synergise their efforts. These cooperative ventures not only bolster their cybersecurity defences but also enhance their collective influence in international forums, potentially accelerating progress in global cybersecurity governance initiatives.

This report is an effort in this direction. It establishes that India and the US's shared priorities and existing partnership provide a robust foundation for collaborative efforts in the cybersecurity domain. We argue that such efforts would also offer valuable insights that could inform the ongoing development of India's

Cybersecurity Strategy and present valuable opportunities for India to incorporate global best practices, advanced technologies, and strategic frameworks to strengthen its technological ecosystems and enhance digital resilience.

The report is divided into five Chapters. The following Chapter traces the emerging threat landscape in India and the US and establishes that the two nations share similar vulnerabilities and threats in cyberspace. In the third Chapter, we explore the strategies employed by both India and the US to secure their digital ecosystems, examining commonalities and divergences in their approaches to priority areas within cybersecurity. This analysis helps identify shared goals and distinct policies that shape each nation's defence against the growing spectrum of cyber threats. The exercise is also useful in understanding the technological shortfalls and possible areas of collaboration. In the fourth Chapter, we map out the extensive network of US—India technology partnerships across bilateral, regional, and multilateral forums, to understand what measures are being employed to make advances in prioritised areas within cybersecurity and what more could be leveraged from these forums. The concluding Chapter builds from the shortfall gap in its strategic policy framework, particularly the absence of a comprehensive National Cybersecurity Strategy, offering strategic insights and recommendations and an implementation roadmap that align with both national needs and international best practices.

Chapter II:
Emerging Threat Landscape

Evolving Risks to ICT Technologies in India and the US

This Chapter delves into the cyberthreat landscapes in the US and India, revealing striking similarities in their exposure to increasingly sophisticated risks driven by rapid advancement of technology. An in-depth analysis indicates that both nations encounter a broad spectrum of cyber threats, with notable parallels in the nature of incidents, the vectors through which these attacks are carried out, and the profiles of threat actors involved. These similarities underscore shared vulnerabilities and highlight the critical areas where collaborative measures could significantly bolster their cyber defences.

The trend analysis of cybersecurity threats in both countries reveals consistent patterns in targeted attacks and exploitation techniques. These include threats to critical infrastructure, supply chain exploitation, increase in ransomware attacks, misuse of commercial spyware, and challenges stemming from malicious use of emerging technologies such as AI, machine learning (ML) and the Internet of Things (IoT). Key sectors such as healthcare, energy, education, banking and finance, manufacturing, IT services, defence, telecom and public utilities, are frequently targeted.

These cybersecurity threats arise from a range of threat actors actively exploiting the vulnerabilities or security weaknesses in organisations' networks, hardware devices and software applications, and intentionally causing damage to individuals, organisations or government entities. Most threat actors fall into one or the other category of cybercriminals, cyberterrorists, hacktivists, nation-state actors and even insider threat actors. These threat actors utilise a variety of techniques to achieve this, including malware, phishing attacks, ransomware, data breaches, cyberespionage and DDoS attacks. In addition, these threat actors are sometimes hidden within networks to perform these activities over extended periods, known as advanced persistent threat (APT) attacks. These threat actors target large corporations, small and medium enterprises (SMEs), government organisations and individuals. This Chapter provides a detailed trend analysis of the five most prevalent cyberthreats in India and the US, followed by a tabular summary of significant recent cybersecurity incidents in both nations, based on which our trend analysis has emerged.

I. Threats to Critical Infrastructure or Critical Information Infrastructure

Critical infrastructure is broadly understood as systems, assets, and facilities vital for the functioning of an economy. The US defines critical infrastructure as systems and assets, whether physical or virtual, so vital to the US that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[5] The US has declared 16 sectors as critical infrastructure sectors. These are the chemical, commercial facilities, communication, critical manufacturing, dams, defence industrial base, emergency services, energy, financial services, food and agriculture, government services and facilities, healthcare and public health, information technology, nuclear reactors, material and waste sector, transportation, and water and wastewaters system. India, on the other hand, defines critical information infrastructure as computer

resources, the incapacitation or destruction of which would have a debilitating impact on national security, economy, public health, or safety.

Commonly Impacted Sectors
Government Undertakings
Healthcare
Banking and Finance
Energy
Defence
Public Utilities
Manufacturing

India has declared telecom, health, transport, strategic and public sector entities, banking and insurance, power and energy, and the government sector as critical information infrastructure.[6] In addition to critical information infrastructure, India also recognised 'protected systems' under each of the identified critical information infrastructure categories, which include computer resources that directly or indirectly affect the facility of critical information infrastructure. Several computer resources and systems are identified as protected systems.[7] In recent years, the digitalisation of these sectors has dramatically increased their vulnerability to cyberattacks. In our analysis, we found commonalities between threat trends in US and Indian critical infrastructure in terms of the sectors impacted, responsible actors and their objectives.

Sectors Impacted

In India, the government sector and essential public services have experienced a notable surge in cyber threats, with approximately 67 percent of entities reporting more than a 50 percent increase in disruptive cyberattacks during the 2022-23 period.[8] The healthcare sector has been particularly targeted, accounting for 21.82 percent of all cyberattacks against Indian entities, with nearly 60 percent of healthcare organisations facing at least one cyberattack last year.[9] Other critical sectors in India facing frequent cyber risks include banking and finance,[10] energy, defence[11] and manufacturing.[12] The financial sector has seen a significant increase in cyber incidents, with the national CERT team addressing around 1.6 million incidents in 2023, up sharply from 53,000 in 2017.[13] Similarly, the Indian manufacturing sector was the most targeted industry for ransomware extortion in 2023.[14] The energy and defence sectors remain vulnerable to risks arising from targeted ransomware attacks and supply chain vulnerabilities.[15]

Similarly in the US, sectors such as healthcare and energy, along with critical manufacturing, have been heavily impacted by cyberattacks.[16] Healthcare institutions are frequent targets due to the vast amounts of personally identifiable information they handle.[17] The energy sector,[18] water systems,[19] and transportation systems[20] have also seen an increase in attacks, which disrupted daily operations and posed severe national security risks.

Responsible Actors, Their Objectives

In both nations, nation-state and non-state adversaries exploit critical infrastructure vulnerabilities to disrupt or destroy essential services.[21] In the US, a clear theme has emerged: nation-state actors target critical

infrastructure to achieve strategic objectives, often unrelated to cyberespionage. These campaigns aim to disrupt operational technology in critical sectors, affecting public services and processes.[22] A notable example is the 2021 Colonial Pipeline attack by the Russian cybercrime group DarkSide, which caused widespread fuel shortages, price hikes, and panic-buying across the East Coast.[23]

India, too, has seen a 278 percent rise in state-sponsored cyberattacks between 2021 and 2023.[24] However, unlike the US, where government agencies commonly attribute such attacks to nation-states, Indian statistics often do not clarify whether these originate from state actors, non-state actors, or individuals, domestic or foreign.[25] This lack of attribution may stem from limited technological capacity, complicating efforts to trace and address these threats.[26] That said, independent researchers have linked attacks on Indian critical infrastructure—spanning defence, aerospace, energy, education, and healthcare—to state-sponsored actors from various nations. Both India and the US are also experiencing an increasing overlap between cybercrime and cyberespionage. Cyberespionage refers to unauthorised access to computer systems and networks to gather sensitive or classified information, typically for political, military, or strategic purposes.[27] Cybercrimes, on the other hand, involve illegal activities carried out using computers or networks, primarily for financial gain or personal benefit. Examples include India's AIIMS ransomware attack[28] and the US Colonial Pipeline attack, where economic motivations intersected with broader strategic aims.[29]

II. Ransomware

Ransomware is a type of malicious software that encrypts data on a victim's system, rendering it inaccessible until a ransom is paid, typically in cryptocurrency to the attackers.[30] Since this form of cybercrime has emerged as a threat globally, India and the US have witnessed a significant rise in ransomware incidents.[31] Below are common emerging trends we have identified based on our analysis of recent ransomware attacks in the US and India.

Growing Frequency, Sectors Impacted

According to the US Cybersecurity and Infrastructure Security Agency (CISA), ransomware attacks in the US increased by 22 percent in April 2023, with an associated increase of 74 percent in the cost associated with such incidents relative to the previous year.[32] Similarly, India is now one of the top targets for ransomware attacks in the Asia Pacific and Japan region, ranking second in terms of successful attacks.[33] Indian experts' analysis predicts that ransomware will be one of the top threats facing Indian cyberspace in 2025 and will continue to evolve to target supply chains and critical infrastructure.[34] Growing ransomware threats can be attributed to factors including limited visibility into operational technology systems, inadequate network monitoring, suboptimal cyber-hygiene implementation, exploitation of known vulnerabilities, and the use of stolen credentials to gain unauthorised access to systems.[35] Sectors primarily impacted in India include manufacturing (29 percent), healthcare (8.89 percent), financial services (8.89 percent), technology, and pharmaceuticals.[36] The US, on the other hand, faces emerging risks from cybercriminal syndicates, exploiting ransomware to disrupt critical services, including healthcare, energy, and education, resulting in significant financial losses and public safety risks.[37]

Growing Sophistication

Ransomware groups are continuously refining their methods to monetise access and bypass defensive measures intended to thwart their operations. A growing trend among attackers is the use of "double" and "triple extortion" tactics. These strategies involve not only encrypting victims' data but also threatening to

sell or publicly expose the data if the ransom is unpaid. In some cases, attackers even escalate demands by threatening to dox victims unless an additional fee is provided. Victims who comply with these demands depend on the attackers' assurances to delete exfiltrated data and refrain from further exploitation. However, these assurances are often broken. Notable examples of double and triple extortion ransomware include the REvil group's attacks against US companies[38] and Rafel RAT, used to target Indian Android users.[39] Ransomware actors also frequently collaborate, dividing responsibilities such as malware development, attack execution, and cryptocurrency ransom collection.[40]

Integration of Emerging Technology with Ransomware

Another increasingly prevalent trend is the demand for cryptocurrency as ransom in ransomware attacks targeting systems in both India and the United States. Globally, over USD 450 million (INR 37.5 crore) was paid in cryptocurrency to ransomware groups in only the first half of 2023. This way, attackers leverage unregulated crypto exchanges to launder funds without being traced. Notable Indian examples include the ransomware attack against AIIMS, where the attackers allegedly demanded USD 24.5 million (INR 2 crore) equivalent in cryptocurrency. In the US, the 2022 ransomware attack against US hospitals and healthcare providers by a state-backed entity was leveraged with demands for ransom in cryptocurrency (see **table 1**).

III. Supply-Chain Vulnerabilities

Supply chain exploitation involves cyberattacks that target vulnerabilities in an organisation's suppliers, vendors, or service providers to gain indirect access to their systems or data. Such attacks capitalise on the interconnectedness of modern digital ecosystems and growing reliance on common third-party suppliers, which allows them to access victims at scale.[41] In both India and the United States, supply chain exploitation has emerged as a growing cybersecurity threat, driven by increased digitisation and reliance on third-party providers.

Based on our analysis of recent cybersecurity events in the US and India (see **table 1**), some key common trends emerge – exploitation of unpatched vulnerabilities, inserting malicious code into trusted software updates, and compromising cloud service providers. Unpathed vulnerabilities in software dependencies allow malicious actors to exploit gaps in third-party software components used by organisations to compromise whole systems through a single weak link. In the US, the 2021 Kaseya VSA Ransomware Attack exploited a vulnerability in the remote IT monitoring software, allowing hackers to deliver ransomware to both Kaseya's customers and the clients (see **table 1**). In India, the BSNL data breach highlighted supply chain vulnerabilities in state-owned enterprises.[42]

Inserting malicious code into trusted software updates is another tactic increasingly used by cybercriminals. During the 2020 SolarWinds attack which impacted US federal agencies and private companies, malicious actors inserted a backdoor into a software update for SolarWinds' Orion platform. The recent CrowdStrike outage – which might be the largest IT outage in history – was caused by a malformed update that was sent to a piece of security software called CrowdStrike Falcon and led to millions of Windows users encountering the dreaded blue screen of death.

Attacks seeking to compromise cloud service providers target vulnerabilities in cloud service infrastructure to access or disrupt the data and systems of organisations relying on the provider's services, often affecting multiple clients simultaneously. The 2022 breach of the Indian government's S3Waas platform is popularly attributed to cloud vulnerabilities (see **table 1**).[43]

IV. Commercial Spyware

The proliferation of commercial spyware exacerbates these cyberthreats in both nations, facilitating intrusive surveillance and endangering human rights and national security. The 2024 Report on the Cybersecurity Posture of the United States highlights persistent threats from state-sponsored actors targeting critical infrastructure for espionage and crisis disruption. This is exemplified by an incident that impacted both India and the US, when a state-sponsored surveillance firm known as the NSO group developed and sold a sophisticated spyware tool that could remotely infiltrate smartphones and other devices without users' consent (see **table 1**). In 2023, state-sponsored attacks on Apple devices belonging to various Indian politicians, journalists, and policymakers.[44]

V. Malicious Usage of Emerging Technology

Emerging technologies are increasingly being leveraged to carry out cybercrimes in both India and the US, exposing critical vulnerabilities in their digital ecosystems. In the US, AI-enabled ransomware attacks have caused significant economic damage, with losses projected to reach USD 20.9 billion (INR 156,750 crore) between 2018 and 2023.[45] Similarly, India faces growing threats from AI-driven phishing campaigns and sophisticated social engineering tactics.[46] As discussed in section II, the integration of cryptocurrency with ransomware raises serious concerns about traceability in both nations. Experts warn that by 2025, AI-powered malware and generative AI will dominate the cyber threat landscape in India, enabling highly adaptive attacks, targeted scams, and impersonations that blur the line between real and artificial interactions.[47]

VI. Overview of Key Cybersecurity Incidents in India and the United States

The following table discusses the specific incidents in India and the US, based on which the above analysis is based.

Table 1: Recent Cybersecurity Incidents in the US and India

Nature of Cybersecurity Event/Attack	Cybersecurity Event/Attack	Description	Effected Country
Attack on Critical Infrastructure	**Hafnium Attack, 2021**[48]	Attributed to a state-sponsored hacker group, the attack targeted Microsoft Exchange Server, exploiting zero-day vulnerabilities in the system that allowed attackers to access email accounts, deploy web shells, and exfiltrate sensitive data from hundreds of thousands of organisations globally. The attack primarily affected US government agencies and defence contractors.	**US**
Critical Infrastructure	**The Colonial Pipeline attack, 2021**[49]	A significant ransomware attack by the state-backed cybercrime group DarkSide targeted one of the largest fuel pipeline operators in the US, causing widespread disruption to fuel supplies on the East Coast.	**US**

Critical Infrastructure	**Typhoon Cyberattacks on US, 2019 – 2024**[50]	Two major hacking operations attributed to state-backed hacker groups targeting US infrastructure and telecommunications systems. In a series of attacks against US infrastructure—including ports, power grids, water utilities—and telecommunications systems, including phone networks and surveillance systems, airports and military supply lines, state-backed hacker groups have targeted critical national assets.	**US**
Critical Infrastructure	**State-sponsored hackers breached the CFIUS, 2025**[51]	Breach of the US Treasury Department's unclassified systems, specifically targeting the Committee on Foreign Investment in the US (CFIUS), which reviews foreign investments for national security risks, particularly in sensitive areas like real estate near military bases.	**US**
Critical Infrastructure	**State-sponsored Spear-Phishing attacks, 2024**[52]	Infiltration of the 2024 US presidential campaign networks primarily targeting the Trump campaign's staff through stolen passwords. The goal appears to have been election interference, with the intent to undermine US political figures and disrupt the democratic process. Leaked documents detailing internal communications within the Trump campaign intended to sway public opinion, particularly against Trump.	**US**
Critical Infrastructure	**State-backed Hackers Targeting the US Water Sector, 2023-2024**[53]	Israeli-made devices commonly used in critical infrastructure sectors, including water and wastewater systems, energy, manufacturing, transportation, and healthcare, were targeted and compromised. Multiple US states and foreign countries were affected.	**US**
Critical Infrastructure	**Microsoft Exchange Intrusion, 2023**[54]	State-sponsored cyberattack exploiting vulnerabilities in Microsoft's cloud-based email services, targeting government agencies, critical industries, and private organisations. The cybercriminal group gained unauthorised access to email accounts by bypassing Microsoft's authentication systems. Microsoft's investigation revealed a flaw in the cloud service provider's identity infrastructure.	**US**
Critical Infrastructure	**AIIMS ransomware attack, 2022**[55]	Attack on the servers of All India Institute of Medical Sciences (AIIMS) India's premier government-run medical research centre and hospital. Servers went down after a malware attack that rendered patient data, registration systems and even the internet inaccessible, and exposed sensitive personal data including medical history, AADHAR and PAN details, among other things. It also disrupted medical services to patients for six days. Experts asserted that a foreign adversary state actor may be responsible.	**India**

Critical Infrastructure	**State-backed hackers step up attacks against Indian govt systems, 2024**[56]	Cyberespionage campaign targeting India's government, defence, and aerospace sectors. Use of spear-phishing emails impersonating Indian defence officials to deliver malware to infiltrate systems and steal sensitive information. Major state-owned companies, including Hindustan Aeronautics Limited (HAL), Bharat Electronics Limited (BEL), and Bharat Earth Movers Limited (BEML), were specifically targeted.	**India**
Critical Infrastructure	**State-backed Cyberespionage, 2023-2024**[57]	Impersonation of recruiters on LinkedIn to lure professionals in the aerospace, defence, and aviation industries with fake job offers to enable unauthorised access and data theft.	**India**
Critical Infrastructure	**Operation FlightNight, 2024**[58]	Cyberespionage campaign targeting Indian government entities and the energy sector. Attackers disseminated a malicious file masquerading as a letter from the Indian Air Force, aiming to compromise offices responsible for electronic communications, IT governance, and national defence.	**India**
Critical Infrastructure	**Data leak exposing espionage, 2024**[59]	Data about cybersecurity firm I-Soon was leaked online, exposing the company's involvement in state-sponsored cyberespionage activities targeting the governments of the United Kingdom, India, Indonesia, Taiwan, and Nigeria.	**Multiple Countries**
Critical Infrastructure	**G-20 website organised cyberattack, 2023**[60]	During India's presidency, the official G20 website experienced a Distributed Denial-of-Service (DDoS) attack, with up to 1.6 million attacks per minute. The Indian Cyber Crime Prevention Centre (I4C) reported that the attack was organised and aimed to disrupt the website's functionality.	**India**
Critical Infrastructure	**State-backed targeting of India's education, 2023**[61]	Adverse state-backed hacker collective intensified its cyber activities against Indian institutions, notably the Indian Army and the education sector. This escalation is part of a series of targeted attacks over the past year, aiming to infiltrate and compromise sensitive information within these sectors.	**India**
Ransomware	**Ransomware Attacks on Healthcare Entities, 2022—2024**[62]	Ransomware attacks against healthcare providers such as Ascension, Change Healthcare and various others have:Led to the theft of data, potentially including protected health information, insurance, and payment records.Caused significant disruptions to the health system's IT infrastructure, including electronic health record systems, and to the overall operations of various pharmacies, hospitals and other health systems.	**US**

Ransomware	**City of Oakland Ransomware attack, 2023**[63]	A ransomware attack forced the declaration of a state of emergency and impacted many non-emergency city services, including permitting, payment collections, and more. Many of the records leaked contained confidential information about the police department.	**US**
Ransomware	**The City of Chicago's Department of Aviation Ransomware attack, 2022**[64]	City of Chicago's Department of Aviation (CDA) was targeted by a ransomware group, Conti. This led to a significant disruption in the city's airport operations, including systems handling flight information and internal communication, and severely impacted the airport's ability to manage services efficiently.	**US**
Ransomware	**City of Riviera Beach, Florida Ransomware attack, 2019**[65]	The incident was caused by an employee in the police department opening an infected email, which took the City of Riviera's main computer system offline, affecting every department. City council members approved the payment of a USD 600,000 (INR 7.5 crore) ransom, payable in Bitcoin.	**US**
Ransomware	**Atlanta Ransomware attack, 2018**[66]	A cyberattack against the City of Atlanta crippled government services, impacting critical police services and the city's court system, including the loss of police dashcam recordings related to active prosecutions. The attackers demanded a ransom of USD 51,000 (INR 42 lakh) to release the government's data, payable in Bitcoin.	**US**
Ransomware	**JBS Foods Ransomware Attack, 2021**[67]	JBS Foods, one of the world's largest meat processing companies, was targeted by the REvil ransomware group, which disrupted its operations across North America and Australia. The attack forced JBS to temporarily shut down several meat processing plants, leading to significant disruptions in the global meat supply chain.	**US**
Ransomware	**Kaseya VSA Ransomware Attack, 2021**[68]	REvil ransomware group exploited a vulnerability in software used to remotely manage IT systems for their clients. The vulnerability allowed hackers to deliver ransomware to both Kaseya's customers and the clients they served. Approximately 1,500 businesses, ranging from small to large enterprises, were affected globally.	**US**
Ransomware	**Mobile subscribers' data leak, 2024**[69]	CloudSEK detected a massive data breach involving the personal information of 750 million Indian telecom users. The compromised data included names, mobile numbers, addresses, and Aadhaar information. It was being sold on the dark web by threat actors. The actor demanded USD 3,000 (INR 2,46,000) for access to the full dataset.	**India**

Ransomware	**Domino's data breach, 2021**[70]	Domino's India experienced a significant data breach compromising sensitive customer information of approximately 180 million food orders, including email addresses, phone numbers, order specifics, and credit card information. The hacker offered the stolen data for sale on the dark web, highlighting the significant value of such information.	**India**
Ransomware	**Ransomware attacks against Polycab, Motilal Oswal, Bira91, 2024**	In March 2024, several prominent Indian companies, including Polycab, Motilal Oswal, and Bira 91, fell victim to ransomware attacks.	**India**
Ransomware	**National Payments Corporation of India (NPCI) ransomware attack, 2024**[71]	Ransomware Attack on C-Edge Technologies Ltd, a Technology Service Provider Catering Primarily to Cooperative and Regional Rural Banks. It led to the temporary shutdown of payment systems across nearly 300 small Indian banks, affecting approximately 0.5 percent of the country's payment system volumes.	**India**
Ransomware	**Star Health attack**[72]	Star Health and Allied Insurance Company, India's largest health insurer, experienced a ransomware attack which led to leakage of sensitive customer information, including medical records and personal identification details on Telegram. Star Health said it received a ransom demand of USD 68,000 (INR 51 lakh) from a cyberhacker in connection with a leak of customer data and medical records.	**India**
Supply Chain	**SolarWinds Cyberattack, 2019-2021**[73]	State-sponsored actors compromised the software supply chain of SolarWinds, a major IT management company by inserting a backdoor into a software update for SolarWinds' Orion platform. The backdoor was then distributed to thousands of organisations, including US government agencies, Fortune 500 companies, and critical infrastructure entities. The attackers used this access for espionage, stealing sensitive data and potentially compromising national security.	**US**
Supply Chain	**Log4shell, 2021**[74]	A critical vulnerability in a popular open-source Java-based logging library allowed remote code execution by exploiting how Log4j handled certain log messages. It gave attackers the ability to execute arbitrary code on affected servers, potentially leading to full system compromise. It is considered one of the most severe vulnerabilities ever discovered due to its widespread use across many applications and services globally.	**US**

Supply Chain	**MOVEit data breach, 2023**[75]	A cyberattack on the MOVEit Transfer software, a popular file transfer solution used by businesses and organisations globally. The breach allowed the attackers to access and exfiltrate sensitive data from multiple organisations using MOVEit for secure file transfers, affecting various industries, including healthcare, finance, and government, exposing personal, financial, and confidential data.	**US**
Supply Chain	**ICICI Bank breach, 2024**[76]	A data breach occurred in ICICI Bank's mobile banking app, iMobile Pay, leading to the exposure of sensitive credit card information of approximately 17,000 users. The breach was due to a technical glitch that erroneously mapped the data of new credit cards in the bank's digital channels, allowing users to view full card details.	**India**
Supply Chain	**Indian Government S3WaaS data breach**[77]	The 'Secure, Scalable and Sugamya Website as a Service' (S3WaaS) platform of the Government of India, developed for hosting government websites, faced a significant vulnerability. The flaw potentially led to the exposure of sensitive personal data of around 250,000 Indian citizens, primarily COVID-19 vaccine beneficiaries. Despite alerts and correspondence with CERT-In and NIC, the vulnerability persisted until March 2024.	**India**
Supply Chain	**BSNL Data Breach, 2024**[78]	A significant data breach of Bharat Sanchar Nigam Limited (BSNL), India's state-owned telecommunications provider. The hacker claimed to have stolen sensitive data, including IMSI numbers, SIM card details, and home location register information.	**India**
Supply Chain	**Defence personnel SPARSH data breach, 2024**[79]	The SPARSH portal, a digital platform managing pension services for India's defence personnel, experienced a significant data breach which exposed sensitive information of over 3 million pensioners from organisations such as the Border Roads Organisation and Military Intelligence. Data included usernames, passwords, pension numbers and other personal details.	**India**
Supply Chain	**WazirX Security Breach, 2024**[80]	India's largest cryptocurrency exchange, WazirX, faced a major breach resulting in the theft of USD 230 million (INR 1,886 crore) in cryptocurrency. Hackers, linked to the state-sponsored Lazarus Group, exploited a multisignature wallet by creating a fake account, depositing tokens, and purchasing cryptocurrencies to drain the funds.	**India**

Commercial Spyware	**Commercial Spyware Incident**[81]	State-sponsored surveillance firm NSO Group had developed and sold a sophisticated spyware tool that could remotely infiltrate smartphones and other devices to extract data, record calls, track locations and activate cameras or microphones without the user's knowledge. Breach incidents were reported in both the US and India.	**Multiple Countries**
Emerging Tech	**State-backed disinformation attacks**	State-backed operatives orchestrated a large-scale disinformation campaign aimed at influencing both domestic and international audiences, with a focus on sowing division within the US and other countries. Using AI, the operatives created fake social media accounts that posed as US residents, spreading propaganda.	**US**

Source: Authors' compilation

Chapter III:
Shared Priorities and Challenges: US-India Cybersecurity Collaboration

Introduction

Building upon the preceding Chapters that discuss the growing imperative of cybersecurity and the evolving threat landscape in relation to ICT technologies, this Chapter delves into the specific priorities and challenges faced by the US and India in this domain. The US, a leader in technological innovation and cybersecurity governance, and India, a rapidly digitising economy with growing cyber capabilities, represent two critical actors in the global cybersecurity ecosystem. Their alignment is not just a bilateral priority but also a necessity for shaping global norms and standards in this space. To this end, the Chapter aims to:

- Examine the approaches adopted by the US and India in securing their digital ecosystems.
- Identify commonalities in their priorities and challenges.
- Explore opportunities for collaboration to enhance global cyber resilience.

I. The US Approach to Cybersecurity

A Broad Overview of United States' Vision for Cybersecurity

The United States recognises cybersecurity as a critical national priority. The increasing connectivity and reliance on digital technologies along with rapid integration of artificial intelligence (AI, Internet of Things (IoT) devices,) has ushered a range of opportunities for economic growth and development and enhanced access to education, health, finance and social services. At the same time, these digital systems, layered with advanced functionalities, have also expanded the attack surface for malicious actors, creating risks having implications for both economic prosperity and national security (as outlined under chapter II).

The National Security Strategy (NSS) 2022[82] sets the overall direction and tone for all subordinate strategies including national defence, economic, diplomatic, or cybersecurity. It envisions a defensible, resilient, and values-driven digital ecosystem that aligns with free, multistakeholder model as an alternative state-controlled paradigm as seen in Russian and Chinese practices. This vision is further embodied in the National Defence Strategy 2022 (NDS),[83] National Cybersecurity Strategy (NCS)[84] and the Executive Order (EO) 14028 on Improving the Nation's Cybersecurity.[85] These strategies collectively emphasise the vulnerabilities of societies and critical infrastructure to cyberattacks, integrate cyber capabilities into national defence through the concept of integrated deterrence, and outline a detailed framework for securing the digital domain with a focus on resilience, accountability and international collaboration.[86]

B. The National Cybersecurity Strategy 2023

The National Cybersecurity Strategy 2023 is the key policy document in this context. It complements these efforts by offering a detailed, action-oriented framework for securing the digital domain, focusing on resilience, accountability, and international collaboration. The NSC 2023 marks a significant departure from its predecessors, which focused heavily on deterrence as a key objective and building resilience against cyberthreats.[87] The strategy makes two fundamental shifts. It rebalanced the responsibility to defend cyberspace by noting that "end users bear too great a burden for mitigating cyber risks" and asserting that "the most capable and best-positioned actors in cyberspace must be better stewards of the digital ecosystem." It further emphasises the need to shift defensive responsibilities toward both public and private sector leaders. Moreover, the strategy stresses that "our economy and society must incentivise decision-making to make cyberspace more resilient and defensible over the long term," outlining how the Federal Government will "reshape incentives and achieve unity of effort" by leveraging mechanisms such as enhanced accountability measures, federal grants, and procurement strategies to promote long-term cybersecurity investments.[88] The strategy is built around five pillars namely:

a, Defend Critical Infrastructure: The first pillar of the NCS relates to protecting critical infrastructure. The Cybersecurity and Infrastructure Protection Agency (CISA) defines critical infrastructure as assets, systems, and networks—whether physical or virtual—that are fundamental to the functioning of a society and economy and whose disruptions would have a debilitating effect on national security, public safety, and economic stability. It lists 16 sectors as critical infrastructure, reflecting their vital role in the nation's operations.[89] The strategy outlines the need for mandatory cybersecurity requirements to address gaps in protections, citing past incidents like the 2021 Colonial Pipeline ransomware attack. Given that around 85 percent of this infrastructure is privately owned, the strategy encourages innovation and collaboration between private operators and federal agencies, ensuring preparedness against malicious cyber activities.[90] The strategy lists several strategic objectives under the pillar. These are:

- *Establish Cybersecurity Requirements for National Security and Public Safety*: Recognising the limitations of voluntary cybersecurity, the strategy calls for performance-based, harmonised, and nimble frameworks tailored to each sector's risks. It assigns federal agencies with the task of setting up and enforcing cybersecurity requirements for government systems, while simultaneously developing voluntary standards and framework (such as Cyber Performance Goal) for the private sector, including critical infrastructure. Efforts will be undertaken to ensure affordability to accommodate entities with limited resources and streamline overlapping regulations to reduce industry burden.
- *Scale Public-Private Collaboration*: The strategy emphasises enhancing collaboration between the public and private sectors to share insights and respond to threats efficiently through technology-enabled connectivity.
- *Update Federal Incident Response Plans and Processes*: Acknowledging that the private sector plays the role of first line of defence in handling most cyber incidents, the strategy underscores the need to build a solid partnership with federal agencies that can provide support when necessary. To this end, the strategy highlights the need to update the National Cyber Incident Response Plan (NCIRP)[91] and implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)[92] to standardise incident reporting and enable rapid responses.
- *Modernise Federal Defences:* The strategy emphasises the implementation of Executive Order 14028, National Security Memorandum-8 on Improving the Cybersecurity of National Security, Department of Defence and Intelligence Community Systems (NSM-8),[93] and zero trust principles to modernise federal systems and bolster security.

b. Disrupt and Dismantle Threat Actors: This pillar emphasises taking a proactive approach to addressing malicious state and non-state actors. It entails leveraging all instruments of national power,

including diplomatic, military, financial, law enforcement and cyber capabilities. The pillar also prioritises collaboration with private sector and international partners to ensure a coordinated response to cyber threats.

- *Integrate Federal Disruption Activities*: This objective focuses on making cybercrime financially and operationally unviable through sustained and targeted federal campaigns. It includes taking pre-emptive actions that include initiatives like "defending forward," wherein attacks are disrupted before they cause harm.
- *Enhance Public-Private Operational Collaboration to Disrupt Adversaries*: Given the private sector's visibility into adversarial activities, this objective highlights the importance of public-private collaboration.
- *Increase the Speed and Scale of Intelligence Sharing and Victim Notification*: This objective seeks to improve the timely sharing of threat intelligence between federal and non-federal partners, thus benefiting from both national and private-sector insights.
- *Prevent Abuse of US-Based Infrastructure***:** Malicious actors often exploit US-based cloud infrastructure, domain registrars, and digital services to launch cyberattacks. This objective aims to collaborate with service providers to detect and disrupt such abuse while balancing privacy concerns by making it difficult to exploit infrastructure-as-a-service (IaaS) platforms for malicious purposes.
- *Counter Cybercrime and Defeat Ransomware*: This objective is targeted to disrupt ransomware operations by enhancing law enforcement actions, strengthening critical infrastructure resilience, fostering international cooperation, and addressing the use of virtual currencies for ransom payments.

c. Shape Market Forces to Drive Security and Resilience: This pillar recognises that market forces have been insufficient in driving the adoption of secure technologies and prioritises the need to shift responsibility from the end users to those best positioned to reduce risks, such as technology developers and service providers.

- *Hold the Stewards of Data Accountable:* The strategy advocates for legislative efforts to establish clear limits on data collection and usage while providing robust consumer protections aligned with National Institute of Standards and Technology (NIST) guidelines.
- *Driving the Development of IoT Devices security:* The objective supports efforts such as the IoT Cybersecurity Improvement Act and security labelling aims to improve device security.
- *Shift Liability for Insecure Software Products and Services:* The objective advocates for legislative measures to hold software vendors accountable for vulnerabilities and the adoption of best practices, such as NIST's Secure Software Development Framework (SSDF), that currently apply to software deployed on Federal networks.[94]
- *Use Federal Grants and Incentives to Build Security:* The objective calls for federal grant programs like the Bipartisan Infrastructure Law [95] and CHIPS and Science Act [96] to be used to prioritise investments in securing critical infrastructure.
- *Leverage Federal Procurement to Improve Accountability:* It supports using federal procurement processes to drive broader progress in cybersecurity, leveraging programmes that require vendors to adhere to secure practices, such as self-attesting to compliance, undergoing third-party assessments, and providing artifacts like Software Bill of Material (SBOMs) and the Secure Software Development Framework to deliver evidence-based indications of cybersecurity for Federal cybersecurity that may be adopted as well by critical infrastructure owners and operators.[97]

c. Invest in a Resilient Future: The pillar underscores the importance of strategic investments in innovation, research and education to build a secure and resilient digital ecosystem. It highlights the need to leverage public investments through the National Science Foundation (NSF) and initiatives such as the CHIPS and Science Act, to strengthen national cybersecurity.[98]

- *Secure the Technical Foundation of the Internet*: This objective focuses on creating more secure technical standards and collaborating with non-governmental organisations, academia and industry to build a stronger, more resilient digital foundation.

- *Reinvigorate Federal Research and Development for Cybersecurity*: The objective advocates utilising federal R&D initiatives like the Federal Cybersecurity Research and Development Strategic Plan to address risks in areas such as computing technologies (quantum, AI etc.), biotechnology and clean energy.
- *Prepare for the Post-Quantum Era*: Acknowledging quantum computing's potential to undermine current encryption methods, this objective calls for investments to replace vulnerable technologies and implement cryptographic standards under frameworks like NSM-10.[99]
- *Strengthen the Cyber Workforce*: The objective highlights the need for education and training pathways, inclusivity, and workforce development through programs like NICE and CyberCorps.[100]

d. Forge International Partnerships to Pursue Shared Goals: The pillar highlights the importance of international collaboration to address the borderless nature of cyberspace and cybercrime.

- *Build Coalitions to Counter Threats*: The objective favours leveraging existing strategic alliances like the Declaration for the Future of the Internet (DFI), Quadrilateral Security Dialogue (QUAD), Indo-Pacific Economic Framework for Prosperity (IPEF), and US-EU Trade and Technology Council to create a shared vision of an open, secure digital future and counter threats from malicious actors operating globally.
- *Strengthen International Partner Capacity*: The objective supports cyber capacity-building with allies. This includes military-to-military partnerships.
- *Expand Assistance to Allies*: It supports provisioning assistance to allies like Costa Rica and Albania in investigating, responding to, and recovering from cyberattacks.
- *Reinforce Global Norms of Responsible State Behaviour*: Under this objective the U.S. seeks to uphold UN-agreed norms for cyberspace, holding irresponsible states accountable through diplomacy, sanctions, and other measures.
- *Secure Global Supply Chains*: Recognising the critical role of technology supply chains, the US emphasises domestic production or close coordination with allies to ensure secure, reliable systems while reducing dependence on adversarial nations.

II. The Indian Approach to Cybersecurity

A. Broad Overview of India’s Vision for Cybersecurity

India is quickly emerging as a key player in the digital landscape. Over the last few years, the country's digital ecosystem has grown tremendously, fuelled by transformative government initiatives and relentless focus on advancing disruptive technologies like AI, machine learning (ML), and quantum computing to foster economic growth. Several key initiatives underline this transformation. For instance, the India Semiconductor Mission aims to strengthen domestic manufacturing capabilities in the semiconductor sector, reducing dependency on imports and building a robust supply chain.[101] Similarly, the India AI Mission seeks to build a comprehensive AI ecosystem by removing bottlenecks in computing access, availability of quality data sets, developing indigenous capabilities through public-private partnerships, and ensuring safe and ethical AI development and deployment.[102] Moreover, the government’s emphasis on cloud services, spearheaded by the MeghRaj initiative, ensures scalability and security for e-governance projects, enhancing efficiency and citizen access. Additionally, India’s Digital Public Infrastructure (DPI) has also been a game-changer. Platforms such as Aadhaar, Unified Payments Interface (UPI), and DigiLocker have redefined public service delivery.[103] The government acknowledges these challenges, recognises cybersecurity as a critical national priority, and implements wide-ranging measures to safeguard its expanding digital ecosystem.[104]

B. India's National Cyber Security Policy

In India, the National Cyber Security Policy 2013[105] outlines an overarching framework to protect India's information infrastructure, mitigate vulnerabilities, and respond effectively to cyber threats. The key objectives include protection of critical information infrastructure (CII) and promoting the development of indigenous cybersecurity technologies. It also focuses on creating a skilled workforce, fostering public-private partnerships, strengthening the regulatory framework, and promoting global cooperation. Its focus areas include:

- **Protection of Critical Information Infrastructure:** The policy mandated the establishment of a National Critical Information Infrastructure centre to monitor and protect CII on a 24/7 basis.[106] The government executed the direction under section 70 A of the Information Technology Act, 2000 (IT Act, 2000).[107] In addition, it also mandated the implementation of global security best practices, business continuity management, and cyber crisis management plans for all critical sectors. It also required security audits and ensuring the use of validated and certified IT products in CII operations.
- **Strengthening Regulatory and Institutional Frameworks:** The policy advocated the development of a dynamic legal framework to address emerging cybersecurity challenges posed by technologies like cloud computing, mobile computing, and encrypted services. To this end, it emphasised periodic reviews and audits of security infrastructure to ensure adherence to regulatory requirements. It also mandated the establishment of national and sectoral CERTs (Computer Emergency Response Teams) to handle cyber incidents and coordinate responses effectively. This requirement was fulfilled by the government under section 70B of the IT Act.[108] CERT-In was made operational in 2004. Additionally, the strategy prioritised enhancing the law enforcement capabilities to enable effective prevention, investigation, and prosecution of cybercrimes through appropriate legislative interventions.
- **Development of Indigenous Cybersecurity Technologies:** The policy promoted collaboration between academia, industry, and the government to foster innovation in cybersecurity technologies. It aimed to develop cost-effective, indigenous solutions tailored for India's cybersecurity needs.
- ***Capacity Building and Training of Cybersecurity Professionals:*** The policy set a benchmark for creating a skilled workforce of 500,000 cybersecurity professionals through capacity-building programs, skill development initiatives, and public-private partnerships. This also included the establishment of cybersecurity concept labs and institutional mechanisms to train law enforcement agencies (LEAs) in tackling cybercrime effectively.
- ***Fostering Public-Private Partnerships (PPP):*** The policy favoured active collaboration between government and private entities to address cyber threats and vulnerabilities.
- ***Promoting Global Cooperation:*** The strategy supported building bilateral and multilateral relationships to enhance collaboration on cybersecurity at the global level. It also involved strengthening cooperation between security agencies, CERTs, and international judicial systems for coordinated responses to cyber incidents.

C. Need for National Cybersecurity Strategy

The National Cybersecurity Policy 2013 was the first formal policy document aimed at strengthening the cybersecurity posture of India. It is complemented with a comprehensive legal[109] and institutional framework[110] spanning multiple central and sectoral laws, and is supported by a dense inter-ministerial and interdepartmental ecosystem addressing various facets of cybersecurity. Despite this, the current cybersecurity framework is fraught with numerous challenges.

While India's cybersecurity policy of 2013 laid a strong foundation, current cybersecurity initiatives are fragmented across various agencies and regulatory frameworks, leading to limited coordination and

inconsistent implementation. For instance, the protection of CII is overseen by the National Critical Information Infrastructure Protection Centre (NCIIPC), which lacks of unified mechanisms for identifying, prioritising, and safeguarding critical and protected sectors. The gap hinders timely threat detection, effective information-sharing, and robust response strategies, leaving sectors such as power, telecom, banking, and transport vulnerable to sophisticated cyberattacks. There is a need for the establishment of sector-specific Information Sharing and Analysis Centres (ISACs) to aid and enhance threat detection, prevention, and response capabilities.[111]

In relation to supply chain security, particularly in strategic areas such as IT hardware and semiconductors, India currently employs import controls and monitoring mechanisms to ensure supply chain resilience and address national security concerns. The absence of mutually recognised standards and certifications results in fragmentation in the market and undermines the potential for integrated, secure supply chain relationships. India's existing threat intelligence network also faces challenges. Despite the pivotal role of agencies like CERT-In, there is a general lack of a centralised, whole-of-economy threat intelligence system that effectively integrates government and private sector insights. There is also shortage of skilled cybersecurity professionals, which has had a negative impact on India's ability to proactively mitigate emerging cyber threats.[112] The rapid adoption of emerging technologies such as AI, IoT, and quantum computing has significantly expanded the cyber threat landscape. However, India's existing policies do not fully addressed the vulnerabilities arising from these technologies. There is also lack of robust mechanisms to ensure safe integration of these technologies into critical systems.[113]

Given these limitations, there have been calls for India to develop a unified and comprehensive National Cybersecurity Strategy. Such a strategy would streamline the fragmented efforts across government agencies, establish clear accountability mechanisms, and ensure that cybersecurity initiatives are well-coordinated, long-term, and aligned with international best practices.

III. Charting out Common Priorities and Challenges for the US-India Cybersecurity Collaboration

Based on our analysis of the material in previous chapters and the challenges and opportunities each nation faces in securing its digital ecosystem, we have identified key areas of convergence and divergence that must be addressed to strengthen cybersecurity partnerships.

A. Protection of Critical Infrastructure/ Critical Information Infrastructure

Convergences	Divergences
Both countries acknowledge the significance of CI/CII protection and have established dedicated agencies and frameworks to address the issue. The efforts are led by CISA, along with sector-specific authorities in the US. In India, NCIIPC and sectoral regulators lead the way. Both countries are investing in cybersecurity measures, including vulnerability assessments, threat intelligence sharing, and incident response capabilities.	The US CI/CII protection framework encompasses a wider range of sectors, including 16 critical infrastructure sectors, while India primarily focuses on sectors like power, banking, telecom, transport, government, and strategic public enterprises. The US has a more mature and developed CI/CII protection ecosystem, with a longer history of addressing these challenges. India's framework is still evolving, with a greater focus on capacity building and developing its cybersecurity capabilities.

	The US adopts a more prescriptive regulatory approach to CI/CII protection, with mandatory cybersecurity standards for certain sectors. India's approach is more collaborative and voluntary, relying on partnerships and incentives to encourage private sector participation in security efforts.

B. Focus on Supply Chain Security

Convergences	Divergences
Both the US and India consider securing supply chains against cyber threats a top priority. The US has implemented comprehensive measures such as Executive Order 14028 on improving cybersecurity, Executive Order 14017 (America's Supply Chains), as well as guidelines and best practices (NIST Cyber Supply Chain Risk Management or C-SCRM) for managing cybersecurity risks related to supply chains. Similarly, India has developed frameworks like the IT Act (2000), the National Cybersecurity Policy (2013), and CERT-In guidelines. Both nations engage in international cooperation to address global supply chain risks by participating in forums like Quad, IPEF, and the Global Forum on Cyber Expertise (GFCE). Both countries also participate in ISO working groups to develop global standards for supply chain security, such as ISO/IEC 27036 (guidelines for cybersecurity in supplier relationships).	The US has a mature and comprehensive cybersecurity ecosystem, supported by well-established frameworks, executive orders, and regulatory mandates. Key initiatives like Executive Order 14028 (Improving the Nation's Cybersecurity) and Executive Order 14017 (America's Supply Chains) emphasize securing supply chains and critical infrastructure. Regulatory frameworks such as the Federal Acquisition Regulation (FAR) and the Defence Federal Acquisition Regulation Supplement (DFARS) mandate stringent cybersecurity measures for federal contractors, ensuring the protection of sensitive information and supply chain integrity. Additionally, the NIST Cybersecurity Framework (CSF) and NIST Special Publication 800-161 (Cyber Supply Chain Risk Management or C-SCRM) provide detailed guidelines for managing cybersecurity risks, including those in supply chains. These frameworks are widely adopted and enforced, reflecting the US's advanced approach to cybersecurity. In contrast, India's cybersecurity frameworks are in a developmental stages. While initiatives like the National Cybersecurity Policy (2013) and CERT-In guidelines provide a foundation for addressing cyber risks, including supply chain vulnerabilities, enforcement and implementation remain inconsistent. India places significant emphasis on reducing dependence on foreign suppliers through initiatives like Make in India and Atmanirbhar Bharat. This is driven by concerns over geopolitical risks and the need for self-reliance. While the US also emphasizes supply chain resilience, its focus is more on diversifying sources and ensuring transparency (e.g., through SBOMs) rather than complete indigenisation.

	The US has a strong focus on securing software supply chains, with initiatives like SBOMs and secure software development practices mandated by EO 14028. While India is increasingly aware of software supply chain risks and has taken recent steps in this direction through CERT-In's SBOM guidelines, its focus has traditionally been more on hardware and critical infrastructure.

C. Strengthening Law Enforcement Capabilities (Improving /Enhancing Threat Intelligence)

Convergences	Divergences
Both India and the US recognise the importance of engaging with private sector entities to enhance cybersecurity measures. For example, the US National Cybersecurity Strategy emphasises scaling public-private collaboration to enhance threat response capabilities. Similarly, India's strategy includes fostering public-private partnerships (PPP) to address cybersecurity vulnerabilities and threats effectively. Both countries invest heavily in capacity-building initiatives to strengthen their cybersecurity posture. The US and India run various training programs and initiatives aimed at upskilling law enforcement and other relevant government personnel in cybersecurity practices. For instance, India's Cyber Surakshit Bharat initiative and the US CyberCorps program aim to build the necessary skills among government officials to handle and respond to cybersecurity incidents.	The US cybersecurity strategy is deeply integrated with its national defence and security apparatus, for protecting government (primarily Federal networks), often linking cybersecurity initiatives directly with national security measures. This integration is evident in the alignment of cybersecurity strategies with national defence strategies. In contrast, India's approach is more decentralised, with multiple ministries and agencies involved, reflecting a broader focus that includes economic development and technology innovation alongside security.

D. Capacity Building

Convergences	Divergences
Both countries acknowledge the critical importance of strengthening their cybersecurity frameworks through capacity building. The US: Initiatives like the CyberCorps: Scholarship for Service programme and the National Initiative for Cybersecurity Education (NICE) focus on cultivating a skilled cybersecurity workforce	The US's approach is highly structured with a clear pathways for integrating cybersecurity into higher education curricula and continuous professional development, facilitated by programmes such as those offered by the National Security Agency (NSA) and Department of Homeland Security (DHS) designated National Centers of Academic Excellence in Cybersecurity.

through scholarships, education, and career development. Similarly, India has launched initiatives like Cyber Surakshit Bharat, which focuses on training government officials, and the Information Security Education and Awareness (ISEA) project that aims to generate qualified cybersecurity professionals. Both the US and India exhibit an inclination towards carrying out capacity building programmes with public–private partnerships. Examples include the US partnering with academic institutions and private organisations under NICE. The Indian Cyber Security Policy advocates for collaboration between the public sector, which is demonstrated by initiatives such as partnerships with NASSCOM for skill development.	While India is rapidly increasing its educational programmes, its approach is more varied and less standardised across the nation. The focus is more on immediate skill development and short-term training programmes to quickly scale up the workforce to meet immediate needs. Indian initiatives tend to focus more broadly on increasing digital access and security for its large population, with a significant emphasis on protecting consumer data and enhancing government service delivery through secure digital platforms.

E. Securing Emerging Technologies and Combatting Cyberthreats

Convergences	Divergences
Both the US and India recognise the importance of technologies like AI, IoT and quantum computing presenting opportunities and challenges for cybersecurity. Both countries emphasise the importance of public-private partnerships in developing and deploying secure emerging technologies and combating cyberthreats.	In October 2023, the US released Executive Order (EO) 14110 on the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence, which directed whole-of-government efforts to shape the values-aligned development of AI. However, this EO has been revoked by the present administration, as part of a broader consideration of regulatory approaches. The new administration's approach to AI emphasises the development of systems that are free from ideological bias or engineered social agendas. The objective is to reinforce the US's role as a global leader in AI technology, striving for a future that benefits all Americans. This shift involves reassessing previous AI policies and directives that may have been seen as limiting American innovation in AI and affecting the country's leadership in the global arena. India, is relatively at more formative stages in this regard. India AI mission is a comprehensive national-level initiative that aims to strengthen the country's AI innovation ecosystem. One of its key components is the Safe & Trusted AI pillar, which focuses on enabling the implementation of responsible AI projects, including the development of indigenous tools and frameworks, self-assessment checklists for innovators, and other guidelines and governance frameworks.

F. International Cooperation and Resilience Building

Convergences	Divergences
Both the US and India actively participate in various regional and multilateral forums engaging on issues pertaining to cybersecurity. This includes UN processes: UNGGE and UNOEWG, Quadrilateral Security Dialogue (Quad), G20, Indo-Pacific Economic Framework for Prosperity (IPEF), among others. Both countries support a rules-based order in cyberspace, advocating for responsible state behaviour and adherence to international law.	The US actively pushes for global norms and rules for cyberspace in UN forums. It also takes more of a leadership role in forming coalitions such as the Counter-Ransomware Initiative to promote its vision of cybersecurity globally. India takes an ideologically agnostic stance on cyber norms. Instead, it focuses more on capacity-building, supply chain security, and actionable models like the proposed Global Cybersecurity Cooperation Portal. India also shows preference towards bilateral and regional arrangements (e.g., with the Quad or Israel) to address immediate cybersecurity threats.

Chapter IV:
Mapping US-India Cybersecurity Collaborations Across Bilateral, Regional, and Multilateral Forums

Introduction

The evolving threat landscape in cyberspace has driven both the United States and India to recognise the critical importance of cybersecurity and adopt robust measures to protect cyber infrastructure, reduce vulnerabilities, and build capabilities to prevent and respond to cyber threats. As outlined in the preceding Chapters, both nations are facing a wide variety and constantly evolving cyber threats, prompting them to bolster their domestic cybersecurity postures. This has led to the emergence of several common priority areas, such as: protection of critical infrastructure/critical information infrastructure, securing supply chains, fostering public-private collaboration and threat intelligence sharing, securing emerging technologies while combating evolving cyber threats, and international cooperation to build resilience.

Since the mid-2000s, India and the US have built a strong and multifaceted partnership across trade, security, and technology sectors. Bilateral trade has grown steadily, with the US emerging as India's largest trade partner in 2022.[114] Defence ties have also deepened, with India designated a "Major Defence Partner" in 2016 and subsequently into Tier 1 of the US Department of Commerce's Strategic Trade Authorization license exception.[115] The two nations have signed foundational defence agreements, facilitated regular bilateral dialogues, conducted joint military exercises, and expanded defence procurements, enabling closer collaboration on security, intelligence sharing, and counterterrorism. India's technology partnership with the US has strengthened significantly over the past decade, marked by initiatives such as the India-US Science and Technology Forum, the Defence Technology and Trade Initiative (DTTI), and the more recent United States–India Initiative on Critical and Emerging Technologies (iCET) and Memorandum of Cooperation (MOU) on Cybercrime Investigations.[116] Cybersecurity remains a core area of discussion across these domains, reflecting its growing importance in trade, defence, and technological collaboration.

This Chapter delves into the collaborative efforts between the US and India across bilateral, regional, and multilateral forums to address the shared cybersecurity priorities. It examines how these common themes are being prioritised and translated into concrete actions through various initiatives, dialogues, and partnerships.

I. US-India Bilateral Cybersecurity Cooperation

The US–India cybersecurity relationship has undergone a profound transformation over the past two decades, evolving from a nascent dialogue to a robust, multi-layered strategic partnership. This evolution is marked by shifting priorities due to emerging threats, deepening trust, and an increasingly sophisticated understanding of the shared challenges in cyberspace. The evolution of the US–India partnership can be understood through three distinct phases: an early phase of foundational dialogue, a second phase focused on operationalising cooperation, and a current phase characterised by strategic alignment on emerging technologies and future threats.

A. Early Discussions: Laying the groundwork

The earliest bilateral engagement on cybersecurity-related issues can be traced back to this phase that marks the establishment of the US-India Cybersecurity Forum in April 2001. The initiative laid the foundation for bilateral cooperation on cybersecurity, focusing on areas such as critical infrastructure protection, legal cooperation, law enforcement, information security standards, and research and development. It also marked the beginning of structured dialogue and collaboration between the two nations to enhance cybersecurity measures in both the civil and defence sectors.[117] Other important bilateral initiatives included the Joint Working Group on Information and Communications Technology (ICT),[118] which established the institutional platform to bring forth and discuss ICT-related issues and developments. The nuances of these early interactions reveal a focus on building a shared vocabulary and understanding of cybersecurity concerns, legal frameworks, and technical capabilities. A key trend was to build legal cooperation for any future joint initiatives.

B. Deepening Trust and Operationalisation (2010-2016):

This phase represents a period of deepening trust and operationalisation in the U.S.-India cybersecurity relationship. Building upon earlier dialogues, this period saw a shift from abstract discussions to concrete actions and the establishment of formal mechanisms for cooperation. The U.S.-India Strategic Dialogue and Homeland Security Dialogue elevated cybersecurity to a core element of bilateral ties, fostering high-level discussions and joint efforts on threat intelligence sharing and incident response, including cooperation at the level of National Security Councils. A Memorandum of Understanding (MOU) was signed between CERT-IN and US-CERT, which enabled real-time information sharing, joint incident response, and the exchange of best practices between the two nations' cybersecurity response teams. A significant milestone was the signing of the Framework for the U.S.–India Cyber Relationship in 2016, which was a comprehensive agreement that advanced a shared vision for an “open, interoperable, and reliable cyberspace environment” and underscored the importance of innovation, free flow of information, and public-private cooperation. The framework outlined specific threats of mutual concern and recognised the leading role of governments in cybersecurity matters related to national security while also stressing the need for capacity building and R&D cooperation. Furthermore, it emphasised bilateral and international cooperation to combat cyber threats, real-time information sharing, developing joint mechanisms for threat mitigation, continued law enforcement cooperation, and joint skill development programs.

C. Strategic Convergence and Emerging Technologies (2016-Present):

The post-2016 era of the US–India cybersecurity relationship represents a distinct shift from standalone agreements to a more integrated approach, embedding cybersecurity within broader agreements that focus on emerging technologies and supply chain resilience. This evolution reflects a mature understanding of cybersecurity as an intrinsic element of national security and economic development in the interconnected digital age. This phase is marked by initiatives such as the US–India Semiconductor Supply Chain and Innovation Partnership and iCET, which underscore a proactive, future-oriented collaboration, emphasising joint R&D, innovation, and capacity building in critical areas like AI, quantum computing, 5G/6G, and semiconductor technology.

Table 4: Strategic Convergence and Emerging Technologies

Mechanism/ Initiative	Year Established/ Launched	Key Focus Area	Objectives/ Key Outcome / Achievements
US-India Cybersecurity Forum[119]	**2001**	• Critical infrastructure protection • Cybersecurity both in the civil and defence fields • Legal cooperation and law enforcement; and • Information security standards and Research and Development	• This initiative laid the foundation for US-India bilateral cooperation on cybersecurity. • Establishment of five working groups focusing on key areas of cybersecurity: ◦ Legal Cooperation and Law enforcement ◦ Research and Development ◦ Critical Information Infrastructure ◦ Defence Cooperation ◦ Standards and Software Assurance • Enhanced bilateral cooperation through joint initiatives, expert exchanges, training, and public-private partnerships.
Joint Working Group on Information and Communications Technology (ICT)[120]	**2005**	• Discussion on ICT and digital economy issues. • Enhancing cybersecurity as part of the digital economy.	• This initiative is part of US-India Economic Dialogue • Promotes development and deployment of secure and reliable ICT ecosystem. • The Joint Working Group serves as a platform for advancing initiatives from other groups such as the QUAD Principles on Critical and Emerging Technology Standards and bilateral iCET. • Recent discussion in May 2023 emphasised: ◦ On the importance of secure and reliable ICT supply chains. ◦ Promotion of open, interoperable, and secure fifth and sixth generation (5G/6G) wireless technologies, networks, and services; ◦ Opportunities for Indian and US information technology, telecommunications, and electronics manufacturing companies in both countries; ◦ Data protection and privacy; the free flow of data; and ◦ Role of Digital Public Infrastructure (DPIs) in expanding access to public services and enabling economic growth.

US India Strategic Dialogue[121]	**2010**	• Expanded counterterrorism cooperation including cybersecurity. • Bilateral cooperation on cyber issues through National Security Councils.	• Enhanced bilateral cooperation on cybersecurity through shared information on cyberattacks, joint response to cybersecurity incidents, cooperation on cybersecurity technology, and the exchange of cybersecurity policy and best practices. • Signed MOU between Computer Emergency Response Teams (CERT-IN and US-CERT). The MOU between the CERTs of both countries focuses on mutual support in the event of cyber incidents, sharing best practices and expertise in cybersecurity, which includes policy exchanges and technology cooperation.
Homeland Security Dialogue (HSD)[122]	**2010**	• Critical Infrastructure Protection • Cybercrime and Illegal Cyber Activities • Capacity Building in Cybersecurity	• Deepen bilateral cooperation in fighting cyberthreats and ensuring cyber safety. • **E**xchange of information on cyberthreats and responses to strengthen cybersecurity measures. • The signed Memorandum of Cooperation focused on law enforcement training, which includes aspects of cybersecurity training between the US Federal Law Enforcement Training Centre and India's Sardar Vallabhbhai Patel National Police Academy.
US-India Cybersecurity Agreement (MOU)[123]	**2011**	• Closer cooperation and timely exchange of information between the cybersecurity organisations of both governments. • Sharing of best practices for exchanging critical cybersecurity information and expertise. • Enhanced coordination on technical and operational cyber issues.	• Facilitates direct communication between the US Computer Emergency Readiness Team (US-CERT) and Indian Computer Emergency Response Team (CERT-In) to enhance the cybersecurity posture of both nations. • Enable both governments and their cybersecurity communities to collaborate on addressing cyber threats, sharing crucial cybersecurity information, and coordinating responses to cyber incidents. • Supports the broader goals of the US-India Strategic Dialogue on advancing global security and countering terrorism by strengthening cybersecurity cooperation.
Framework for the US–India Cyber Relationship[124]	**2016**	Development of joint mechanisms for cybersecurity, and enhancing the security of ICT infrastructure.	• Established designated points of contact for specific areas of cooperation to facilitate timely and effective communication and coordination.

		• Cybersecurity-related research and development. • Joint training and skill development programmes. • Enhancing cooperation on cybercrime through legal frameworks and law enforcement. • Supporting international law in cyberspace and promoting norms of responsible state behavior during peacetime.	• Strengthen cooperation between the Computer Emergency Response Teams (CERTs) of both countries. • Improve cybercrime cooperation through established mechanisms and treaties, notably the Treaty on Mutual Legal Assistance in Criminal Matters, to enhance the effectiveness of combating cybercrime. • Undertake Joint efforts in promoting the integrity of the supply chain and enhancing the security of ICT products and services. • Ongoing dialogue and engagement in international forums on cyber issues, supporting a multistakeholder model of internet governance. • Establish of a high-level cyber dialogue mechanism to oversee and review the implementation of the framework.
US-India Semiconductor Supply Chain and Innovation Partnership (MOU) under US-India Commercial Dialogue[125]	**2023**	• Establishing a collaborative mechanism to enhance the resilience and diversification of semiconductor supply chains, in alignment with the US's CHIPS and Science Act and India's Semiconductor Mission.	• Utilise the complementary capabilities of both countries to foster commercial opportunities and develop semiconductor innovation ecosystems. • Facilitate discussions on various aspects of the semiconductor value chain to promote joint innovation and development. • Encourage mutually beneficial R&D initiatives aimed at advancing semiconductor technologies. • Promote the development of necessary skills and talents required to support the semiconductor industry.
United States and India Elevate Strategic Partnership with the Initiative on Critical and Emerging Technology (iCET)[126]	**2023 (announced in 2022)**	• Strengthening of Innovation Ecosystem • Defence Innovation and Technology Cooperation • Resilient Semiconductor Supply chain • Cooperation on next generation telecommunications	• Collaborate on artificial intelligence, quantum technologies, advanced wireless, and high-performance computing (HPC). • Focus on joint development and production in defence technologies, including jet engines and munitions. • Develop robust semiconductor design and manufacturing ecosystem in India. • Strengthen collaboration in human spaceflight and commercial space engagements. • Enhance 5G and 6G research and development, and promoting Open Radio Access Network or Open RAN deployments in India.

US-India MOU on Cybercrime Investigations	**2025**	• Cybercrime Investigation • Cyber Threat Intelligence • Digital Forensics • Training and Capacity Building	• Bolster India-US security cooperation as part of their comprehensive and global strategic partnership • Effectively address common security challenges linked to cybercrime, such as terrorism, drug trafficking, human trafficking, and financial crimes. • Improve the investigative capabilities of both Indian and US agencies.

Source: Authors' compilation

II Cybersecurity Cooperation in Regional and Multilateral Contexts

A. Quadrilateral Security Dialogue (Quad)

The Quadrilateral Security Dialogue (Quad) is a diplomatic partnership between Australia, Japan, India and the US.[127]It is dedicated to delivering tangible outcomes for the Indo-Pacific region on issues pertaining to health security, climate action, infrastructure development, critical and emerging technologies, cybersecurity, humanitarian assistance and disaster relief, space, maritime security, countering disinformation and counter-terrorism. The Quad was formally established in 2007. However, it was paused in 2008 due to differing views on its significance and concerns about potential repercussions on economic ties with China. The Quad was revitalised in 2017 by the US and Japan. Since its revival, the Quad has expanded its agenda to include areas such as global health, infrastructure development, climate change mitigation, people-to-people exchanges, critical and emerging technologies, cybersecurity and space exploration.[128]

Quad cybersecurity initiatives include the formation of the Quad Senior Cyber Group (QSCG) consisting of leader-level experts in cybersecurity who would work towards adopting and implementing shared standards in the cybersecurity field, developing secure software, building workforce and talent in cybersecurity and promoting the growth and safety of digital infrastructure.[129] **Since its inception the QSCG has taken several initiatives towards enhancing cybersecurity education and awareness.** Since its inception, the QSCG has taken several initiatives towards enhancing cybersecurity education and awareness. Other notable cybersecurity initiatives under Quad include Joint Principles for Secure Software to reduce the number and potential impact of software vulnerabilities and develop a system to exchange information on cyberattacks or critical infrastructure damage among the cyber sections of the Quad governments.[130]

B. Group of 20

The Group of 20, or G20, is an intergovernmental forum comprising 19 member countries, the European Union (EU), and the African Union (AU).[131] The G20 annual summit is a prominent platform for global leaders to deliberate on economic challenges and other critical international issues. Additionally, bilateral discussions among the leaders at the side lines of the G20 have at times resulted in significant international accords. Cybersecurity issues are not traditionally addressed under the G20. However, India took the initiative to prioritise cybersecurity during its 2023 G20 presidency.[132] These discussions explored the need for international cooperation in combating cybercrime, particularly in the context of emerging technologies, but yielded no immediate tangible outcomes. However, it has laid the groundwork for future collaboration within the G20 framework.

C. Indo-Pacific Economic Framework (IPEF)

The Indo-Pacific Economic Framework (IPEF) is an economic initiative launched by the US in 2022 to build resilience, sustainability, inclusiveness, economic growth, fairness, and competitiveness to benefit 14 IPEF economies. It consists of 14 member countries and includes Australia, Brunei Darussalam, Fiji, India, Indonesia, Japan, Malaysia, New Zealand, the Philippines, the Republic of Korea, Singapore, Thailand, the United States, and Vietnam. The initiative is built around four pillars: trade, supply chain, clean economy and fair economy.[133] India is currently participating in the IPEF's supply chain, clean economy, and fair economy pillars, while holding observer status in the trade pillar.[134] The cybersecurity-related issues are most evidently being addressed under the supply chain pillar. Six of the IPEF members concluded and entered the IPEF Supply Chain Agreement in November 2023. The agreement aims to develop a shared understanding of regional supply chain, sharing of information and best practices on opportunities and challenges, mobilising investments to strengthen investments, creating response mechanisms as well as promoting supply chain resilience in critical sectors. In December 2024, both the US and India assumed the position of chair and vice-chair of the Supply Chain Council under the said Agreement.[135]

D. UN Processes

The discussions on ICT security at the UN can be traced back to April 1, 1998, starting with a resolution introduced by Russia and adopted as UNGA 53/70.[136] This resolution initiated critical discussions on international security and the rule of law in the context of cyberspace. It also led to the formation of the UN Group of Governmental Experts (GGE). The group consisted of governmental experts from different regions, tasked with analysing the impact of ICTs on international security. The GGE convened six times from 2004 to 2021 and resulted in substantive reports with conclusions and recommendations. Notable progress has was made through the outcome reports generated in 2010, and 2013 which laid the groundwork for defining responsible state behaviour in cyberspace under international law, established voluntary non-binding norms, and encouraged confidence and capacity-building measures. The 2021 final report of the Open-Ended Working Group (OEWG) reaffirmed the applicability of international law to cyberspace, including the principles of the UN Charter. It emphasised voluntary non-binding norms, confidence and capacity-building measures, and the importance of cooperation among states to ensure peace and stability in the use of ICTs. Parallel to this, in December 2018, the UN General Assembly through resolution 75/240 established a five-year Open Ended Working Group on security of and in the use of information and communications technology. Unlike the GGE, the OEWG was open to all 193 UN Member Countries. The OEWG submitted its final report in 2021 reaffirming the application of international law to state behaviour in cyberspace.[137] It also endorsed non-binding norms for responsible conduct, and stressed the need for capacity-building. Mandated by UNGA resolution (75/240)[138] dated December 31, 2020, the OEWG is currently progressing on deliberations on the States' use of ICTs in the context of international peace and security. The scope of the OEWG until 2025 is to further develop international norms and rules for responsible state behaviour in cyberspace, establish regular dialogues under the UN for continuous engagement on cybersecurity issues, and enhance global cooperation on capacity-building and confidence-building measures to ensure a secure, stable, and peaceful ICT environment.

The US has been an active participant in the UN's cybersecurity initiatives, emphasising the application of international law to cyberspace and promoting responsible state behaviour through the OEWG and GGE processes. The US advocates for a consensus-based approach that includes capacity building and confidence-building measures to manage cyber threats.[139] India's participation is characterised by a preference for pragmatic engagement over ideological alignment. India has been proactive in advocating for global cooperation on cybersecurity capacity building, particularly for developing countries. This is exemplified by its support for the creation of a Global Cybersecurity Cooperation Portal, aimed at facilitating knowledge exchange and supporting the cybersecurity needs of the Global South.

global cooperation on cybersecurity capacity building, particularly for developing countries. This is exemplified by its support for the creation of a Global Cybersecurity Cooperation Portal, aimed at facilitating knowledge exchange and supporting the cybersecurity needs of the Global South.[140]

E. UN Cybercrime Treaty

In December 2024, the United Nations General Assembly (UNGA) adopted the United Nations Convention against Cybercrime.[141]The convention is the culmination of five years of efforts undertaken by UN member states led by an open-ended ad hoc committee established under the UN General Assembly Resolution 74/247,[142] following a proposal by the Russian Federation and 17 co-sponsors in 2019. The convention will be opened for signature in 2025. It seeks to boost international cooperation among law enforcement agencies, offer technical assistance to countries lacking adequate infrastructure, and criminalise a range of cybercrimes, including illegal interception, money laundering, hacking, and online child sexual abuse material (CSAM). The treaty requires member states to enact legislation criminalising activities like unauthorised access and data manipulation and prohibits the production and distribution of devices designed for cybercrime. Both India and the US played an active role in negotiating the Convention.[143]

F. International Counter Ransomware Initiative

The International Counter Ransomware Initiative (CRI) is a US-led effort following the ransomware attack on the Colonial Pipeline to combat the growing threat of ransomware.[144]It aims to foster cooperation between nations to build cross-border resilience and collectively disrupt and defend against malicious cyberactors.[145] Since its inception, CRI has expanded to become the world's largest international cyber partnership.[146] It comprises 68 member states and organisations and is structured into three pillars: the International Counter Ransomware Taskforce (ICRTF), the Policy Pillar, and the Diplomacy and Capacity Building (DCB) Pillar. The International Counter Ransomware Taskforce (ICRTF) is currently led by Australia and Lithuania, who spearhead projects aimed at delivering practical tools to counter malicious cyber tools and disrupt ransomware. Their notable contribution includes onboarding members for sharing platforms allowing members to share threat information and indicators of compromise. CRI's Policy Pillar is led by Singapore and the United Kingdom (UK) undertake policy research and provide recommendations on ransomware-related issues. Its notable work includes outcomes relating to secure software and labelling, methods to counter the use of virtual assets as part of the ransomware business model, policies to reduce ransom payments, increase and improve reporting, cyber insurance, and a playbook to guide businesses on how to prepare for, deal with, and recover from a ransomware attack. The Capacity Building Pillar is led by Germany and Nigeria, who focus on fostering collaboration, forging new partnerships, and recruiting new members into the initiative. The pillar also maps out the capacity building needs of the partner countries.[147] The recent convening of CRI was held in Washington D.C. in October 2024. During this meeting, members discussed a range of issues, including the use of AI to counter ransomware attacks, the development of secure software, and the importance of public-private partnerships. The CRI also released a joint statement at the end of the meeting, reaffirming its commitment to working together to combat ransomware and hold perpetrators accountable.[148]

III. Overview of Priority Areas and Corresponding Initiatives in the US-India Cybersecurity Collaboration

Based on our comprehensive survey of US and India collaborations across bilateral, regional, and multilateral forums, we have concluded that both nations actively engage in the priority areas delineated by their respective domestic policies and frameworks. The following table highlights various priority areas identified from prior discussions and outlines the initiatives undertaken within each area. This exercise is instrumental in mapping the breadth and depth of engagement, serving as a solid foundation for evaluating potential future collaborations in the field of cybersecurity.

Table 5: Priority areas and initiatives

Critical Infrastructure/Critical Information Infrastructure	Supply Chain Security	Strengthening Law Enforcement Capabilities (Improving Enhancing Threat Intelligence)	Capacity Building	Securing Emerging Technologies while Combating Evolving Cyber threats	International Cooperation to Build Resilience
• High-level discussions and dialogue on critical infrastructure or critical information infrastructure protection. • Sector-specific initiatives focusing on critical infrastructure sectors like energy and telecommunications. • Information sharing on cyberthreats and vulnerabilities targeting critical infrastructure.	• Prioritisation towards Strategically diversifying the semiconductor supply chain to reduce dependence on single sources and fostering collaboration between trusted partners. • Joint research and development, technology transfer, and co-production in critical and emerging technologies.	• Measures pertaining to real-time information sharing, joint incident response, and the exchange of best practices. • Establishing CERT-to-CERT coordination to enable exchange of information regarding threats, vulnerabilities, and incidents.	• Joint training, and skill development programmes for law enforcement agencies and other relevant personnel. • Technical assistance to partner countries to enhance their capacity to combat ransomware and other cyberthreats.	• Joint research and development, promoting secure design principles, and ensuring the integrity of the supply chain for these technologies. • Collaboration in respect of research and development on issues relating to AI, quantum technologies, and advanced wireless communication.	• Development of norms, principles, and frameworks to bolster international cybersecurity cooperation. • Enhanced law enforcement collaboration to strengthen mutual cybersecurity postures. • Provision of technical assistance to partner countries, aiming to fortify their capabilities against ransomware and other cyber threats.

• Collaboration on policies, procedures, and technical aspects of securing ICT infrastructure, which is crucial for protecting CII that relies heavily on ICT. • Capacity-building initiatives to strengthen cybersecurity capabilities related to CII protection, such as training programs and technical assistance.	• Focus on developing secure software through joint principles and information sharing to ensure that software used in critical infrastructure and supply chains is free from vulnerabilities. • sharing information, best practices, and coordinating responses to disruptions.	• Legal and law enforcement cooperation. This includes, cross-training between agencies, cyber drill exercises, to combat cybercrime and enhance mutual cybersecurity postures.		• Bilateral frameworks to foster reciprocal investments in AI and related technologies. • Initiatives focused on securing emerging technologies and mitigating evolving cyber threats, and promoting secure design principles.	

Source: Authors' compilation

Chapter V:
Pathways to Resilience: Recommendations and Roadmap

Introduction

Despite its robust participation in bilateral, regional, and multilateral cybersecurity dialogues, India's approach to cybersecurity remains relatively nascent, highlighting a significant gap in its strategic policy framework. The absence of a comprehensive National Cybersecurity Strategy has positioned India as a late mover in an arena where pre-emptive and dynamic policies are crucial. This lag not only impacts India's ability to leverage international collaborations effectively but also limits its responsiveness to emerging cyber threats. However, this "late mover" status can be strategically advantageous if India takes proactive steps to identify and leverage lessons learned from the US and other allies who have refined their national cyber strategies over multiple iterations.

Recognising these challenges, it is imperative for India to craft a forward-looking cybersecurity strategy that not only catches up with global standards but also sets a proactive stance on cybersecurity governance. In this section, we will delve into the core pillars of a potential Indian Cybersecurity Strategy, offering strategic insights and recommendations that align with both national needs and international best practices. By redefining its approach, India can transform its cybersecurity landscape to secure its digital infrastructure and enhance its geopolitical stature in cyberspace.

I. Pillar I: Protection of Critical Infrastructure

The protection of critical information infrastructure is already an important aspect of India's cybersecurity framework, evident in initiatives like the National Cybersecurity Strategy, which recognises the protection of critical information infrastructures as one of its key objectives. In 2014, the government also established the NCIIPC to oversee cybersecurity in critical sectors. These mechanisms form a strong foundation to build on, and it is imperative for India to take a whole-of-nation approach to cybersecurity of its critical infrastructure. This would involve the establishment of sector-specific Information Sharing and Analysis Centres for critical sectors. Further, in order to build robust deterrence capabilities, the government must take steps to strengthen critical infrastructure defences to make successful attacks prohibitively costly and resource-intensive. Deterrence measures also seek to ensure continued functioning of critical infrastructures during cyberattacks.

A. Recommendation 1: Sectoral Approach to Critical Infrastructure Protection

The critical sectors which fall under the aegis of the NCIIPC are power and energy, banking, financial services and insurance, telecom, transport, government, strategic and public enterprises. India's cybersecurity posture in relation to critical infrastructure should prioritise the establishment of sector-specific Information Sharing and Analysis Centres (ISACs) for each of these designated sectors to aid and enhance threat detection, prevention and response capabilities. These ISACs, modelled on successful frameworks in

the EU and the US, would be central resources that collect, analyse and disseminate actionable threat information and device tools to mitigate risks and enhance resilience. They would serve as information sharing platforms between private stakeholders on critical infrastructure security by essentially facilitating cooperation between owners and operators of critical infrastructure.

ISACs are generally non-profit, industry-driven organisations with governmental oversight for their administration.[149] Industry participation enables information sharing between public and private stakeholders, whereas governmental involvement ensures increased formality and transparency. For instance, European regulations such as the NIS Directive and the Cybersecurity Act have facilitated the creation of 18 sectoral ISACs,[150] while the US has established 28 ISACs across critical sectors for sectoral resilience.[151]

In India, self-governed, private sector-run ISACs for designated critical sectors could be formed under the oversight of the NCIIPC. It could also establish a governing council to streamline information exchange across ISACs and enhance intersectoral collaboration. Additionally, India should expand its cybersecurity capabilities by creating national-level CERTs (Computer Emergency Response Teams) for all critical sectors, building on the existing CERT-Power. These CERTs should collaborate closely with key players such as national regulators, industry associations, and law enforcement agencies. Participation of sectoral regulators would ensure that sector-specific concerns are prioritised appropriately. For example, healthcare requires dedicated cybersecurity oversight given the increasing targeting of the sector, with the National eHealth Authority (NeHA) playing a pivotal regulatory role. Drawing inspiration from best practices in the US and EU, India can proactively address emerging threats and ensure the resilience of its critical infrastructure in an increasingly hostile cyber environment.

B. Recommendation 2: Building Robust Deterrence Capabilities

This pillar also focuses on making cyberattacks prohibitively difficult and resource-intensive, thus discouraging adversaries from targeting critical infrastructure. This approach involves fortifying defences through advanced measures, such as multilayered s security protocols, robust network segmentation, and employing zero-trust architectures. By reducing the likelihood of successful intrusions, deterrence by denial increases the cost of attacks, effectively dissuading threat actors. Enhanced cybersecurity measures further contribute to this strategy by creating a protective barrier that intercepts most attacks before they can cause harm. Key practices include implementing stringent authentication systems, encrypting sensitive data and communication channels, conducting regular malware assessments, and ensuring timely updates or patches for vulnerabilities. These measures collectively create resilient critical infrastructure, capable of neutralising threats and maintaining operational integrity.

Active defence strategies also play a pivotal role in identifying and responding to cyberattacks, especially in light of India's limited capacity to attribute malicious activity to specific actors. By leveraging tools like network monitoring, traffic analysis, hostile packet blocking, etc., organisations can detect and mitigate threats in real-time. These measures not only safeguard systems but also aid in attributing attacks to perpetrators, supporting legal action and deterrence. In tandem, ensuring the operational continuity of critical infrastructure during an attack is vital. Infrastructure redundancy, such as backup systems and failover mechanisms, ensures functionality even during disruptions. This redundancy minimises cascading failures, enabling essential services to remain active and fostering public trust in the resilience of national critical infrastructure systems.

II. Pillar II: Supply Chain Security

As discussed in Chapter IV above, both the US and India have focused on strategic diversification of their semiconductor supply chain to reduce dependence on single sources and foster collaboration between trusted partners. In order to achieve the full potential of the robust foundation of their strategic partnerships, especially in the cyberspace, the countries must take steps towards ensuring safety and continuity in their supply chain relations.

A. Recommendation 1: Mutual Recognition Agreements (MRAs) to Facilitate Trusted Supply Chains

Non-tariff barriers such as import controls and monitoring systems have become a common way for governments to regulate the flow of goods into their countries. We see this happen most commonly in key industries such as coal, steel and paper in India. In 2023, the Government of India imposed import quotas on IT hardware products such as laptops, tablets, computers and servers. This was later changed to an import monitoring system, with the government acknowledging the need to monitor IT hardware imports to ensure India's trusted supply chains. However, unilateral measures like import quotas and monitoring systems risk straining relationships with trusted trade partners and may provoke retaliatory actions.

A promising alternative approach is through Mutual Recognition Agreements (MRAs), which classify imports from trusted traders as low security risks. By creating a more secure and predictable supply chain, MRAs enable companies to access markets of trusted trade partners more efficiently, offering competitive advantages such as expedited customs clearance. As discussed in Chapter 4, both the US and India emphasise strategic diversification of their supply chains to minimise dependence on single sources and foster collaboration with trusted partners, particularly in the semiconductor space. Leveraging MRAs for partnerships between the two nations can enhance economic resilience through trusted supply chains and result in mutual benefits in critical sectors. Cooperation on these lines would also be aligned with the two nations' IPEF commitments to develop a shared understanding of regional supply chains and promote supply chain resilience in critical sectors.

For instance, the Indian Telegraph (Amendment) Rules, 2017, provides that every telecom equipment must undergo mandatory testing and certification prior to sale, import or use in India. This is regulated through the Mandatory Testing and Certification of Telecom Equipment (MTCTE) Scheme to ensure compliance with safety and regulatory requirements. Under the MTCTE Scheme, the security requirements for software bill of materials (SBOM) differ from the globally recognised SPDX format, an open standard used internationally to assess security and licensing risks in software. Indian security requirements also mandate the disclosure of source code and other proprietary information, which is not required under the globally recognised Common Criteria for Information Technology Security Evaluation. These discrepancies create barriers for US-manufactured products in the Indian market and vice versa, fragmenting the telecom sector. US–India MRAs would allow the two nations to recognise and accept each other's conformity assessments, testing and certification processes for IT hardware. This would eliminate the need for duplicate testing or certification, reducing compliance costs and delays for manufacturers and foster trade by ensuring that hardware certified in one country can be sold in another without additional regulatory barriers, while maintaining shared standards for quality, safety and security.

B. Recommendation 2: Standardisation of Indian Sectors and Alignment with Global Standards

India's cybersecurity posture must prioritise standardisation of security requirements for ICT products sold, used and imported to India. In order to achieve the true potential of MRAs, which allow mutual recognition of testing requirements, standardisation of testing requirements within India beyond the telecom sector should be prioritised.

These standards would also have to be aligned with global standards, unless absolutely necessary due to national security concerns. A good example is India's telecom testing and certification regime, which has the potential to fragment the telecom market, as discussed above. Standardisation of the domestic market

III. Pillar III: Strengthening Law Enforcement Capabilities (Threat Intelligence)

To effectively strengthen India's cybersecurity framework, the strategy should prioritise the enhancement of threat intelligence capabilities across government and industry sectors. The government should utilise its specialised access to classified intelligence to inform and prepare the private sector for potential cyber threats, creating a proactive defence stance. In parallel, industries must be encouraged to share real-time threat data and vulnerabilities, which will enrich the government's response strategies and improve the nation's overall cyber resilience. This two-way exchange of information is critical for anticipating and mitigating sophisticated cyber threats. Additionally, India's cybersecurity strategy should advocate for the adoption of advanced technologies and methodologies that facilitate the scalable sharing of threat intelligence.

A. Recommendation 1: Establish a Whole-of-Economy Threat Intelligence Network

India's National Cybersecurity Strategy should explicitly prioritise the creation of a nationwide threat intelligence network that integrates government and private sector insights. This network would be centrally coordinated by the NCIIPC, which would play a pivotal role in developing and enforcing standardised protocols for secure and efficient sharing of threat intelligence across all relevant sectors. Integration with existing frameworks like the Cyber Crisis Management Plan and operations of CERT-In is crucial. This integration would streamline processes and reinforce the national cybersecurity posture by providing a unified approach to incident response and management. Additionally, the creation of state-level Incident Response Teams, under the authority of state governments, would enable localised rapid response capabilities. These teams would operate under clear protocols for incident escalation to the national level, ensuring a cohesive response strategy throughout the country.

The effectiveness of this network can be enhanced by leveraging technological advancements. The implementation of automated threat detection systems that utilise artificial intelligence and machine learning could significantly improve the speed and accuracy of threat identification and response. These technologies would facilitate real-time data exchange and analysis, making the threat intelligence network more dynamic and proactive.

Besides, fostering public-private partnerships is vital to enrich the threat intelligence network. Collaboration with the private sector, particularly in telecommunications and technology, would bring innovation and additional expertise. This would not only enhance the capabilities of the threat intelligence network but also

ensure that it stays ahead of emerging cyber threats by incorporating the latest technological advances and industry practices. Such partnerships are crucial for a resilient and responsive cybersecurity framework that protects national interests and critical infrastructures effectively.

B. Recommendation 2: Scale Advance Threat-Blocking Capabilities

India's National Cybersecurity Strategy should prioritise the development of advanced threat-blocking technologies that utilise AI and machine learning (ML) to pre-emptively identify and mitigate cyber threats. This commitment would involve collaborating with technology firms and academic institutions to push the boundaries of current technologies. Additionally, implementing incentive programs would encourage the private sector's involvement in both developing and deploying these systems, thereby accelerating innovation and application in real-world scenarios.

Telecommunications and internet service providers (ISPs) are crucial stakeholders in this strategy as they have adopted a variety of approaches to threat blocking. However, these entities often face challenges due to inadequate access to high-confidence threat information. By improving the sharing of actionable, timely, and contextualised threat intelligence between the government and industry, these providers can be better equipped to implement comprehensive measures to block malicious cyber activities.

As the capabilities for threat intelligence sharing are enhanced, the development of threat-blocking technologies that operate at machine speed can also be realised. These technologies would leverage machine learning algorithms to actively adapt to the evolving threat environment. To foster widespread adoption, the strategy should also promote and incentivise threat blocking across the economy, targeting those best positioned to implement these measures, such as telecommunication providers and ISPs.

C. Recommendation 3: Leverage International Threat Intelligence Sharing Initiatives

India's National Cybersecurity Strategy should prioritise leveraging international threat intelligence sharing initiatives by formalising partnerships and integrating these efforts into national frameworks. Signing Memoranda of Understanding (MOUs) with key platforms like Asia-Pacific Computer Emergency Response Team (APCERT) and the Cyber Threat Alliance ensures a structured engagement for rapid exchange of cyber threat data. This should be complemented by incorporating the intelligence into India's response mechanisms, enhancing the readiness and resilience of critical infrastructure. To manage this effectively, specialised liaison units could be established within existing cybersecurity agencies such as CERT-In, tasked with the coordination and operationalisation of these international collaborations. Additionally, enhancing the capabilities of national cybersecurity personnel through targeted training programs, developed in collaboration with international partners, will ensure that the workforce is equipped to analyse and act on the intelligence received effectively. These steps will solidify India's position in the global cybersecurity landscape and fortify its defences against emerging cyber threats.

Pillar IV: Capacity Building

India has consistently acknowledged the importance of capacity building in its approach to cybersecurity, as reflected in the National Cybersecurity Policy, various bilateral and regional agreements, and its participation in multilateral forums such as the UN Open-Ended Working Group (OEWG) and the UN Group of Governmental Experts (GGE). Recognising the evolving cyber landscape and the enhanced threats posed by emerging technologies that expand the threat surface, there is a critical need to continuously enhance its cybersecurity capabilities.

India's broader vision for capacity building in cybersecurity should encompass several key areas: firstly, skill building, where the focus is on developing a robust pipeline of cybersecurity professionals through structured education and training programs. This includes establishing career pathways, apprenticeships, and standardised pay frameworks to attract, train, and retain talent. Secondly, promoting a cyber awareness culture across government sectors and among the general populace is crucial. This effort aims to instil best practices and foster a proactive approach to cybersecurity readiness and response. Lastly, diversity and inclusion are pivotal, with initiatives aimed at encouraging participation from women, youth, and underrepresented groups in the cybersecurity domain, thereby enriching the field with diverse perspectives and enhancing the nation's defensive capabilities.

A. Recommendation 1: Enhancing Cyber Workforce Capabilities

To enhance India's cyber workforce capabilities, India's National Cybersecurity Strategy should prioritise the development of a skilled, professional, and diverse cybersecurity workforce. This involves expanding existing educational programmes such as the Information Security Education and Awareness (ISEA) initiative and integrating them with real-world application opportunities through partnerships with private sector entities. The strategy should establish clear professional standards and career pathways, facilitated by MeitY in collaboration with the Ministry of Education and the Ministry of Skill Development and Entrepreneurship. State governments can play a crucial role in promoting cybersecurity education and training programs at the state and local levels, leveraging their existing infrastructure and resources. Training programs should focus on key areas, including raising awareness about cybersecurity issues, emerging threats, and secure e-governance frameworks. Additionally, programs should delve into the cyber resilience ecosystem, exploring the role of Artificial Intelligence (AI) in cybersecurity, and educate participants on the significance of Cyber Suraksha Kendra for protecting state-level e-governance systems. Furthermore, in-depth training sessions should be offered on data protection, including the Data Protection Bill (DPDP Act 2023), application security, and endpoint security. Cyber Crisis Management Plans should also be a focus area, training attendees on developing CCMPs to ensure effective responses to cybersecurity incidents.

Support can also be drawn through public-private partnerships to keep the curricula up-to-date and relevant to current cyber threats, thus ensuring a continual pipeline of qualified cybersecurity professionals. It should be noted that India already has an enormous pool of educated professionals to tap into. Therefore, Cybersecurity capacity can also be built by reskilling these existing professionals in cybersecurity, a method adopted by countries such as the United States. Private-public partnerships should be established to drive these reskilling efforts as well, leveraging both resources and expertise from the private sector to enhance the training and professional development of cybersecurity personnel across the country.

B. Recommendation 2: Cybersecurity Awareness for All

Recognising that cybersecurity is not just a technical issue but a broader societal concern, it is crucial for the National Cybersecurity Strategy to promote cyber awareness across all layers of society. This should be addressed as a priority by launching nationwide campaigns that educate and inform all citizens about the best practices in digital hygiene. India has already taken some positive steps in this regard. For instance the National Council for Educational Research and Training (NCERT) has approved the syllabus developed by C-DAC for integration into the current ICT curriculum in schools.

In addition to these efforts, it would be beneficial to complement existing initiatives with programs similar to the UK's Cyber Aware Campaign, which effectively communicates basic but crucial cybersecurity tips, through targeted messages on social media, advertising, and collaborations with business promoters. It is

also recommended that CERT-In and NCIIPC allow for a broader dissemination of its Common Vulnerabilities and Exposures (CVE) reports.

To ensure inclusivity and reach a broader audience, programs should be developed in regional languages, catering to the diverse linguistic landscape of India. State governments play a vital role in this endeavor, as they can facilitate the translation and dissemination of cybersecurity awareness programs in local languages, thereby promoting digital literacy and online safety among citizens.

To further amplify these efforts, private-public partnerships should be established to drive awareness activities. International examples, such as the US, demonstrate the effectiveness of such collaborations. The White House has initiated several programs to enhance cybersecurity awareness and resilience within K-12 educational institutions, aiming to protect schools from cyber threats and equip them with the necessary tools and knowledge to maintain a secure learning environment. These programs focus on teaching immediate and relatively low-cost prevention strategies such as keeping software up-to-date, implementing multifactor authentication, using strong passwords, and spotting and reporting email phishing threats. Schools can also be encouraged to join the Multi-State Information Sharing and Analysis Center (MS-ISAC) for free, accessing cybersecurity tools, resources, and information sharing to build cybersecurity

C. Recommendation 3: International Collaboration and Standardisation

In a globally connected digital world, no country can effectively safeguard its cyberspace in isolation. Therefore, while drawing its roadmap for capacity building and skill development, India’s cybersecurity strategy should emphasise on international collaboration and alignment with global cybersecurity standards. It should include collaborating with international bodies such as the United Nations and other cybersecurity alliances that can help India both contribute to and learn from global efforts, ensuring that its cybersecurity measures are at par with other leading countries.

V. Pillar V: Leveraging Emerging Technologies

Despite the challenges posed by emerging technologies such as AI and quantum computing, they also have the potential to enhance India's overall cybersecurity posture. While AI can be exploited for malicious purposes like crafting realistic phishing campaigns or automating attacks, it also provides critical benefits in detecting and responding to cyber threats more efficiently. Similarly, while quantum computing could potentially compromise existing cryptographic measures, it also presents opportunities to develop breakthrough encryption methods that can secure data against future threats.

Recommendation

The National Cybersecurity Strategy of India should comprehensively acknowledge both the potential benefits and inherent risks posed by emerging technologies including AI and quantum computing. It should emphasise the importance of targeted research, development, and demonstration (R&D) activities to effectively address vulnerabilities present in current technologies and anticipate those in future developments. To this end, the AI Application Development Pillar under the India AI Mission should consider developing specific AI solutions to strengthen cybersecurity across critical sectors. In addition, India should accelerate the establishment of an Artificial Intelligence Safety Institute (AISI) as it can play a central role in ensuring the safe development and deployment of AI technologies. The institute should collaborate with existing AI safety institutes and other critical agencies worldwide and advance globally

recognised standards and best practices in AI safety. Furthermore, the strategy should prioritise accelerating the development and adoption of quantum-resistant cryptographic methods. This proactive measure is crucial to protect against the potential threats posed by quantum computing, which could significantly compromise existing cryptographic standards.

VI. Pillar VI: Global cooperation/ International Cooperation

Given the rapid evolution of cyber threats, India's active engagement in global cybersecurity dialogues is crucial to enhance its cyber resilience and shape international cyber norms and standards. It has an active participation across bilateral, regional, and international forums, which positions it as an important factor in current cybersecurity discussions. India can leverage its position by collaborating with global allies by establishing mechanisms for real-time intelligence sharing and coordinated responses to emergent cyber threats. These partnerships can help make significant progress in respect of Mutually Agreed Standards in relations to ICT products and services and capacity-building initiatives targeted towards assisting developing and least developed countries. This form of strategic engagement can help in advancing India's interests at international forums. Over the long term, these efforts can elevate India's role as a leader in strengthening norms of responsible state behaviour, holding nations accountable for irresponsible actions in cyberspace, and disrupting networks behind dangerous cyberattacks globally.

A. Recommendation 1: Strengthen Representation in International Bodies

India's engagement at the bilateral, regional and multilateral forums (including the UN) highlights its commitment to enhancing international cooperation on trusted ICT products and services, emphasising the need for robust cybersecurity standards. To ensure that the development of cybersecurity standards and best practices is aligned with India's cyber-specific legislative or regulatory approach, India's participation in standard-setting organizations like the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and International Telecommunication Union (ITU) should be strengthened. Despite being a participatory country at the ISO, the depth and impact of India's involvement, particularly in IT security, have not matched that of its global counterparts. The National Cybersecurity Strategy must address this discrepancy by prioritising enhanced representation in these forums. It should clearly outline strategies to increase India's contributions, including allocating resources to train and deploy skilled professionals who can actively shape international cybersecurity protocols.

Moreover, India should accelerate the development and implementation of cybersecurity standards aligned with ITU or Common Criteria ISO standards. Initiatives like the 5G testbed at IIT Madras present valuable opportunities for India to lead by example, embedding advanced security benchmarks that could set precedents globally. By advocating and implementing proactive best practice standards and harmonising cyber-specific legislative and regulatory frameworks across industries, India can ensure its cybersecurity measures align with international expectations.

B. Recommendation 2: Cybersecurity Integration in International Agreements

India should drive efforts to incorporate comprehensive cybersecurity clauses into bilateral and plurilateral trade and investment agreements. These clauses should focus on the establishment and adherence to international cybersecurity norms, confidence-building measures, and cybersecurity capacity building. The Ministry of Commerce, leveraging its experience in handling cross-border data issues, should lead this

cybersecurity should not be peripheral but a core element of the agreements, especially in sections dealing with data. This includes defining clear terms for data protection, mechanisms for secure data exchange, and commitments to uphold cybersecurity standards across borders. For example, frameworks similar to the EU's General Data Protection Regulation (GDPR) can be considered as a benchmark for developing clauses related to data privacy and security.

Endnotes

1 Sharma, S., Securing India's Digital Future: Cybersecurity Urgency and Opportunities (THE DIPLOMAT) available at: https://thediplomat.com/2024/01/securing-indias-digital-future-cybersecurity-urgency-and-opportunities/, 'Most targeted' countries facing cyberattacks in 2023 (TIMES OF INDIA) https://timesofindia.indiatimes.com/gadgets-news/most-targeted-countries-facing-cyberattacks-in-2023/photostory/105013886.cms?picid=105013907

2 Efrony, D., The UN Cyber Groups, GGE and OEWG – A Consensus is Optimal, But Time is of the Essence (Just Security) available at: https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/

3 Framework for the US—India Cyber Relationship (USEMBASSY) available at: https://in.usembassy.gov/framework-u-s-india-cyber-relationship/

4 Ministry of External Affairs, India and US sign MoU on Cybercrime Investigations (MEA) available at: https://www.mea.gov.in/press-releases.htm?dtl/38924/India+and+US+sign+MoU+on+Cybercrime+Investigations#:~:text=India%20and%20the%20US%20signed,of%20Homeland%20Security%20(DHS)

5 Glossary, Computer Security Resource Centre (NIST) https://csrc.nist.gov/glossary/term/critical_infrastructure#:~:text=Definitions%3A,any%20combination%20of%20those%20matters.

6 National Critical Information Infrastructure Protection Centre (NCIIPC), available at: https://nciipc.gov.in/

7 Critical Information Infrastructure (CII) (RBI) available at: https://financialservices.gov.in/beta/en/page/cii

8 IANS, 67% of Indian govt & essential services faced over 50% cyberattacks in last 12 months: Report (ET) available at: https://ciso.economictimes.indiatimes.com/news/vulnerabilities-exploits/67-of-indian-govt-essential-services-faced-over-50-cyberattacks-in-last-12-months-report/103490769

9 Lohchab, H., Cyberattacks on healthcare sector rising, 60% of organisations hit in a year: report (ET) https://economictimes.indiatimes.com/tech/technology/cyberattacks-on-healthcare-sector-rising-60-of-organisations-hit-in-a-year-report/articleshow/104917689.cms?from=mdr

10 Reserve bank of India, India's Digital Revolution: Opportunities and Challenges (RBI) available at: https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=22457#S5

11 Lakshmanan, R., Hackers Hit Indian Defense, Energy Sectors with Malware Posing as Air Force Invite (HACKERNEWS) available at: https://thehackernews.com/2024/03/hackers-target-indian-defense-and.html

12 ET staff, Manufacturing sector worst hit by ransomware in India: Palo Alto Networks' report (ET) available at: https://economictimes.indiatimes.com/tech/technology/manufacturing-sector-worst-hit-by-ransomware-in-india-palo-alto-networks-report/articleshow/108795601.cms?from=mdr

13 R., India's Critical Infrastructure Suffers Spike in Cyberattacks (DARK READING) available at: https://www.darkreading.com/cyber-risk/india-s-critical-infrastructure-suffers-spike-in-cyberattacks

14 Indian Manufacturing Sector Witnesses Most Ransomware Extortion In 2023: Report (BUSINESS WORLD) available at: https://www.businessworld.in/article/indian-manufacturing-sector-witnesses-most-ransomware-extortion-in-2023-report-514695

15 Deore, P., et al., India Cyber Threat Report 2023 (DSCI) available at: https://www.dsci.in/files/content/knowledge-centre/2023/India-Cyber-Threat-Report-2023_0.pdf

16 Cyber attacks on critical infrastructure (ALLIANZ) available at: https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html

17 What is Critical Infrastructure Protection (CIP)? (DARKTRACE) available at: https://darktrace.com/cyber-ai-glossary/critical-infrastructure-protection-cip#:~:text=The%20Healthcare%20and%20Public%20Health%20Sector.%20This,prime%20target%2C%20necessitating%20proactive%20healthcare%20cybersecurity%20measures.

18 Kearney, L., US electric grid growing more vulnerable to cyberattacks, regulator says (REUTERS) available at: https://www.reuters.com/technology/cybersecurity/us-electric-grid-growing-more-vulnerable-cyberattacks-regulator-says-2024-04-04/

19 Rosenbaum, E., America's largest water utility hit by cyberattack at time of rising threats against US infrastructure (CNBC) available at: https://www.cnbc.com/2024/10/08/american-water-largest-us-water-utility-cyberattack.html

20 Veillon, D., Cyber Attacks in Transportation (ARCHITEKS) available at: https://www.itarchiteks.com/8-recent-cyber-attacks-that-have-affected-the-transportation-industry

21 Office of the National Cyber Director Executive Office of the President, *2024 Report on the Cybersecurity Posture of the United States* (THE WHITE HOUSE) available at: https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf

22 Office of the Director of National Intelligence, Annual Threat of the U.S. Intelligence Community (ODNI) available at: https://www.odni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

23 Easterly, J., The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years (CISA) available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

24 Ajaykumar, S., Securing India's critical infrastructure: Prioritising cybersecurity in chemical facilities (ORF) available at: https://www.orfonline.org/expert-speak/securing-india-s-critical-infrastructure-prioritising-cybersecurity-in-chemical-facilities

25 Chawla, G., 'The legal contours of India's 'sovereign cyberspace', (INDIA SEMINAR) available at: https://www.india-seminar.com/2020/731/731_gunjan_chawla.htm

26 Id.

27 'Cyberespionage' Module 14: Hacktivism, Terrorism, Espionage, Disinformation Campaigns and Warfare in Cyberspace (UNODC) available at: https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html

28 Barik, S., AIIMS cyberattack probe points to 'foreign state actor', Govt looks at mandatory audits (INDIAN EXPRESS) available at: https://indianexpress.com/article/cities/delhi/aiims-cyberattack-probe-points-to-foreign-state-actor-govt-looks-at-mandatory-audits-8303330/

29 Cyber Case Study: Colonial Pipeline Ransomware Attack (INSURICA) available at: https://insurica.com/blog/colonial-pipeline-ransomware-attack/

30 Aggarwal, M., Ransomware Attack: An Evolving Targeted Threat (MEITY) available at: https://www.meity.gov.in/writereaddata/files/Ransomware_Attack_An_Evolving_Targeted_Threat.pdf; What is Malware vs. Ransomware? (PALOALTO) available at: https://www.paloaltonetworks.com/cyberpedia/what-is-malware-vs-ransomware

31 Crowdstrike 2024 Global Threat Report (CLOUDSTRIKE) available at: https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

32 Supra note 22.

33 Mukherjee, M., India second highest target for ransomware attacks in Asia Pacific: Report (BUSINESS STANDARD) available at: https://www.business-standard.com/india-news/india-second-highest-target-for-ransomware-attacks-in-asia-pacific-report-124101500791_1.html

34 Deore, P., et al., India Cyber Threat Report 2023 (DSCI) available at: https://www.dsci.in/files/content/knowledge-centre/2023/India-Cyber-Threat-Report-2023_0.pdf

35 Manufacturing the worst hit by ransomware in India (ENTERPRISE IT WORLD) available at: https://www.enterpriseitworld.com/manufacturing-the-worst-hit-by-ransomware-in-india/; Mukherjee, M., India second highest target for ransomware attacks in Asia Pacific: Report (BUSINESS STANDARD) available at: https://www.business-standard.com/india-news/india-second-highest-target-for-ransomware-attacks-in-asia-pacific-report-124101500791_1.html

36 Mukherjee, M., India second highest target for ransomware attacks in Asia Pacific: Report (BUSINESS STANDARD) available at: https://www.business-standard.com/india-news/india-second-highest-target-for-ransomware-attacks-in-asia-pacific-report-124101500791_1.html

37 Supra note 22.

38 Constantin, L., REvil ransomware explained: A widespread extortion operation (CSO) available at: https://www.csoonline.com/article/570101/revil-ransomware-explained-a-widespread-extortion-operation.html

39 Deore, P., et al., India Cyber Threat Report 2023 (DSCI) available at: https://www.dsci.in/files/content/knowledge-centre/2023/India-Cyber-Threat-Report-2023_0.pdf

40 Supra note 22.

41 Supra note 22.

42 Govt Confirms Data Breach At BSNL, Says Panel Formed To Audit Telecom Networks (INC42) available at: https://inc42.com/buzz/govt-confirms-data-breach-at-bsnl-says-panel-formed-to-audit-telecom-networks/

43 Singh, J., Indian government's cloud spilled citizens' personal data online for years (TECHCRUNCH) available at: https://techcrunch.com/2024/04/02/indian-government-cloud-spilled-citizens-personal-data-online-for-years/?ref=static.internetfreedom.in

44 The Wire, Apple Warns Top Indian Opposition Leaders, Journalists About 'State-Sponsored' Attack on Phone, available at: https://thewire.in/rights/apple-india-state-sponsored-spyware

45 Supra note 22.

46 Research Report: AI-Driven Phishing Attack on a Financial Institution in India (2024) (CYBER PEACE) available at: https://www.cyberpeace.org/resources/blogs/research-report-ai-driven-phishing-attack-on-a-financial-institution-in-india-2024

47 Deore, P., et al., India Cyber Threat Report 2023 (DSCI) available at: https://www.dsci.in/files/content/knowledge-centre/2023/India-Cyber-Threat-Report-2023_0.pdf

48 Microsoft 365 Security, HAFNIUM targeting Exchange Servers with 0-day exploits (MICROSOFT) available at: https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/; Cybersecurity and Infrastructure Security Agency, Cybersecurity Advisory: Mitigate Microsoft Exchange Server Vulnerabilities (CISA) available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-062a

49 Easterly, J., The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years (CISA) available at: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

50 Volz, D., How Chinese Hackers Graduated From Clumsy Corporate Thieves to Military Weapons (WSJ) available at https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95?utm_

51 Lyngaas, S., Chinese hackers breached US government office that assesses foreign investments for national security risks (CNN) available at: https://edition.cnn.com/2025/01/10/politics/chinese-hackers-breach-committee-on-foreign-investment-in-the-us/index.html?iid=cnn_buildContentRecirc_end_recirc

52 Bing, C., Exclusive: Accused Iranian hackers successfully peddle stolen Trump emails (REUTERS) available at: https://edition.cnn.com/2025/01/10/politics/chinese-hackers-breach-committee-on-foreign-investment-in-the-us/index.html?iid=cnn_buildContentRecirc_end_recirc

53 IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities (CISA) available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a#:~:text=CyberAv3ngers%20is%20an%20Iranian%20IRGC,%2C%20Israel%2C%20and%20other%20countries.

54 Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023 (HOMELAND SECURITY) available at: https://www.dhs.gov/news/2024/04/02/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer

55 Barik, S., AIIMS cyberattack probe points to 'foreign state actor', Govt looks at mandatory audits (INDIAN EXPRESS) available at: https://indianexpress.com/article/cities/delhi/aiims-cyberattack-probe-points-to-foreign-state-actor-govt-looks-at-mandatory-audits-8303330/

56 Lohchab, H., Pakistan-based hackers step up attacks against Indian govt systems (ET) available at: https://economictimes.indiatimes.com/tech/technology/pakistan-based-hackers-step-up-attacks-against-govt-systems/articleshow/110649581.cms?utm

57 Lakshmanan, R., Iranian Hackers Use "Dream Job" Lures to Deploy SnailResin Malware in Aerospace Attacks (THE HACKER NEWS) available at: https://thehackernews.com/2024/11/iranian-hackers-use-dream-job-lures-to.html

58 EclecticIQ details Operation FlightNight targeting Indian government entities, energy sector (INDUSTRIAL CYBER) available at: https://industrialcyber.co/ransomware/eclecticiq-details-operation-flightnight-targeting-indian-government-entities-energy-sector/?utm

59 Singh, R., Explained: The massive data leak from a Chinese cybersecurity agency, whose targets include India (THE INDIAN EXPRESS) available at: https://indianexpress.com/article/explained/china-data-leak-surveillance-india-github-9175313/?utm

60 Singh, V., G-20 website was subjected to an organised cyber attack during India summit: CEO of I4C (THE HINDU) available at: https://www.thehindu.com/news/national/g-20-website-was-subjected-to-an-organised-cyber-attack-during-india-summit-ceo-of-i4c/article67702605.ece

61 Antonuik, D., Pakistan-linked hackers target India's education sector with Crimson malware (THE RECORD) available at: https://therecord.media/pakistan-linked-hackers-target-indias-education-sector?utm_

62 House Homeland Releases "Cyber Threat Snapshot" Highlighting Rising Threats to US Networks, Critical Infrastructure (HOMELAND SECURITY) available at: https://homeland.house.gov/2024/11/12/new-house-homeland-releases-cyber-threat-snapshot-highlighting-rising-threats-to-us-networks-critical-infrastructure/?utm_; Fox, A., Ascension confirms data breached in Black Basta ransomware attack (HEALTHCARE IT NEWS) available at: https://www.healthcareitnews.com/news/ascension-confirms-data-breached-black-basta-ransomware-attack; Capoot, A., Ransomware group Blackcat is behind cyberattack on UnitedHealth division, company says (CNN) available at: https://www.cnbc.com/2024/02/29/blackcat-claims-responsibility-for-cyberattack-at-unitedhealth.html

63 City of Oakland Restores and Recovers Systems Affected by Ransomware Attack (OAKLAND CA) available at: https://www.oaklandca.gov/news/city-of-oakland-restores-and-recovers-systems-affected-by-ransomware-attack

64 Tye, C., Cyberattack temporarily takes down websites for O'Hare and Midway airports (CBS) available at: https://www.cbsnews.com/chicago/news/cyberattack-ohare-midway-airport-websites-russian-hackers/

65 Mazzei, P., Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000 (NYT) available at: https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html

66 Atlanta US Attorney Charges Iranian nationals for City Of Atlanta ransomware attack (DOJ) available at: https://www.justice.gov/usao-ndga/pr/atlanta-us-attorney-charges-iranian-nationals-city-atlanta-ransomware-attack

67 Meatpacker JBS says it paid equivalent of $11 mln in ransomware attack (REUTERS) available at: https://www.reuters.com/technology/jbs-paid-11-mln-response-ransomware-attack-2021-06-09/

68 Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers (CISA) available at: https://cisa.gov/news-events/news/kaseya-ransomware-attack-guidance-affected-msps-and-their-customers

69 Mishra, A., Personal information of 750 mn Indians up for sale on dark web: CloudSEK (BUSINESS STANDARD) https://www.business-standard.com/companies/news/personal-information-of-750-mn-indians-up-for-sale-on-dark-web-cloudsek-124012500973_1.html?ref=static.internetfreedom.in

70 KVN, R., Details of 18 crore Domino's India customers on sale on dark web (DECCAN HERALD) available at: https://www.deccanherald.com/specials/details-of-18-crore-dominos-india-customers-on-sale-on-dark-web-989336.html?

71 Reg: Interruption in retail payments (NPCI) available at: https://www.npci.org.in/PDF/npci/press-releases/2024/NPCI-Press-Release-Interruption-in-Retail-Payments.pdf

72 PTI, Bots sharing Star Health data removed; monitoring any recreation: Telegram (BUSINESS STANDARD) available at: https://www.business-standard.com/technology/tech-news/bots-sharing-star-health-data-removed-monitoring-any-recreation-telegram-124101100939_1.html

73 SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic) (USGAO) available at: https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

74 What is the Log4j vulnerability? (IBM) available at: https://www.ibm.com/think/topics/log4j

75 Kapko, M., Progress Software's MOVEit meltdown: uncovering the fallout (CYBERSECURITY DRIVE) available at: https://www.cybersecuritydive.com/news/progress-software-moveit-meltdown/703659/

76 Chadha, S., Explained: 17,000 ICICI Bank credit cards blocked after data breach (BUSINESS STANDARD) https://www.business-standard.com/finance/personal-finance/17-000-icici-bank-credit-cards-mapped-to-wrong-users-what-this-means-124042600115_1.html

77 Panjiar, T., IFF Explains: How a vulnerability in a government cloud service could have exposed the sensitive personal data of 2,50,000 Indian citizens (IFF) available at: https://internetfreedom.in/vulnerability-in-a-government-cloud-service/

78 India Confirms State-Owned Telecom Giant BSNL's Data Breach, Millions of User Records Compromised (CYBER EXPRESS) available at: https://thecyberexpress.com/india-confirms-bsnl-data-breach/

79 Mishra, A., Govt pension portal for defence personnel SPARSH suffers data breach (BUSINESS STANDARD) available at: https://www.business-standard.com/india-news/govt-pension-portal-for-defence-personnel-sparsh-suffers-data-breach-124011000128_1.html?ref=static.internetfreedom.in

80 Lakshmanan, R., WazirX Cryptocurrency Exchange Loses $230 Million in Major Security Breach (HACKER NEWS) available at: https://thehackernews.com/2024/07/wazirx-cryptocurrency-exchange-loses.html

81 How US Court Found Pegasus Maker Liable For Attacks On 1,400 WhatsApp Users (NDTV) available at: https://www.ndtv.com/world-news/us-court-finds-pegasus-spyware-maker-liable-over-whatsapp-hack-explained-7299703

82 The White House, *National Security Strategy of the United States* (2022) available at: https://bidenwhitehouse.archives.gov/about-the-white-house/.

83 Department of Defence, National Defence Strategy of United States of America 2022, available here: https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf

84 The White House, National Cybersecurity Strategy 2023, available here: https://bidenwhitehouse.archives.gov/therecord/

85 Executive Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity, 2021-10460 (86 FR 26633) available at https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

86 It is informed by and implements the values of the DFI, the Freedom Online Coalition, and other long-standing efforts to realize a democratic vision for our digital ecosystem. It carries forward the foundational direction of Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," National Security Memorandum (NSM) 5, "Improving Cybersecurity for Critical Infrastructure Control Systems," NSM 8, "Improving the Cybersecurity of National Security, Department of Defense (DoD), and Intelligence Community Systems," and other executive actions. It integrates cybersecurity into the once-in-a-generation new investments made by the Bipartisan Infrastructure Law, the Inflation Reduction Act, the Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act, and EO 14017, "America's Supply Chains."

87 Jacquelyn Schneider, From Offense to Defence: America's Cyber Strategy Pivot, YouTube video (HOOVER INSTITUTION), available at https://www.youtube.com/watch?v=2Dg6Myn2ymU&list=TLGG_weJ4q_pvhwxNTAxMjAyNQ&t=1s.

88 The White House, National Cybersecurity Strategy 2023, available here: https://bidenwhitehouse.archives.gov/therecord/

89 These include: Chemical Sector, Commercial Facilities Sector, Communications Sector, Critical Manufacturing Sector, Dams Sector, Defense Industrial Base Sector, Emergency Services Sector Energy Sector, Financial Services Sector, Food and Agriculture Sector, Government Facilities Sector, Healthcare and Public Health Sector, Information Technology Sector, Nuclear Reactors, Materials, and Waste Sector, Transportation Systems Sector and, Water and Wastewater Systems Sector. America's Cyber Defence Agency, Critical Infrastructure available at: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

90 Rosenzweig, P., Turns Out It is not 85 Percent (LAWFARE) available at: https://www.lawfaremedia.org/article/turns-out-it-not-85-percent#:~:text=For%20many%20years%2C%20American%20leaders,if%20those%20statistics%20were%20accurate.

91 Homeland Security, The National Cyber Incident Response Plan 2016 (NCIRP) available here: https://www.cisa.gov/sites/default/files/2023-01/national_cyber_incident_response_plan.pdf

92 The Cyber Incident Reporting for Critical Infrastructure Act, 2022 was enacted to enhance the United States' cybersecurity defenses by mandating that critical infrastructure entities report certain cyber incidents and ransom payments to the Cybersecurity and Infrastructure Security Agency (CISA). Cyber Incident Reporting for Critical Infrastructure Act of 2021, H.R. 5440, 117th Cong. (2021-2022) available here: https://www.congress.gov/bill/117th-congress/house-bill/2471/text

93 The National Security Memoranda (NSM) are directives issued by the President of the United States that pertain specifically to the national security interests of the country. These documents can outline strategic priorities, direct specific actions to be taken by federal departments and agencies, or set policy frameworks for how certain national security issues should be handled. The list of NSMs released under present US Administration can be accessed here: National Security Memorandum 8, Improving the Cybersecurity of National Security, Department of Defence, and Intelligence Community Systems (2022) https://irp.fas.org/offdocs/nsm/index.html

94 The Secure Software Development Framework by NIST is set of fundamental, sound, and secure software development practices based on established secure software development practice documents to reduce the vulnerability. National Institute of Standards and Technology, Secure Software Development Framework available here: https://csrc.nist.gov/projects/ssdf

95 Infrastructure Investment and Jobs Act, H.R. 3684, 117th Cong. (2021) available at: https://www.congress.gov/bill/117th-congress/house-bill/3684/text

96 CHIPS and Science Act, H.R. 4346, 117th Cong. (2021-2022) available here: https://www.congress.gov/bill/117th-congress/house-bill/4346

97 America's Cyber Defence Agency, CISA Software Bill of Materials (SBOM) available at: https://www.cisa.gov/sbom

98 CHIPS and Science Act, H.R. 4346, 117th Cong. (2021-2022) available here: https://www.congress.gov/bill/117th-congress/house-bill/4346

99 National Security Memorandum on Promoting US Leadership in Quantum Computing while Mitigating Risks to Vulnerable Cryptographic Systems available at: https://crsreports.congress.gov/product/pdf/IN/IN11921

100 National Institute of Standards and Technology, NICE available at: https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan

101 Ministry of Electronics and Information Technology (MeitY), India Semiconductor Mission available at https://www.ism.gov.in/

102 Ministry of Electronics and Information Technology, IndiaAI Mission available at: https://indiaai.gov.in/

103 Ministry of Electronics and Information Technology (MeitY), Annual Report 2023-2024 available at: https://www.meity.gov.in/writereaddata/files/MEITY-AR-2023-24.pdf

104 Ministry of Electronics and Information Technology, Year-end Review 2024 of Ministry of Electronics and Information Technology available at: https://pib.gov.in/PressReleasePage.aspx?PRID=2088990 See also: https://pib.gov.in/PressReleasePage.aspx?PRID=2037115

105 Indian National Cybersecurity Policy 2013 available at: https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf

106 Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013 define "Critical Sector" as sectors, which are critical to the nation and whose incapacitation or destruction will have a debilitating impact on national security, economy, public health, or safety. At present, there are seven critical sectors designated by NCIIPC. These include, Transport, Power and Energy, Telecom, Government, Banking, Financial Services and Insurance, Strategic and Public Enterprises, and Healthcare.

107 The Information Technology Act 2000, available at: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

108 Ibid

109 In India, the Information Technology (IT) Act 2000 is foundational legislation on cybersecurity provides statutory recognition to electronic transactions and communications, aims to prevent unauthorized access and cybercrimes, and defines offences such as hacking, phishing, and identity theft. The Act is supplemented by rules such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Information Technology (CERT-In and Manner of Performing Functions and Duties) Rules, 2013, and Critical Information Infrastructure (Protection) Rules, 2014, among others. In addition, specific regulations/ guidelines are also issued by sectoral regulators. For instance, the Reserve Bank of India (RBI) mandates standards for banks, such as cyber security/ resilience framework. Similarly, the Securities and Exchange Board of India (SEBI) and Insurance Regulatory and Development Authority (IRDAI) impose similar obligations on their regulated entities. Additionally, guidelines for the protection of Critical Information Infrastructure (CII), issued by the National Critical Information Infrastructure Protection Centre (NCIIPC), ensure enhanced security in sectors like telecom, banking, and power.

110 The architecture of cybersecurity institutions in India consists of a complex inter-ministerial inter-departmental ecosystem. The National Security Advisor (NSA) oversees cybersecurity at the highest level, heading the National Security Council Secretariat (NSCS) and the National Technical Research Organization (NTRO). Aside from this, various ministries and departments look after the different aspects of cybersecurity. The Ministry of Defence (MoD) handles cybersecurity threats and vulnerabilities specific to the defence sector. MeitY acts as the national nodal ministry for cyberspace, and addresses broader cybersecurity concerns, including non-critical government sectors and private sector CII. The Ministry of Communications (MoC) oversees telecom policies, licensing, and cybersecurity aspects of telecommunication infrastructure. The Ministry of External Affairs (MEA) New Emerging and Strategic Technologies (NEST) Division handles international engagement on emerging technologies, cybersecurity diplomacy, and coordination with foreign governments. The Ministry of Home Affairs (MHA) plays a critical role in framing policies related to the classification, handling, and security of government information.

111 Chawla, G., Aravindakshan, S. and Srivastava, V., Comments to the National Security Council Secretariat on the National Cybersecurity Strategy 2020 (CCG NLUD) available at: https://drive.google.com/file/d/14XfyXu-5sAPgzAmEaKE78vphTTfH_Y5s/view

112 Sharma, S., Securing India's Digital Future: Urgency and Opportunities (THE DIPLOMAT) available at: https://thediplomat.com/2024/01/securing-indias-digital-future-cybersecurity-urgency-and-opportunities/

113 Ibid.

114 Ministry of External Affairs, India-US Bilateral Relations available at: https://www.mea.gov.in/Portal/ForeignRelation/Bilateral_Brief_as_on_09.10.2023.pdf

115 Kronstadt, K. A., & Akhtar, S. I., India-U.S. Relations: Issues for Congress (R47597). Congressional Research Service. Available at: https://crsreports.congress.gov/product/pdf/R/R47597

116 Ray, T. (2024). India-U.S. Technology Ties: Charting an Ambitious Course for the Future (OBSERVER RESEARCH FOUNDATION) Available at: https://www.orfonline.org/research/india-u-s-technology-ties-charting-an-ambitious-course-for-the-future.

117 U.S.-India Cyber Security Forum: Enhanced Cooperation to Safeguard Shared Information Infrastructures (US DEPARTMENT OF STATE) available at: https://2001-2009.state.gov/p/sca/rls/fs/2006/62530.htm

118 Jain, R. Revival of India-US ICT Working Group: Significance for India – Analysis (EURASIA REVIEW) available at: https://www.eurasiareview.com/16032015-revival-of-india-us-ict-working-group-significance-for-india-analysis/

119 Ministry of External Affairs, India- US Cybersecurity Forum- Factsheet, available at: https://www.mea.gov.in/bilateral-documents.htm?dtl/6014/IndiaUS+Cyber+Security+Forum++Fact+Sheet/; See also: US Department of States Archive, US-India Cybersecurity Forum: Enhanced Cooperation to Safeguard Shared Information Infrastructure available at: https://2001-2009.state.gov/p/sca/rls/fs/2006/62530.htm, Ministry of External Affairs, Indo-US Cyberterrorism Initiative Plenary Meeting of Indo-us Cybersecurity Forum, available at: https://www.mea.gov.in/press-releases.htm?dtl/13416/IndoUS+Cyberterrorism+Initiative+Plenary+Meeting+of+IndoUS+Cyber+Security+Forumhttps://www.mea.gov.in/bilateral-documents.htm?dtl/6014/IndiaUS+Cyber+Security+Forum++Fact+Sheet/

120 Embassy of India at Washington DC, USA, First Meeting of Joint Working Group on Information and Communications Technology (ICT) available at https://www.indianembassyusa.gov.in/ArchivesDetails?id=481

121 Ministry of External Affairs, India US Strategic Dialogue Joint Statement available at: https://www.mea.gov.in/bilateral-documents.htm?dtl/89/IndiaUS+Strategic+Dialogue+Joint+Statement
Ministry of Home Affairs, India US Senior Officials Homeland Security Dialogue in New Delhi available at: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2009797

122 Ministry of Home Affairs, India US Senior Officials Homeland Security Dialogue in New Delhi available at: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2009797

123 Homeland Security, United States and India Sign Cybersecurity Agreement, available at: https://www.dhs.gov/archive/news/2011/07/19/united-states-and-india-sign-cybersecurity-agreement

124 US Embassy and Consulates in India, Framework for US Inda Cybersecurity Relationship, available at: https://in.usembassy.gov/framework-u-s-india-cyber-relationship/

125 Ministry of Commerce and Industry, MOU on Semiconductor Supply chain and Innovation Partnership between India and US signed following the Commercial Dialogue 2023 available at: https://pib.gov.in/PressReleasePage.aspx?PRID=1905522

126 Ministry of External Affairs (MEA), Joint Fact Sheet : United States and India Elevate Strategic Partnership with the Initiative on Critical and Emerging Technology available at: https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/31/fact-sheet-united-states-and-india-elevate-strategic-partnership-with-the-initiative-on-critical-and-emerging-technology-icet/

127 Department of Foreign Affairs and Trade, Australian Government, The Quad available at https://www.dfat.gov.au/international-relations/regional-architecture/quad

128 Diletta, F., Cybersecurity though QUAD (SASAKAWA PEACE FOUNDATION) available at: www.spf.org/iina/en/articles/diletta_01.html. See also:

129 Ministry of External Affairs, 2024 QUAD Leaders' Summit available at: https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-quad-leaders-summit/

130 Supra note 149.

131 Group of 20 (G20)https://www.g20.in/en/about-g20/about-g20.html

132 Ministry of Home Affairs, Full text of Union Home Minister Shri Amit Shah's address at the inaugural session of G20 Conference on Crime and Security in the age of NFTs, Artificial Intelligence and Metaverse (PIB) available at: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1939176

133 US Department of Commerce, Press Release on Indo-Pacific Economic Framework for Prosperity Ministerial Meeting in Singapore available at: https://www.commerce.gov/news/press-releases/2024/06/press-statement-indo-pacific-economic-framework-prosperity-ministerial

134 Haidar, S., India Stays out of 'trade pillar' at the Indo Pacific Meet (THE HINDU) available at https://www.thehindu.com/business/Industry/india-not-part-of-ipefs-trade-pillar-broader-consensus-yet-to-emerge-among-nations/article65873087.ece

135 Ministry of Commerce and Industry, Supply Chain Council formed under Supply Chain Resilience Agreement, with USA as Chair and India as Vice-Chair (PIB) https://pib.gov.in/PressReleseDetailm.aspx?PRID=2080247&reg=3&lang=1

136 UNGA Resolution 53/70, UN Doc A/RES/53/70 (4 January 1999) available at: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/a_res_53_70.pdf

137 United Nations office for Disarmament Affairs, Developments in the field of information and telecommunications in the context of international security available at: https://disarmament.unoda.org/ict-security/

138 UN General Assembly, Resolution [A/RES/75/240], UN Doc A/RES/[A/RES/75/240] [January 2021] https://documents.un.org/doc/undoc/gen/n21/000/25/pdf/n2100025.pdf

139 US Department of State, United States International Cyberspace and Digital Policy Strategy 2024 available at: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/

140 Basu, A., Ideological Agnosticism and Selective Engagement: How India Sees the Global Cybersecurity Norms Debate available at: https://casi.sas.upenn.edu/iit/arindrajitbasu

141 https://news.un.org/en/story/2024/12/1158521

142 UN General Assembly, Resolution 74/247, UN Doc A/RES/[Number] ([Date] https://documents.un.org/doc/undoc/gen/n19/440/28/pdf/n1944028.pdf

143 UN General Assembly, Resolution A/AC.291/L.15 (August 2024) https://documents.un.org/doc/undoc/ltd/v24/055/06/pdf/v2405506.pdf

144 International Counter Ransomware Initiative (CRI) https://www.counter-ransomware.org/aboutus

145 Department of Home Affairs, Australian Government, Counter Ransomware Initiative available at: https://www.homeaffairs.gov.au/cyber-security-subsite/Pages/counter-ransomware-initiative.aspx

146 Dobell, A., The International Counter Ransomware Initiative (CRI): Form Forming to Norming to Performing available at: https://www.centerforcybersecuritypolicy.org/insights-and-research/the-international-counter-ransomware-initiative-from-forming-and-norming-to-performing

147 https://www.homeaffairs.gov.au/cyber-security-subsite/Pages/counter-ransomware-initiative.aspx

148 The White House, International Counter Ransomware Initiative jhttps://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/

149 Information Sharing and Analysis Centres (ISACs): Cooperative Models (ENISA) https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-1-3%202%20Information%20Sharing%20and%20Analysis%20Center%20%28ISACs%29%20Cooperative%20models.pdf

150 EU-ISACs By the Numbers 2021 (EU) https://www.isacs.eu/sites/default/files/flmngr/EU%20ISACS%20BY%20THE%20NUMBERS%202021_1.pdf

151 ISACs are member-driven organizations, delivering all-hazards threat and mitigation information to asset owners and operators (NATIONAL COUNCILS OF ISACS) https://www.nationalisacs.org/

Notes

Notes

Authors
Sukanya Thapliyal and Vedika Pandey

Acknowledgements
We extend our sincere gratitude to Shri Rakesh Maheshwari, Former Sr. Director and Group Coordinator, Cyber Laws and Data Governance, Ministry of Electronics and Information Technology, Ms Ranjana Khanna, DG & CEO, AMCHAM India, Mr Pranav Mishra, Director Cyber Security Committee, AMCHAM India, Mr Binu George, Head of Government Affairs - India, Fortinet and Members of the American Chamber of Commerce (AMCHAM). Their valuable contributions and support have greatly enriched this publication.

©2025 Koan Advisory Group and AMCHAM India