

Digital infrastructure in South Asia:

China's role and the potential for Australia–India cooperation

REPORT

Shruti Jargad



About the author

Shruti Jargad is a visiting fellow at ASPI. Her fellowship is supported by DFAT and Centre for Australia-India Relations.

Acknowledgements

I would like to thank Justin Bassi and James Corera for their guidance, and I am especially grateful to Dr Rajeswari Rajagopalan for her dedicated mentorship over the course of this fellowship. Her expert feedback and encouragement throughout the drafting process were vital to the completion of this report.

I wish to thank the reviewers, Dr Geoff Wade (ASPI), Dr Devendra Kumar (Shiv Nadar University) and Dr Sameer Patil (Observer Research Foundation) for their rigorous review and for providing critical perspectives that enhanced the depth of the report.

I would also like to express my sincere appreciation to the ASPI Cyber, Technology and Security team for their collegiality and support.

About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

About Reports

Reports deliver original and deeply researched analysis and judgements on issues of strategic significance and ongoing importance. Reports aim to inform and influence national strategic choices with original, deeply researched analysis that surfaces implications, tests assumptions, and may consider future courses of action.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services.

© The Australian Strategic Policy Institute Limited 2026

This publication is subject to copyright. Except as permitted under the *Copyright Act 1968*, no part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission. Enquiries should be addressed to the publishers. Notwithstanding the above, educational institutions (including schools, independent colleges, universities and TAFEs) are granted permission to make copies of copyrighted works strictly for educational purposes without explicit permission from ASPI and free of charge.

First published August 2026

Published in Australia by the Australian Strategic Policy Institute

ISSN: 3083-2853 (Online), 3083-2861 (Print)

ASPI

Level 2

40 Macquarie Street

Barton ACT 2600

Australia

Tel Canberra + 61 2 6270 5100

Email enquiries@aspi.org.au

www.aspi.org.au

www.aspistrategist.org.au



[Facebook.com/ASPI.org](https://www.facebook.com/ASPI.org)



[@ASPI_org](https://twitter.com/ASPI_org)

Cover image: iStockphoto/sutlafk.

Contents

Executive summary	2
Recommendations	3
Introduction	4
The geopolitics of digital infrastructure	5
The state of digital infrastructure in South Asia	6
China's digital engagements in South Asia	7
The Digital Silk Road	7
Mapping China's footprint	8
Emerging risks and challenges	10
Advancing India–Australia synergy for digital transformation	11
Conclusion	13
Appendix	14
Acronyms and abbreviations	17

Executive summary

South Asia's digital transformation is gathering pace. It has also become a critical arena of strategic competition, especially between India and China. A central finding of this report is that the main risk facing the region isn't Chinese involvement in itself, but the combination of limited alternatives and weak state capacity, which can leave governments with fewer choices over vendors, standards, financing and governance models.

China has established a comprehensive presence in the digital economy of the region under the Digital Silk Road Initiative while furthering its strategic objectives. Chinese firms have become deeply embedded across South Asia's digital ecosystem, supplying telecommunications equipment, smartphones, fibre-optic networks, submarine cables, data centres, surveillance technologies, cloud services, digital payment systems and e-commerce platforms. This 'supply' doesn't necessarily prioritise the South Asian nations. Supported by state-backed financing, which has augmented their competitive pricing and implementation capacity, Chinese companies have helped to accelerate digital connectivity and infrastructure development throughout the region. However, that often comes with strings attached, such as fixed vendors, legal opacity, unsustainable financing and Chinese technical standards. Thus, China's growing digital presence has raised concerns regarding technological lock-in, data governance, transparency, cybersecurity and strategic autonomy. As digital systems become increasingly integrated into critical infrastructure and government services, these questions have assumed growing strategic importance for South Asian states.

This report argues that the central challenge facing South Asia is how to pursue digital transformation alongside resilience, institutional capacity and policy autonomy. Examining regional digital development with a geopolitical lens, the report emphasises the importance of expanding the choices available to South Asian governments through trusted, transparent and locally responsive partnerships. The objective should be to support countries in pursuing digital transformation on terms that reflect their own development priorities rather than creating new forms of technological dependence.

Within this context, India and Australia possess complementary capabilities that position them to become valuable partners in supporting digital development in the region. For India, strengthening digital cooperation with its neighbours aligns closely with broader objectives of enhancing regional connectivity, resilience and economic integration. India's internationally recognised experience in deploying digital public infrastructure (DPI) at scale demonstrates how affordable and interoperable digital systems can improve governance, financial inclusion and public service delivery. Australia, meanwhile, has developed recognised expertise in e-governance, cybersecurity, infrastructure

financing, institutional capacity building and regulatory cooperation. Both countries also share an interest in promoting secure, trusted and interoperable digital ecosystems across the Indo-Pacific.

The report acknowledges important structural constraints. Neither India nor Australia offers a vertically integrated digital ecosystem. There's also an asymmetry in motive: India's interest in South Asian digital connectivity is inseparable from its security concerns about Chinese influence on its periphery, while Australia's interest is more diffuse, centred on Indo-Pacific stability and alignment with Quad partners. Australia carries less political baggage in the region than India, but it also has less leverage, given its weaker historical, economic and diaspora ties to South Asia. Despite those constraints, the strength of the Australia-India partnership lies in using existing bilateral, regional and public-diplomacy mechanisms to address gaps in digital infrastructure financing, regulatory governance, cybersecurity and human capacity. This approach emphasises collaboration, local ownership and institutional resilience. Together, the two countries can facilitate international partnerships, strengthen regional digital frameworks and support more secure, inclusive and interoperable digital ecosystems. The report outlines a series of practical policy recommendations, including expanding existing regional initiatives to focus on digital investment, connectivity, collaboration, security and resilience.

Recommendations

1. Expanding SARIC to include digital infrastructure

The SARIC (South Asia Regional Infrastructure Connectivity) initiative should be expanded to incorporate digital infrastructure as a core pillar alongside transport and energy connectivity.

As digital connectivity increasingly underpins economic growth, public service delivery and regional integration, investments in submarine cables, terrestrial fibre networks, internet exchange points, data centres and resilient communications infrastructure should be viewed as essential components of development. Australia's experience in facilitating infrastructure financing from multilateral institutions such as the International Finance Corporation and in project preparation, combined with India's extensive implementation at scale experience, through initiatives such as BharatNet and regional connectivity projects, creates opportunities for jointly supporting capital-intensive digital infrastructure projects across South Asia. Such efforts would address persistent connectivity gaps while promoting the diversification of vendors.

2. Regionalising the Australia–India Partnership on Cyber, Critical Technologies and Supply Chains (PACTS)

Australia and India should establish a regular bilateral digital dialogue under PACTS involving political leadership, regulators, industry stakeholders and researchers.

The PACTS, formed in 2026, should be used as a strong institutional basis for extending India–Australia digital cooperation beyond the bilateral relationship. Its predecessor, the 2020 Framework Arrangement on Cyber and Cyber-Enabled Critical Technology Cooperation, supported research collaboration between India and Australia on cybersecurity, critical technologies, telecommunications, artificial intelligence (AI), quantum technologies and submarine cable resilience. The two countries should establish a dedicated South Asia component within the PACTS framework to facilitate regional cooperation and knowledge sharing on telecommunications security, cloud infrastructure, AI governance, digital standards and critical technology supply chains.

3. Supporting digital public infrastructure and e-governance

Australian and Indian complementary capabilities in DPI and e-governance should be leveraged to support dedicated agencies of South Asian nations with grant assistance, capacity building and sharing of governance experience and best practices in the region.

E-governance and public service delivery are a key priority for governments in South Asia. The reusability of DPI across sectors makes it a cost-effective method for achieving whole-of-society digital transformation, which is particularly helpful when working with financing constraints. India's DPI stack, including digital identity (Aadhaar), digital payments (UPI) and cloud storage (DigiLocker), for instance, has improved financial inclusion, service delivery and administrative efficiency at scale. At the same time, Australia has emerged as a global leader in digital government. In 2025, Australia ranked among the top five countries in the World Bank's GovTech Maturity Index and second globally in the Organisation for Economic Co-operation and Development Digital Government Index, reflecting strengths in interoperability, digital identity systems, service integration and citizen-centred digital governance. Importantly, Australian and Indian cooperation should emphasise adaptation to local contexts rather than the replication of any single model, ensuring that digital transformation initiatives remain responsive to national priorities and institutional capacities. India's ongoing grant assistance to establish Sri Lanka's Unique Digital Identity is a step in the right direction.

4. Building human capital and institutional capacity

Establish a South Asia Digital Capacity Initiative to provide training and technical exchanges on cybersecurity, regulation and data governance for public officials and scientific communities and professionals from the region. This should also include scholarships for technical higher education at premier institutions in India and Australia.

Successful digital transformation depends not only on infrastructure but also on the human and institutional capacity needed to govern digital systems effectively. India and Australia possess strong foundations for cooperation through educational partnerships, research collaborations and extensive people-to-people ties, including Australia's large South Asian diaspora communities. Attention should be given to supporting digital literacy and increasing the participation of women and under-represented groups in the digital economy. Such efforts would help to ensure that technological adoption is accompanied by the institutional capacity necessary to manage associated risks and maximise developmental benefits.

5. Strengthening regional cybersecurity and digital resilience

Support strengthening of computer emergency response teams, conduct regional cyber exercises and facilitate information-sharing mechanisms and expert consultations for developing cybersecurity legislation and governance best practices.

Australia's 2023–2030 Cyber Security Strategy demonstrates its commitment to strengthening regional cyber resilience through capacity building, information sharing, critical infrastructure protection and international partnerships. Building on those existing frameworks, India and Australia could jointly support the strengthening of computer emergency response teams (CERTs) across the region. Such initiatives would address growing vulnerabilities arising from the rapid expansion of digital services while helping to build trust in digital systems and strengthen the resilience of critical infrastructure.

6. Mobilising private-sector innovation and technology partnerships

Create a Launching Pad program to connect technology firms with local markets and mobilise private capital investment in the digital infrastructure sector.

Private-sector participation, innovation ecosystems and entrepreneurial networks are essential drivers of technological development and adoption. Australia has already demonstrated the effectiveness of this approach through initiatives such as Austrade's Landing Pad program, which connects technology firms with local markets, investors and government stakeholders in Southeast Asia. India similarly possesses a vibrant technology sector, globally recognised IT services firms and one of the largest

start-up ecosystems globally. Areas of cooperation could include fintech, cybersecurity, digital health, edtech, AI, cloud computing and digital agriculture. Joint innovation funds, start-up accelerators and venture capital partnerships would help to mobilise private investment while creating opportunities for technology transfer and regional market integration.

7. Leveraging existing regional and multilateral platforms

Align bilateral initiatives with regional and multilateral platforms to build trust and political support and mobilise additional financial resources.

India and Australia could maximise the use of existing regional and multilateral platforms. Both countries are active participants in the Quad's initiatives on secure telecommunications, critical technologies, submarine cable resilience and cybersecurity capacity building.¹ They've also collaborated through the G20, particularly during India's presidency, which elevated DPI to a global development priority.² By aligning bilateral initiatives with those broader frameworks, India and Australia can mobilise additional financial resources, technical expertise and political support while avoiding duplication and ensuring greater regional legitimacy. Such an approach would allow both countries to position themselves as providers of digital public goods that complement existing development efforts in South Asia.

Introduction

Digital infrastructure and technologies are the backbone of modern societies, powering economic growth and governance and offering tremendous potential for the global South to leapfrog challenges to development.³ At the same time, they're also one of the most contested domains in the 21st century. Strategic control over telecommunications networks and submarine cables to cloud computing, digital platforms and data, confers economic advantage, geopolitical and normative influence⁴ through sway over technical standards, data governance and long-term dependence on digital ecosystems.

South Asia—comprising India, Pakistan, Nepal, Sri Lanka, Bangladesh, Bhutan, Afghanistan and the Maldives—sits at the centre of those developmental and geopolitical dynamics. Home to more than 2 billion people with a high percentage of youth, South Asia is one of the fastest growing regions in the world in terms of internet adoption. Governments in the region have ambitious digitalisation plans to enhance connectivity, upgrade industrial productivity and business efficiency, improve the delivery of public services and foster growth. However, despite rapid progress, digital development remains uneven. Persistent gaps in broadband connectivity, network infrastructure, capital investment,

institutional capacity and regulatory frameworks—and unequal access—continue to constrain the region's digital transformation.

Growing demand and structural gaps in the provision of digital infrastructure have created space for external actors to shape the region's digital landscape. China has emerged as one of the most significant providers of digital infrastructure and technologies in South Asia through a combination of commercial investment, state-backed financing and diplomatic engagement, particularly under the Digital Silk Road (DSR) initiative. Chinese companies now play important roles across the region's digital ecosystem, ranging from telecommunications networks and fibre-optic infrastructure to smartphones, data centres, cloud services, smart cities, digital payments and e-commerce. While those investments have expanded access to digital technologies and supported economic development, they've also generated concerns regarding technological dependence, cybersecurity, data governance and long-term strategic vulnerability.

These developments have important implications for regional geopolitics. As global competition over critical and emerging technologies intensifies, South Asian governments increasingly face the challenge of balancing developmental imperatives with concerns

over national security, digital sovereignty and overdependence. China's rising influence in South Asia is particularly significant for India, which has traditionally occupied a predominant position in the region. India not only has a central geographic location with deep historical and economic ties but, importantly from the perspective of partners like Australia, offers the region a democratic and resilient alternative to China's techno-authoritarian model.⁵

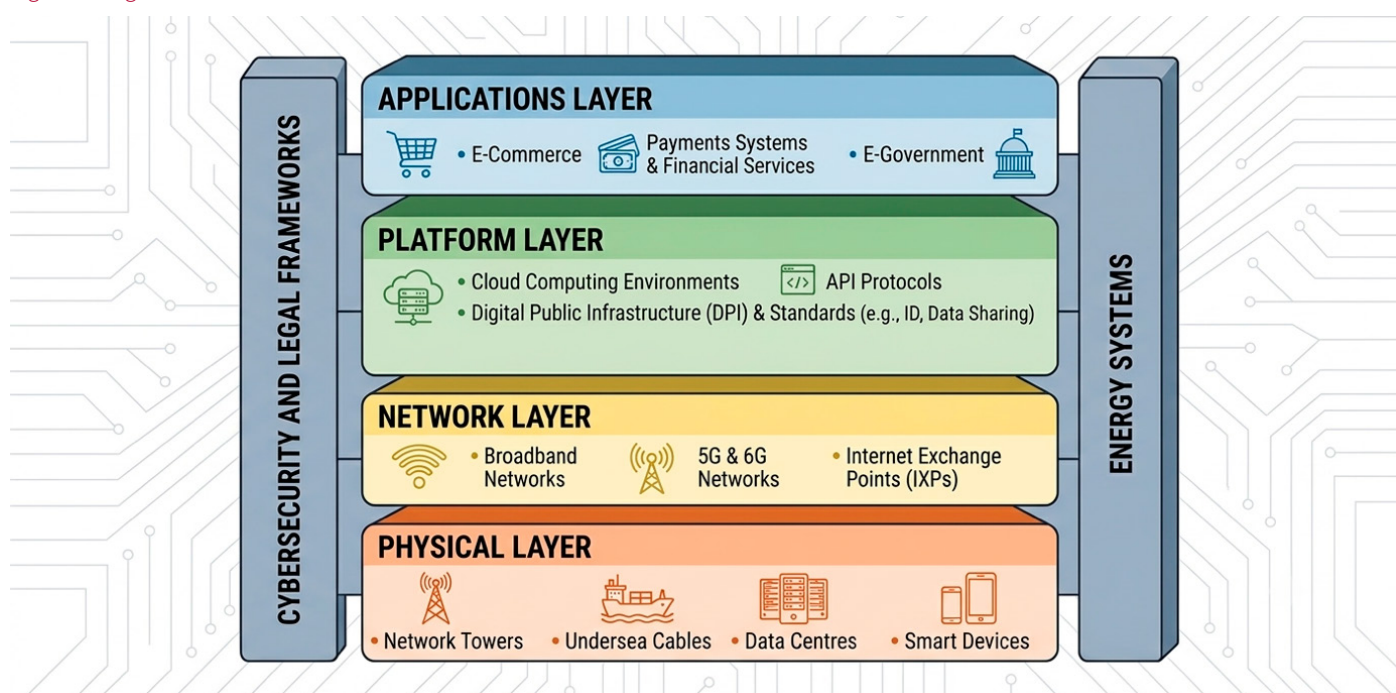
As a key player in the Indo-Pacific, Australia engages in South Asia on issues ranging from maritime security, economic development, climate and energy,⁶ particularly under its SARIC (South Asia Regional Infrastructure Connectivity) initiative. The regeneration of the Quad partnership from 2017 signalled alignment between Indian and Australian security interests in the region vis-à-vis China. The 2026 Australia–India Partnership on Cyber, Critical Technologies and Supply Chains (PACTS) framework⁷ elevated

the bilateral ambition, but there remains a lack of discussion and action on how the two countries might collaborate to support regional digital transformation.

In this context, this report outlines how India and Australia can leverage their complementary strengths and existing joint initiatives for the short- and long-term development of secure and resilient digital infrastructure in South Asia. It initially sets out the strategic importance of digital infrastructure and the state of development in South Asia. On those foundations, the report draws on official policy documents, public reporting and analysis, development finance records and company announcements to map China's role across different layers of the digital ecosystem and identify the challenges arising from that growing presence. The final section assesses the potential for India–Australia cooperation to strengthen the bilateral relationship and the region's digital resilience.

The geopolitics of digital infrastructure

Figure 1: Digital infrastructure architecture



Source: Author's compilation.

Infrastructure, such as roads, bridges, energy grids and telecommunications networks, has long been understood as foundational to modern societies, enabling the flow of goods, people and ideas across space and undergirding economic and political life.⁸ Digital infrastructure extends that into the information age, encompassing the physical assets, systems and frameworks that sustain digital activity.

At its most tangible, digital infrastructure includes hardware such as network towers, undersea cables, data centres and smart devices, including mobile phones, and security and surveillance systems (Figure 1). Layered above those physical assets are

the network systems (broadband, 5G and 6G networks and internet exchange points), that enable connectivity. Above those sit platform-level systems: cloud computing environments, protocols and standards, as well as digital public infrastructure (DPI). Rapid advancements in information and communications technologies have also produced hybrid forms, in which physical infrastructure is merged with digital management systems, as in intelligent water management, smart electricity grids and smart cities. Commercial and other digital services such as e-commerce, payments systems, financial services and e-government are built on top of those foundational systems. Cutting across all these

layers are cybersecurity and legal compliance frameworks and the energy systems that power them.

Digital infrastructure is seen as having profound ‘public good’ characteristics⁹ and significant political ramifications, including international influence.¹⁰ First, digital infrastructure promotes economic development, with positive effects on efficiency and productivity for firms, the creation of newer avenues for entrepreneurship and other multiplier effects.¹¹ It boosts accessibility to services, such as health care and education, in rural and underserved areas, thereby improving quality of life.¹² A World Bank study concluded that countries with elements of digital public infrastructure in place were able to mount responses more quickly, transparently and effectively to the Covid-19 pandemic.¹³ The digital economy makes up an increasing share of GDP, amounting to 15% of global GDP in 2024.

However, the importance of digital infrastructure traverses into the arena of global geopolitical and geo-economic competition. Historically, control of global communications infrastructure has resulted in major advantages in the battle for neutral hearts

and minds, including through the use of information warfare by the Allied powers during World War II¹⁴ and the US’s exercise of soft power after the war. Control over global undersea cable networks, which carry over 90% of all civilian and military digital data, telephonic and communication data, internet, social media and financial data, has been cited as a building block of American hegemony¹⁵ over the past several decades.

In 2015, China announced its ‘Made in China 2025’ plan (with the objective of upgrading its industry, achieving self-sufficiency and taking over the US’s dominance in advanced technologies¹⁶) and formally launched its DSR initiative. Both initiatives have become core aspects of China’s foreign policy, with an expansive geographical scope extending beyond the Belt and Road Initiative (BRI) and a technological remit from building 5G network infrastructure and fintech to AI and quantum computing. The strategy is seen as an attempt to ‘rewire’ global digital architecture.¹⁷ This intensification of strategic competition has resulted in export controls by the US on Chinese companies such as Huawei,¹⁸ while China has leveraged its control over supply chains of rare earths and minerals essential for high-tech industries.

The state of digital infrastructure in South Asia

In South Asia, alongside this context of global geopolitical contestations and polarisation, there are three factors mediating the expansion of digital infrastructure.

First, while digital infrastructure is recognised as an enabler of economic growth and social development, accessibility to digital services remains low due to lack of adequate investment in internet infrastructure.

Second, digital sovereignty (that is, control over data flows and software, standards and protocols and hard infrastructure) is a persistent concern. The influence of multinational corporations and foreign governments at the architectural level of the digital ecosystem gives rise to economic domination, strategic dependency and even narrative manipulation.¹⁹ Furthermore, once adopted, digital infrastructure creates a long-term lock-in effect or path dependence by embedding specific technologies, platforms, standards and data structures and making systems reliant on controlled software updates and hardware repairs.

Third, in addition to issues of accessibility and sovereignty, there’s the challenge of infringement of citizens’ privacy and human rights using imported digital surveillance technology, that at the same time is important for crime control and public safety in densely populated cities.

Those three issues of economic growth, national security and citizens’ rights are often in contest with each other. For instance, increasing accessibility of digital services in underserved areas needs economical and low-cost options and investments, and those domestic considerations might affect adoption decisions

by local officials more than geopolitical and security concerns in choosing vendors.

There are significant divergences in the scale and accessibility of digital infrastructure between South Asian states (Table 1). Most countries in the region have seen a remarkable growth in mobile internet usage and 4G network coverage over the past decade—a key indicator of digital growth. Data from the World Bank and the International Telecommunication Union (ITU) shows that, with the exception of Afghanistan, all countries in the region have almost 80% population coverage of 4G/LTE. Household access to internet ranges between 28% in Afghanistan to over 90% in Bhutan and the Maldives.²⁰ However, the use of fixed-line broadband networks, which provide higher quality internet access, remains abysmally low at under 10% subscription rate in all countries but the Maldives. In comparison, China has 47.2 subscriptions per 100 people.²¹

Table 1: Internet access indicators in South Asia

Country	Mobile cellular subscriptions (per 100 persons)	Broadband fixed line subscriptions (per 100 persons)
India	79.4	3.15
Sri Lanka	132.5	8.47
Bangladesh	108.1	8.09
Bhutan	99.8	2.92
Pakistan	76.9	1.47
Maldives	148.1	19.65
Afghanistan	60.1	0.08
Nepal	99.8	10.07

Source: World Bank data.

There are both upstream and downstream factors affecting internet usage. Upstream gaps include exorbitant costs of international internet bandwidth via submarine cables (first-mile), particularly for landlocked countries. Middle-mile infrastructure (that is, national fibre-optic and microwave networks) is expanding in all countries, but last-mile connectivity remains a challenge, especially in rural areas. Government programs like BharatNet²² (India), Info-Sarker²³ (Bangladesh), Communication to the Village²⁴ (Sri Lanka), Fibre-to-the-Home (Nepal) aim to reduce broadband coverage gaps and improve access to digital services via private and community connections.

Most of the governments in the region have national programs that centre digital transformations. Key focus areas include the expansion of physical infrastructure such as network towers

and optical fibre cable networks, data centres and smart cities, e-government and online public service delivery via digital public infrastructure (digital identity, payments, cloud etc.) and creating economic opportunities by skilling. There's an increasing focus on improving cybersecurity and data governance via specialised institutions and legal provisions. However, across the region the adoption of digital technologies and the associated risks, such as data and privacy breaches, have outpaced governance measures. Other challenges include insufficient interoperability, limited digital literacy and skills, unaffordability, lack of content in vernacular languages and lack of foundational infrastructure such as electricity and power. Table 3 (in the Appendix) provides a snapshot of the key policy priorities and government initiatives in the region.

China's digital engagements in South Asia

China has become an important provider of digital infrastructure in South Asia in the context of rapidly expanding demand, especially post-Covid. Several factors make China an attractive partner: its active diplomatic and commercial outreach, alignment with local priorities, availability of financing, the narrative of China's domestic growth and rapid digitalisation, promises of data sovereignty and participation in China-led multilateral institutions. From being largely reliant on Western-built ICT ecosystems until the 1990s, China has seen a tremendous growth in its domestic digital technology industry over the past three decades, becoming a leader in the sector and a major provider of good-quality but low-cost products across the world. That includes a mix of state-owned or backed enterprises such as China Mobile, ZTE and Hikvision, as well as big private tech companies, often with close links to the party-state, such as Huawei, Alibaba, Tencent and Baidu. Simultaneously with the expansion of internet usage and digital tech, China has also contended with cyberspace governance, arguing for cyber sovereignty (that is, greater state control over the internet) via the Great Firewall and laws and regulations on sharing user data.

The Digital Silk Road

The DSR, apart from creating opportunities for the Chinese giants to 'go out' of China, is part of Xi Jinping's broader strategic ambitions for China: national rejuvenation and preservation of the rule of the Chinese Communist Party (CCP), leadership of the developing world and outcompeting the US in digital technologies and their global governance.²⁵ Chinese narratives frame this in terms of economic cooperation and social modernisation in developing countries.

The DSR is broad in scope and combines physical infrastructure with over-the-top (OTT) services and even rules and standards. Table 2 presents the four pillars of the DSR. While Chinese ICT companies were active internationally from the 2000s, the DSR

provided a major policy incentive to 'go out'. Accordingly, research finds that, while physical infrastructure projects are rolled out by state-owned enterprises, private-sector companies dominate services and platforms. However, unlike the BRI, for which a large portion of finance comes from the government, in the DSR less than 10% of projects reported state funding until 2021.²⁶ That funding was generally directed towards physical projects like 'safe cities' and telecommunication networks. This affects the level of control that the Chinese government can potentially exercise over those projects. However, the 2020 crackdown on the tech sector, highlighted by the disappearance of Jack Ma, founder of Alibaba and Ant Group, shows the flux in the relationship between the state and the private sector in China.

Table 2: Pillars of the Digital Silk Road initiative

Hard infrastructure - Submarine optical cables and undersea datalinks 4G and 5G base stations - Satellite navigation systems	Platform trade - Cross border e-commerce - Digital payments systems - Alternative financial cycles to US\$
Cloud systems - Cloud services - Smart cities and the internet of things (IoT) - E-governance	Governance and standards - Chinese standards in emerging fields - Deep embedding and long-term binding - Multilateral governance institutions

While there are debates over the extent of state control and centralised planning²⁷ in China's digital outreach, several developments point to its strategic nature. The 13th Five-Year Plan (2016–20) had designated data as a 'basic strategic resource'.²⁸ In 2024, the CCP Central Committee and the State Council released the 'Opinions on the Reform and Innovative Development of Digital Trade' (hereafter 'Opinions'). The Opinions called for active government support for the development of foreign trade in

communication, internet of things (IoT), cloud computing, AI, blockchain and satellite navigation, and the development of cross-border e-commerce and integration of e-commerce with the industrial belt. It also asserted adherence to and strengthening of the CCP's comprehensive leadership of digital trade²⁹. Previously, laws such as the National Security Law, the National Intelligence Law, the Cyber Security Law and the Counter Espionage Law had been cited by critics as granting the Chinese state backdoor access to network and other data from tech companies such as Huawei.³⁰

Setting international standards, governance and legal frameworks is also a key focus area in the Opinions. On this front, China has set up institutional mechanisms including the Cross-border e-commerce standard framework (2018), the Global Cross-Border Data Flow Cooperation Initiative³¹ (2024) and the World Data Organization³² (2026), which reflect its domestic approach to data: maximising state access and restricting outbound flows. Possessing immense organisational capacity, Beijing also regularly vies for hosting major standards discussions, which allows for agenda setting and local participation.³³ Finally, norms and standards are not only propagated through workshops and conferences organised for officials from global South countries, but also by bundling them with Chinese-built infrastructure.³⁴

Mapping China's footprint

In South Asia, China's presence varies greatly across countries. Six of the eight countries in the region are part of the BRI and have extensive economic relations with China. Pakistan is one of China's closest strategic partners and home to massive infrastructure and energy projects being built under the China–Pakistan Economic Corridor. India–China diplomatic relations, on the other hand, are only just beginning to thaw after the 2020 border clashes in Galwan. Smaller states in the region such as Bangladesh, Sri Lanka, Nepal and the Maldives often have to balance between India, the dominant economic and military player in the region and China, which has become a major source of capital, technology and even defence equipment. China's digital engagement is thus often mediated by those political and diplomatic factors as much as economic factors like market size, profitability, ease of doing business and so on.

Apart from government-to-government memorandums of understanding, there also exist a range of long-term partnership agreements between companies, for instance between Huawei and Sri Lanka Telecom, or ZTE and BTCL. Furthermore, Chinese-built digital technologies also come bundled as 'smart' features in traditional infrastructure such as ports and business centres. Alongside bilateral agreements, there exist various other regional level institutional mechanisms to promote digital trade. In 2024, the digital and green economies were identified as the key sectors for China – South Asia economic and trade cooperation at the 8th China – South Asia Expo.³⁵ The provincial government of Yunnan has organised multiple editions of the 'South and South-East Asia Digital Cooperation Conference',³⁶ with participation from industry and government stakeholders. Yunnan is also strategically positioning itself as a regional hub with the Digital South and

Southeast Asia Project of the Yunnan Mobile company, comprising international land-based cable routes, computing centres and data exchange platforms.³⁷

Mobile devices

China's digital presence in the region exists at the most basic and consumer-facing level in the form of mobile phones, computers and other smart devices. Brands such as Xiaomi, Oppo, Vivo, Transsion, Huawei and HONOR occupy a majority share of the market in each of the South Asian countries, which some analysts assess as 'winning people's hearts and minds'.³⁸ This is particularly noteworthy in the case of India, where Chinese companies have been able to sustain their market dominance in the face of increased scrutiny and regulatory control amid bilateral geopolitical tensions. This has been attributed to their competitive pricing and localised marketing strategies. However, dependence on Chinese mobile phone brands comes with potential dangers for data privacy,³⁹ software and hardware repairs lock-in, supply-chain vulnerabilities and trade imbalance. Challenged with domestic measures to reduce import dependence by governments in India, Bangladesh and Pakistan, several companies such as Transsion, Vivo and HONOR have invested in setting up local manufacturing facilities or outsourcing to local manufacturers. However, those facilities more often focus on lower value final assembly; they're still reliant on imports from China for crucial components and core manufacturing.⁴⁰

Network infrastructure

Chinese companies are not only market leaders in mobile phone sales, but also in building the network infrastructure forming the backbone of all IT and communications sectors across the region. Huawei, the global telecommunications company that's been under fire from the US and other Western nations for allegations of espionage and intellectual property theft,⁴¹ as well as its close linkages to the CCP, is the dominant provider of 2G/3G/4G network equipment, alongside another Chinese semi-state-owned enterprise, ZTE. Both companies are also involved in 5G rollouts in Pakistan, Nepal, Bangladesh, the Maldives and Sri Lanka, in cooperation with public and private telecom companies, often forming a duopoly. For instance, in the Maldives, Dhiraagu and Ooredoo, which are the two largest operators, both rely on Huawei for equipment. Similarly in Sri Lanka, the top two operators (Dialog Axiata and SLT Mobitel) have ZTE and Huawei as their main technology partners. Chinese network infrastructure is most deeply embedded in Pakistan, providing not just hardware and technical standards but also telecom services to consumers. Zong, a subsidiary of China Mobile, is the country's second-largest operator, with 50 million subscribers and a 26% market share. In India, Huawei was the biggest supplier for 3G and 4G network equipment, in many ways enabling India's digital revolution.⁴² However, Chinese vendors were effectively excluded from the 5G rollout via tighter screening processes and 'trusted sources' requirements⁴³ in the aftermath of the border skirmishes in Galwan in 2020.

Huawei and ZTE are also involved in laying fibre-optic networks for broadband and cross-border connectivity under major projects funded by the Export-Import Bank of China (China Eximbank) (Figure 2). Examples include the ZTE-BTCL Nationwide Optical Fibre Transmission Network in Bangladesh and the Gyirong (China) to Rasuwagadi (Nepal) cross-border fibre-optic link that connected Nepal to the Chinese network. Alongside terrestrial cables, companies such as HMN Tech (formerly Huawei Marine Network) and Hengtong Group have made inroads in laying submarine cables in geopolitically critical zones. Those include the Maldives – Sri Lanka Cable (2021), which is the Maldives' primary international cable, and the 1,200-kilometre Ooredoo National Submarine Cable that connects the six major islands of the Maldives. The PEACE cable, which extends from Singapore to France via Africa, landing in Pakistan and the Maldives,⁴⁴ is the first privately owned submarine cable system from China.⁴⁵

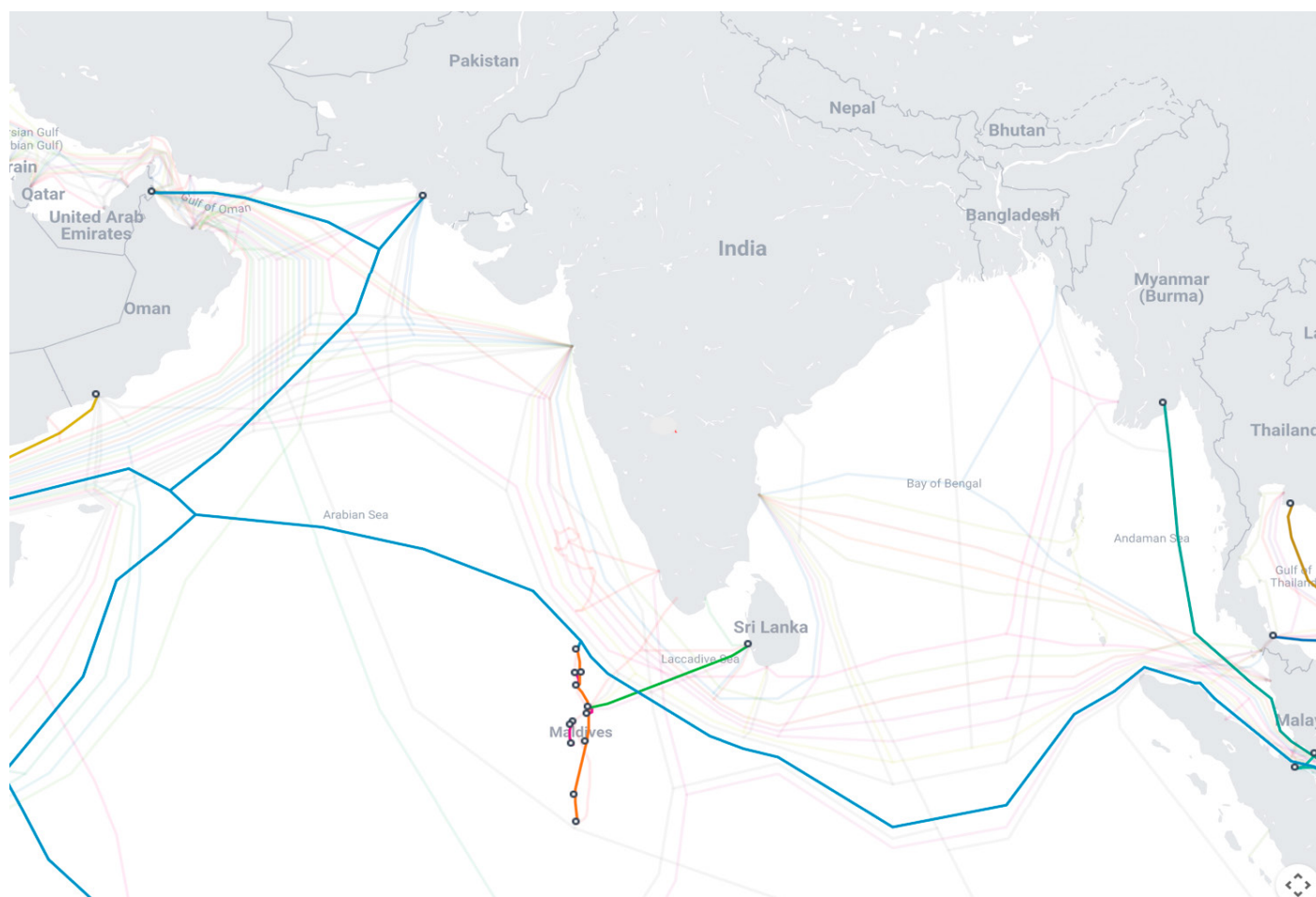
Smart cities and surveillance technology

A third important category of Chinese presence is in the form of smart city development. Smart cities are in a way an amalgamation of all digital infrastructure, ranging from back-end networks to consumer-facing devices, apps, platforms and cloud services. It involves the collection and sharing of disaggregated granular

data using embedded sensors, metering devices, surveillance cameras and other monitoring technologies for better management of public spaces and services.⁴⁶ Security analysts argue that Chinese smart city initiatives are instruments not only for exporting technologies and standards but also for disseminating non-democratic governance practices via mass surveillance. Apart from the invasion of individual privacy, the collection and synthesis of massive amounts of real-world, real-time data can be used to threaten national security and critical infrastructure⁴⁷.

In South Asia, where concerns such as traffic management and violent crime often overshadow privacy concerns, the market for surveillance systems such as closed-circuit television (CCTV) cameras has been growing rapidly and dominated by Chinese companies such as Hikvision and Dahua Technologies. Hikvision is a subsidiary of state-owned defence electronics conglomerate China Electronics Technology Group. Dahua is the second-largest video surveillance company globally after Hikvision. Both are facing sanctions and restrictions in many parts of the world due to allegations of the use of their equipment in China's Xinjiang region, their work with the People's Liberation Army and other national security concerns, such as backdoor access through installations in government facilities.⁴⁸

Figure 2: Chinese-built submarine cables in South Asia: PEACE cable (blue), Ooredoo National Submarine Cable (orange), Maldives – Sri Lanka Cable (green), Maldives' domestic cable (magenta).



Source: Submarine cable map, online.

However, these firms continue to be popular in the region both in commercial purchases as well as in government procurement for ‘safe city’ projects, particularly as they come with financing options. For instance, in 2015, China Eximbank provided RMB850 million in concessional loans for the Safe City Islamabad Project, which was implemented by Huawei Technologies and Beijing E-Hualu IT Co. Ltd.⁴⁹ The project involved the installation of 1,950 surveillance cameras, a facial-recognition system and software, communication devices and a command centre to monitor important buildings, commercial centres and residential areas and respond in real time. Subsequently, similar safe city projects have been implemented in major cities such as Lahore, Karachi, Gwadar and Peshawar in Pakistan by provincial governments in partnership with Huawei and other Chinese vendors. In Nepal, another US-sanctioned firm, Uniview,⁵⁰ provides surveillance equipment to Kathmandu police, not just for tourist and residential areas but also for security sensitive areas such as government buildings, Parliament House and the Prime Minister’s residence and office.⁵¹ In India, Hikvision and Dahua held up to one-third of the market before their internet-connected CCTV cameras were refused certification under the quality and standardisation certification rules in April 2026.⁵²

Smart city initiatives aren’t restricted to upgrading existing infrastructure; they’re also developing newer ones. The Colombo Port City is an example. Financed by the China Development Bank and implemented by China Harbour Engineering Co. Ltd (a subsidiary of China Communications Construction, which had been blacklisted by the World Bank until 2017 on allegations of corruption⁵³), this US\$1.4 billion project involves land reclamation and the development of a smart financial hub with modern facilities.⁵⁴ Huawei and Sri Lanka Telecom have partnered to provide smart city solutions built around IoT and AI.⁵⁵ In the neighbouring island state of the Maldives, Chinese infrastructure and telecommunications companies such as China Machinery Engineering Corporation (CMEC) and Huawei have been involved in building housing, smart electric grids, fibre-optic networks and roads for the Hulhumale smart city.⁵⁶ Finally, with the rapid advancement of AI and greater emphasis on data localisation and data sovereignty, countries across the South Asian region are expanding their data centres and cloud facilities. ZTE built the Tier IV National Data Centre in Gazipur, Bangladesh, in 2019,⁵⁷ while Huawei is involved in building multiple data centres in Pakistan, including the country’s largest Tier III data centre.⁵⁸

E-governance, education, fintech and e-commerce

Contrary to common perceptions of the BRI and DSR as being focused on large-scale physical infrastructure, over the past decade China’s footprint in ‘soft’ sectors such as e-governance, education and training, e-commerce and fintech have also rapidly expanded in the region, giving access to large amounts of consumer data to Chinese actors. With Chinese-built infrastructure already forming the backbone of digital services in Pakistan, recent reports show that under CPEC 2.0 the strategic focus is moving further towards digital governance tools, AI and cloud computing.⁵⁹

China Eximbank, Huawei Technologies, CMEC and China Railway International Group are the key actors involved in developing Bangladesh’s national ICT infrastructure network: Info-Sarker Phase II and III. This project has connected all government offices, from central ministries to rural administrative centres and police stations with fibre-optic networks and has the provision of e-services in rural areas, skills enhancement and ICT training as its objectives.⁶⁰ Apart from its flagship ‘Seeds for the Future’ program, which provides training in AI, cloud computing, 5G etc., Huawei is also involved in various ICT skilling and ‘smart classroom’ initiatives in South Asia, for instance in remote areas in Nepal.⁶¹ In Sri Lanka, under a G2G grant framework, China is providing aid for education digitisation involving smart classrooms, centralised education cloud data centres and the sharing of best practices from China’s experience.⁶²

Alibaba’s 2018 acquisition of Daraz, then South Asia’s largest e-commerce platform operating across Pakistan, Bangladesh, Sri Lanka and Nepal, gave it a strong foothold in the regional market.⁶³ In fintech, affiliate Ant Group has pursued a mix of equity investment and payment-network integration: it acquired a 20% stake in Bangladesh’s bKash and a 45% stake in Pakistan’s Telenor Microfinance Bank (operator of Easypaisa) in 2018, while more recently extending its Alipay+ cross-border infrastructure into the region through interoperability arrangements with platforms such as NayaPay (Pakistan), LankaPay⁶⁴ (Sri Lanka), FonePay (Nepal) and the Bank of Maldives.⁶⁵ ANT was also one of the early investors in India’s Paytm mobile payments system. Huawei and Banglalink have tied up to develop a new digital payments platform, MuktoPay in Bangladesh.⁶⁶

Emerging risks and challenges

While Chinese investments and technology have been critical in enabling telecommunications development and added to economic growth in the region, they come associated with several immediate risks and could create long-term vulnerabilities that need urgent attention.

First, China’s expanding role across South Asia’s digital ecosystem raises concerns regarding technological dependency, market concentration and digital sovereignty. Chinese firms are increasingly present across multiple layers of the digital economy, including telecommunications networks, data centres, cloud services, surveillance systems, digital payments, e-commerce platforms and emerging AI cooperation. This creates the risk of vendor lock-in, whereby governments become dependent on a limited number of suppliers for upgrades, maintenance and future expansion.⁶⁷ Such dependence may reduce policy autonomy and complicate efforts to diversify suppliers or establish independent technological standards. Concerns have also emerged regarding data sovereignty, particularly where Chinese firms seek involvement in both core telecommunications infrastructure and associated digital services. Nepal’s Supreme Court, for example, ordered the cancellation of a tender awarded to Huawei in 2024, arguing that the vendors supplying telecommunications billing systems

shouldn't simultaneously control core network infrastructure, citing risks to personal data protection and information security.⁶⁸

Second, several Chinese-backed digital infrastructure projects have faced governance, transparency and accountability challenges. Furthermore, as in other BRI projects, debt repayment has proven to be a major challenge for borrowing countries, resulting in public criticism.⁶⁹ A widely publicised case is that of Hambantota Port. Critics questioned China's motivations in approving massive loans (amounting to \$1.4 billion) for a project that had failed feasibility studies and was rejected by other lenders. The project, which was marred by charges of corrupt practices and construction delays, remained highly unprofitable in its first decade, and the accrued debt exacerbated Sri Lanka's economic crisis. In 2017, the strategically located port was leased out to a Chinese state-owned enterprise for 99 years in exchange for \$1.12 billion, raising alarms about 'debt-trap diplomacy'.⁷⁰ The project highlighted both the lack of sustainable and transparent lending practices by Chinese firms as well as weak regulatory and enforcement capacity on part of recipient states.

Sri Lanka's Lotus Tower project, financed and constructed by Chinese entities, became mired in controversy following allegations that millions of dollars transferred to a Chinese contractor had disappeared, triggering parliamentary investigations and public scrutiny.⁷¹ Beyond financial concerns, the Lotus Tower project highlighted broader issues surrounding opaque procurement processes and limited public oversight of strategically significant digital infrastructure. While it was initially planned as an IT and telecommunications hub, critics claim that it's merely a leisure centre and events venue.⁷² A similar situation is unfolding in the Colombo Port Smart City, which has faced several delays and failed to attract foreign investment. Research also shows how exceptional legal frameworks have been created by the political elite in order to broker those projects.⁷³ In Bangladesh, Huawei's involvement in a major 5G modernisation project attracted charges of procurement irregularities even from another Chinese firm, ZTE.⁷⁴ In another example of technology moving faster than regulation, WeChatPay

was banned in 2019 in Nepal, as Chinese business operators were found using the payments app to repatriate earnings to China, thereby evading local tax systems.⁷⁵ Those cases don't necessarily imply systemic wrongdoing, but they underscore the difficulties many South Asian governments face in ensuring transparency, competitive tendering and effective regulatory oversight in large-scale technology projects.

Third, China's digital footprint has generated growing concerns regarding democratic governance, civil liberties and geopolitical influence. Chinese companies have supplied surveillance systems, facial-recognition technologies and smart-city platforms across South Asia, often as part of broader public security and urban management initiatives.⁷⁶ Such technologies may facilitate governance practices that prioritise state control and monitoring over privacy and individual freedoms.⁷⁷ In Nepal, human rights organisations and Tibetan advocacy groups have alleged that surveillance infrastructure has been used to monitor Tibetan refugee communities and politically sensitive activities, raising concerns regarding transnational repression and the protection of democratic freedoms.⁷⁸ At the same time, strategically significant projects such as Pakistan's safe-city projects and Sri Lanka's Lotus Tower have fuelled debate over the potential dual-use nature of digital infrastructure for both civilian and security purposes. Although evidence of direct misuse remains contested, these cases illustrate how digital infrastructure has become deeply intertwined with questions of national security, political influence and the future governance of information. As a result, South Asian states increasingly face the challenge of balancing developmental benefits with commitments to democratic values, privacy protections and strategic autonomy.

These risks don't mean that South Asian states should reject Chinese digital infrastructure outright. Rather, they point to the need for stronger governance, procurement transparency, cybersecurity safeguards and a wider set of credible alternatives. This is where Australia and India should increase cooperation.

Advancing India–Australia synergy for digital transformation

Three structural limitations have constrained deeper Australia–India cooperation in South Asia's digital sector.

First, neither country offers a vertically integrated digital ecosystem that spans telecommunications hardware, cloud services, digital platforms, financing and implementation capacity. Australia has limited telecommunications manufacturing capacity, while India's strengths lie primarily in DPI, software and digital services rather than advanced hardware. Moreover, previous regionalisation efforts in South Asia have been marred by India–Pakistan rivalry and delayed project implementation, as well as concerns among smaller states about India's dominant position.⁷⁹

Second, India and Australia have had different policy priorities in the digital sector. India's approach, as a developing country, is primarily driven by regional connectivity, digital sovereignty, cost-effectiveness and inclusive development. Australia, by contrast, places greater emphasis on trusted technology, cybersecurity, democratic digital governance and maintaining an open and rules-based Indo-Pacific.

Finally, much of the India–Australia bilateral digital agenda has focused on high-profile public diplomacy efforts and partnership announcements. Translating those commitments into tangible outcomes will require greater operationalisation through

dedicated funding, focused implementation mechanisms and sustained engagement with research communities, industry and regional governments.

Those limitations, however, don't diminish the rationale for cooperation. Rather, they reinforce the need for a pragmatic partnership that builds on complementary strengths, focuses on achievable areas of collaboration and implementation, and is sensitive to the developmental needs of regional partners.

For India, its immediate neighbourhood is the mainstay of its strategic and foreign policy objectives. While India remains the predominant power in the region, due to its geographical and economic position, as well as its historical and cultural ties, China's rapidly expanding presence has raised concerns about encirclement. It has spurred policy initiatives to promote regional connectivity, develop infrastructure, de-risk supply chains and enhance regional resilience. India's ongoing digital transformation, headlined by its indigenously developed DPI stack, has been generally hailed as a success⁸⁰ and a potential model for other global South countries seeking to digitise with limited resources. Building on that experience, India is actively pursuing tech diplomacy and digital cooperation, including in emerging and frontier sectors, with the ambition to leverage its normative, demographic and market power to influence a more open and democratic tech order.⁸¹ Cooperating with like-minded partners such as Australia, India can alleviate resource constraints and augment technical capacity while enabling wider partnerships, scaling and timely implementation of initiatives.

For Australia, the South Asian region offers a large and rapidly digitising market that's largely commercially untapped by Australia's burgeoning tech start-ups. Beyond commercial interests, deeper engagement is underpinned by Australia's broader objective of supporting a stable, open and rules-based Indo-Pacific. As countries across South Asia build telecommunications networks, submarine cables, cloud infrastructure, digital payment systems and digital governance frameworks, decisions made today will shape patterns of data governance, technological dependence and digital connectivity for decades. The region has therefore become an important arena in which technical standards, interoperability, cybersecurity practices and digital governance norms are being contested. Furthermore, understanding China's tools and strategies in South Asia is instructive for Australia's own neighbourhood as well. Supporting trusted digital infrastructure and open standards in South Asia aligns closely with Australia's strategic interest in promoting transparency, resilience and democratic governance while reducing the risks associated with concentrated technological dependencies.

India and Australia are well positioned to bolster digital transformation across South Asia by leveraging their complementary strengths. IT and technology is a priority sector in the New Roadmap for Australia's Economic Engagement with India. PACTS (2026) is aimed at deepening institutional linkages, fostering policy exchange and supporting collaboration in these

sectors.⁸² Other existing initiatives include the Australia–India Innovation Network, which is aimed at increasing access of Australian tech companies to India's digital sector, and the Strategic and Technology Policy Initiative, which has the objective of creating greater understanding and joint action for a peaceful, prosperous and stable region. These efforts and tangible commitments attest to the political will underpinning Australia–India ties. Both countries must build upon existing bilateral mechanisms, including PACTS, the Australia–India Economic Cooperation and Trade Agreement and Australia's SARIC initiative, to develop a coordinated approach that promotes regional digital development, resilience and economic integration.

Conclusion

Digital infrastructure is a foundational component of economic development, governance and geopolitical influence in the 21st century. Across South Asia, governments are investing heavily in telecommunications networks, data centres, digital public infrastructure, smart cities and digital services to accelerate economic growth and improve public service delivery. Yet persistent deficits in connectivity infrastructure, institutional capacity and regulatory frameworks continue to constrain those ambitions. In this context, China has been able to use its economic and technological leverage to become an influential strategic actor in the region. Chinese firms have a notable and sometimes dominant presence across every layer of the digital ecosystem—from mobile devices and telecommunications networks to cloud infrastructure, surveillance technologies, e-commerce, fintech and e-governance platforms. Those investments have expanded digital connectivity and contributed to technological modernisation. However, the investments aren't merely economic or altruistic decisions and have created risks such as technological dependence, data governance irregularities, lack of transparency and threats to strategic autonomy. While the dependency risks and security implications are widely known, a common feature is an absence of viable alternatives. This is where Australia and India have a vital role.

From India's perspective, China's expanding footprint has reinforced the importance of strengthening regional connectivity and digital resilience through partnerships with like-minded countries such as Australia. The dilemma of balancing rapid digital transformation with security requires a nuanced response that

gives primacy to agency and policy priorities of the smaller states in the region. Australia and India share an interest in promoting secure digital ecosystems, trusted technology and an open Indo-Pacific. The strength of the Australia–India partnership lies in shared values, deep economic and diplomatic ties and complementary capabilities. India's experience in deploying cost-effective DPI at scale, together with Australia's expertise in e-governance, cybersecurity, infrastructure financing and aid facilitation, offers a practical foundation for supporting inclusive and sustainable digital development across South Asia.

The recommendations advanced in this paper aren't about an unrealistic regional decoupling from Chinese technology. Rather, the recommendations seek to ensure that Australia and India strengthen their cooperation and leadership in the region to both ensure that partner states have an increased awareness of the risks and have access to viable alternatives that prioritise the sovereignty of those individual nations and resilience of the entire region. This can be achieved by sharpening the toolkit and broadening the scope of existing frameworks of cooperation. Facilitating digital connectivity financing through SARIC, regionalising PACTS, supporting DPI, strengthening cybersecurity cooperation, investing in human capital, mobilising private-sector innovation and leveraging existing multilateral platforms represent practical avenues through which India and Australia can contribute to the region's digital future. Those initiatives would broaden the choices available to South Asian governments, strengthen institutional resilience and encourage greater interoperability, transparency and trust in regional digital ecosystems.

Appendix

Table 3: Digitalisation plans in South Asia*

Country	Flagship program	Key focus areas	Legal framework	Key actors
India	Digital India (July 2015) Smart Cities Mission (June 2015)	- Digital identity: Aadhaar - Digital payments and financial inclusion: UPI, BHIM, Jan Dhan - Broadband and connectivity: BharatNet - AI: IndiaAI Mission 2024–29; quantum computational lab, data centres - E- government services: DigiLocker (documents) UMANG app; GovDrive (Cloud), etc. - Smart cities: integrated command and control, e-health, e-waste management, surveillance via CCTV cameras	Digital Personal Data Protection Act, 2023 (DPDPA) + DPDP Rules, 2025 Information Technology Act, 2000 + IT (Amendment) Act, 2009 Digital India Act (proposed)	Ministry of Electronics & IT; Ministry of Housing and Urban Affairs; private-sector IT and telecom companies
Nepal	Digital Nepal Framework 2.0 IT Decade (2024–2034)	- Digital ID: Nagarik app - Digital payments, cross-border payments - E-government and DPI - Infrastructure (FAST): national data centres, cloud guidelines, cybersecurity; nationwide 4G and early 5G rollout; broadband expansion - AI: AI integration across health care, finance, agriculture, tourism, education and disaster management - Skills: coding and AI literacy in secondary schools; mandatory digital training for civil servants	Individual Privacy Act, 2018; Data Centre and Cloud Service (Operation and Management) Directives, 2025; E-commerce Act, 2025	Ministry of Communications & IT (MoCIT); Digital Transformation Council; World Bank; ADB; private sector
Bangladesh	Smart Bangladesh 2041 (2022–2041) Digital Bangladesh (2009–21)	- Four pillars: Smart Citizen, Smart Government, Smart Economy, Smart Society - Broadband connectivity and IT exports, smart cities - a2i: e-government services, e-health and e-education - AI: 2024 National AI Policy; National AI Centre of Excellence with ethical guidelines and data governance - Start-ups and workforce skilling		ICT Division; a2i Agency; private sector IT and Telecom companies
Pakistan	Digital Pakistan Policy 2018	- Broadband connectivity, land and submarine cables - ID: PDA to create centralised citizen digital identity consolidating health, assets and social data; coordinating with NADRA - AI: NCAI - IT exports - Tech zones: 40 special technology zones in secondary/tertiary cities - Skilling	Digital Nation Pakistan Act 2025; Personal Data Protection Bill (proposed)	Ministry of IT & Telecom; Pakistan Digital Authority National Digital Commission (NDC); private sector IT and telecom companies
Maldives	Maldives 2.0 National digital transformation initiative	- Digital identity and transactions: eFaas (since 2012) eFaas 3.0 planned for 2026 - Digital payments: Favara instant payment system (launched August 2023) - Data sharing and governance (Maldives Data Exchange Platform) - Cybersecurity: National Cybersecurity Operations Centre and National Cyber Incident Response Team - Secure and Sovereign Digital Infrastructure (Gov Cloud) - E-government services - Digital transformation in health, education and public finance - Skilling and start-up ecosystem - Connectivity through fibre-optic cable	Digital Identity Bill (drafted 2025) Cybersecurity Act (2025) Personal Data Protection Act (2026) Maldives Digital Services Act (2025) AI Act (planned)	Dhiraagu (telecom company), NCIT; Maldives Monetary Authority (MMA); private sector IT and telecom companies

*Afghanistan not included due to lack of complete and credible data.

Bhutan	Digital Drukylul Flagship Programme (2019) Digital Strategy: Intelligent Bhutan (2024)	- Digital identity: NDI launched 2023 on self-sovereign identity principles; migrated to Ethereum blockchain October 2025 - Infrastructure: Digital Drukylul (2019) connected 1,084+ government offices via fibre - Fintech & crypto: Crypto-tourism payments via Binance; QR-code and fintech payment systems in development - e-Government: centralised citizen services portal - Blockchain: NDI issues verifiable credentials (foundational IDs, residence permits, academic certificates) using decentralised identifiers	Information Communications and Media Act 2018 Data Management Guide 2023	GovTech Agency (est. 2022) (Department of Digital Infrastructure); private sector IT and telecom companies
Sri Lanka	Digital Sri Lanka 2030 Digital Economy Blueprint Implementation roadmap, 2025	- Digital identity: SLUDI (Sri Lanka Unique Digital Identity) - e-Government: PIC-Net (Public-Impact Champions Network); integrated citizen services portal; government cloud platform; cross-agency data sharing; digital document locker - Payments: GovPay digital payment system; CBDC - AI & skills: training in AI, robotics and financial technologies - Start-ups: Digital startup accelerator	Personal Data Protection Act 2022 Digital Economy Act (planned) Cyber Security Act (proposed)	Ministry of Digital Economy; Information Communication Technology Agency; Data Protection Authority; private sector IT and telecom companies

Notes

- Department of Foreign Affairs and Trade (DFAT), 'Quad', Australian Government, [online](#).
- G20 Research Group, 'India's G20 presidency: a synopsis', University of Toronto, 30 November 2023, [online](#).
- World Bank, 'South Asia's digital economy: an opportunity to build back better, digitally', 2022, [online](#).
- Dan Ciuriak, 'The digital revolution has transformed geopolitics', Centre for International Governance Innovation, 2023, [online](#).
- Constantino Xavier, Jabin T Jacob (eds), *How China engages South Asia: in the open and behind the scenes*, Centre for Social and Economic Progress, 2025; Alduri Subramanyam Raju (ed.), *South Asia and China: engagement in the twenty first century*, Routledge, 2022.
- DFAT, 'Australia–South Asia (Regional) Development Partnership Plan 2024–2029', Australian Government, [online](#).
- DFAT, 'Australia–India Partnership on Cyber, Critical Technologies and Supply Chains (PACTS)', Australian Government, [online](#).
- Brian Larkin, 'The politics and poetics of infrastructure', *Annual Review of Anthropology*, 2013, 42:327–43, [online](#).
- 'Urban infrastructure in political science and public administration', *Governing Infrastructure Interfaces Research Note 03*, London School of Economics, 2018, [online](#).
- Austin Strange, *Chinese global infrastructure*, Cambridge University Press, 2024, [online](#).
- World Bank, 'Digital connectivity and economic diversification', 7 February 2022, [online](#).
- Don J Webber, Ellen Hughes, Gail Pacheco, Glenn Parry, 'Investment in digital infrastructure: why and for whom?', *REGION*, 2022, 9(1):147–63, [online](#).
- Jonathan Marskell, Georgina Marin, Minita Varghese, 'Digital public infrastructure: transforming service delivery across sectors', in *Digital Progress and Trends Report 2023*, World Bank, [online](#).
- Richard Dunley, 'Under cable control: the information dimension', *The Interpreter*, 5 May 2025, [online](#).
- Romain Dufetie, 'The data roads under the seas: American hegemony over global undersea cable network and its potential challengers', master's thesis, University of Chicago, August 2023.
- Scott Kennedy, 'Made in China 2025', Center for Strategic and International Studies (CSIS), 1 June 2015, [online](#).
- David Gordon, Meia Nouwens (eds), *The Digital Silk Road: China's technological rise and the geopolitics of cyberspace*, International Institute for Strategic Studies / Adelphi, 2022, [online](#).
- Congressional Research Service, 'US restrictions on Huawei Technologies: national security, foreign policy, and economic interests', US Congress, 5 January 2022, [online](#).
- Erman Akilli, 'Digital asymmetry in the technopolar world', in *Cognitive diplomacy and digital autonomy*, Palgrave Macmillan, 2025, [online](#).
- International Telecommunication Union (ITU), 'Households with internet access at home', data query, [online](#).
- ITU, 'Broadband subscription per 100 people', data query, [online](#).
- Press Information Bureau, 'BharatNet', media release, Government of India, 21 April 2025, [online](#).
- 'Bangladesh brings 100m under high-speed internet', *The Financial Express*, 15 July 2026, [online](#).
- 'TRCSL accelerates 4G expansion through "communication to the village" project', SAMENA Telecommunications Council, 19 February 2026, [online](#).
- Damien Ma, 'The Digital Silk Road: China's grand strategic ambitions', in Gordon & Nouwens, *The Digital Silk Road: China's technological rise and the geopolitics of cyberspace*.
- Gordon & Nouwens, *The Digital Silk Road: China's technological rise and the geopolitics of cyberspace*.
- Wang Zheng, 'China's Digital Silk Road in Southeast Asia: progress and challenges', ISEAS Perspective 2024, No. 1, ISEAS – Yusof Ishak Institute, 5 January 2024, [online](#).
- Nigel Cory, 'The World Data Organization: China's expanding influence on global data', National Bureau of Asian Research, [online](#).
- 'Opinions of the General Office of the CPC Central Committee and the General Office of the State Council on the reform, innovation and development of digital trade' [中共中央办公厅国务院办公厅关于数字贸易改革创新发展的意见], *Renmin Wang*, 29 November 2024, [online](#).
- 'Huawei would have to give data to China government if asked: experts', *CNBC*, 5 March 2019, [online](#); 'China's national security laws: implications beyond borders', *CNA*, 2023, [online](#).
- 'Global Cross-Border Data Flow Cooperation Initiative released', *Science and Technology Daily*, 13 December 2024, [online](#).
- Wang Yunshan, 'World Data Organization established to bridge global data divide', *Qishi*, 9 April 2026, [online](#).
- Cory, 'The World Data Organization: China's expanding influence on global data'.
- Alex He, 'The Digital Silk Road and China's influence on standard setting', Centre for International Governance and Innovation, April 2022, [online](#).
- 'Ministry of Commerce: China and South Asia have a broad scope for cooperation in the field of digital and green economy' [商务部: 中国与

- 南亚国家在数字和绿色经济领域具有广阔合作空间], *Xinhua*, 9 July 2024, [online](#).
- 36 'Join hands to promote digital cooperation in South Asia and Southeast Asia and open up a new space for the development of digital industry in Yunnan' [携手推进南亚东南亚数字合作 云南开辟数字产业发展新空间], *Xinhua*, 3 May 2024, [online](#); 'Promote the construction of digital countries. The 2025 South Asia-Southeast Asia Digital Cooperation Conference and Industry and Trade Supply and Demand Docking Activity opens in Bangkok [促进区域数字合作 助力数字国家建设 2025 年南亚东南亚数字合作大会暨工贸供需对接活动在曼谷开幕]', *Xinhua* (Yunnan), 1 September 2025, [online](#).
- 37 'Yunnan Mobile: Build a large digital information channel and strive to be the pioneer of "digital two Asia"' [云南移动: 建设数字信息大通道 争做“数字两亚”先行者], *People's Daily*, 11 December 2025, [online](#).
- 38 Anand P Krishnan, 'Building influence by "rising step by step"? Chinese capital's permeation of India's electronics industry', Centre for Social and Economic Progress, 2025, [online](#); 'Chinese smartphones expand market dominance', *Xinhua* Silk Road Database, 22 January 2026, [online](#).
- 39 'Revealed: China suspected of spying on Americans via Caribbean phone networks', *The Guardian*, 15 December 2020, [online](#); 'China is everywhere: your iPhone, Android phone now at risk', *Forbes*, 17 April 2025, [online](#).
- 40 Karen Hui, 'Despite de-risking, China's role in global smartphone supply chains remains resilient', Asia Pacific Foundation of Canada, 14 March 2024, [online](#); 'Chinese mobile companies making more in India to dim regulatory glare', *Economic Times*, 4 June 2025, [online](#); 'Honor begins local production in Gazipur', *New Age*, 3 December 2025, [online](#); 'Chinese tech firm opens new factory in Bangladesh amid growing demand for smart devices', *Xinhua*, 26 May 2023, [online](#); 'Chinese company opens \$22m factory', *The Daily Star*, 25 May 2023, [online](#); 'Bangladesh's smartphone city gathers Chinese manufacturers', Belt and Road Studies Network, 20 July 2022, [online](#).
- 41 Noah Berman, Lindsay Maizland, Andrew Chatzky, 'Is China's Huawei a threat to US national security?', Council on Foreign Relations, 8 February 2023, [online](#).
- 42 Ananth Krishnan, 'Wedged between conflicting interests: India's Huawei dilemma', *Global Asia*, 14(3), [online](#).
- 43 'Govt unlikely to ease curbs on Chinese telecom gear', *Communications Today*, 29 August 2025, [online](#).
- 44 'PEACE', Submarine Cable Networks, [online](#).
- 45 'Hengtong bringing first carrier neutral open submarine cable system to Pakistan', PEACE Cable International Network, 19 April 2019, [online](#).
- 46 Katherine Atha, Jason Callahan, John Chen et al., *China's smart cities development*, US-China Economic and Security Review Commission, January 2020, [online](#).
- 47 Katherine Atha et al. 2020
- 48 'Where Dahua and Hikvision are banned', *IPVM*, 5 July 2024, [online](#).
- 49 'China Eximbank provides RMB 850 million government concessional loan for Safe City Islamabad Project', *AidData*, William and Mary College, [online](#).
- 50 US Federal Register, 'Additions to the Entity List', 11 December 2024, [online](#).
- 51 'Uniview guards Nepal's First City', *Uniview*, 6 December 2019, [online](#).
- 52 'Hikvision and Dahua almost barred from selling in India as government refuses to certify made-in-China CCTVs', *The Times of India*, 1 April 2026, [online](#).
- 53 'World Bank applies 2009 debarment to China Communications Construction Company Limited for fraud in Philippines roads project', World Bank, 29 July 2011, [online](#).
- 54 Wade Shepard, 'A look at Colombo Port City: the frontline of China and India's geopolitical showdown', *Forbes*, 12 August 2016, [online](#); 'China Development Bank provides \$805 million loan for Colombo Port City Project Phase 1', *AidData*, William & Mary College, [online](#).
- 55 'SLT-Huawei to partner for Colombo Port City's smart city project', *Daily Mirror*, 26 March 2019, [online](#).
- 56 'China's CMEC to develop Hulhumale Phase III', *Atoll Times*, 27 March 2024, [online](#); 'Belt and Road: Chinese techno-nationalism in Maldives', *Asia Times*, April 2024, [online](#); 'Chinese investment in the Maldives: appraising the string of pearls', Asia Maritime Transparency Initiative, CSIS, [online](#); 'Hulhumalé: The smart city', *Maldives Financial Review*, 15 December 2022, [online](#).
- 57 'Bangladesh has the world's 7th largest data centre. Here's how it can earn foreign currency', *The Daily Star*, 30 December 2021, [online](#).
- 58 Ismail Dilawar, 'Pakistani company signs agreement with Huawei for country's largest Tier III data center', *Arab News*, 6 June 2026, [online](#).
- 59 Abdul Hannan Mansoor, 'CPEC 2.0: China's grip tightening on Pakistan's digital future', *Asia Times*, 9 June 2026, [online](#); 'China-Pakistan ties: digital economy in focus as Pakistani PM Shehbaz Sharif attends investment conference in Hangzhou', *CGTN*, 25 May 2026, [online](#).
- 60 'National ICT infra-network for Bangladesh Government (Info-Sarker) project', ITU, project 1516263237, [online](#).
- 61 'Huawei sets up smart classroom in central Nepal village', Huawei, February 2025, [online](#).
- 62 'China-aid Digital Transformation Project of General Education in Sri Lanka holds groundbreaking ceremony', Embassy of the People's Republic of China in Sri Lanka, 19 January 2026, [online](#); 'China provides expert help and grant to digitalise Sri Lanka education', *Sunday Times*, 18 January 2026, [online](#).
- 63 'Alibaba buys Rocket Internet's Daraz', *TechCrunch*, 8 May 2018, [online](#).
- 64 'Alipay+ is now enabled in Sri Lanka', LankaPay, 26 March 2026, [online](#).
- 65 'Bank of Maldives, Alipay and Visit Maldives sign agreement to promote Maldives and strengthen Maldives' digital ecosystem', Bank of Maldives, 11 December 2025, [online](#).
- 66 'Banglalink, Huawei ink deal to develop digital payments platform Mukto Pay', *Prothom Alo*, 6 March 2026, [online](#).
- 67 Sanjana Hattotuwa, 'Are Chinese telecoms acting as the ears for the Sri Lankan government?', *Groundviews*, 16 February 2012, [online](#).
- 68 'NT's aborted billing system tender exposes systemic dysfunction', *Annapurna Express*, 27 January 2026, [online](#).
- 69 *AidData*, William & Mary College, projects 37016 and 33431, [online](#).
- 70 Michael Himmer, Zdenek Rod, 'Chinese debt trap diplomacy: reality or myth', *Journal of the Indian Ocean Region*, 2022, [online](#); Shahar Hameiri, 'Debunking the myth of China's "debt trap diplomacy"', *The Interpreter*, Lowy Institute, 9 September 2020, [online](#); Brahma Chellaney, 'China's debt trap diplomacy', *The Strategist*, 24 January 2017, [online](#); Ganeshan Wignaraja, Dinusha Panditaratne, Pabasara Kannangara, Divya Hundlani, 'Chinese investment and the BRI in Sri Lanka', Chatham House, March 2020, [online](#); Mark Green, 'China's debt diplomacy', *Foreign Policy*, 25 April 2019, [online](#).
- 71 Chulanee Attanayake, 'Lotus Tower: iconic building mired in controversy', Institute of South Asian Studies, National University of Singapore, 7 October 2019, [online](#).
- 72 Rathindra Kuruwita, 'Colombo Lotus Tower and the case for transparency', *The Diplomat*, 14 October 2022, [online](#).
- 73 Thiruni Kelegama, 'Engineering exception: infrastructure brokers and the Colombo Port City Project', *Geopolitics*, 16 October 2026, [online](#); Dilini Pathirana, 'Domestic legal impacts of Chinese funded infrastructure projects in Sri Lanka', Centre for Social and Economic Progress, July 2025, [online](#).
- 74 Mahmudul Hasan, 'BTCL's Tk 463cr 5G project: Huawei's win marred by controversy', *The Daily Star*, 2 December 2023, [online](#).
- 75 'Unregulated transactions via WeChat Pay', *Annapurna Express*, 15 January 2025, [online](#).
- 76 Shih-Ting Lin, 'Chinese citizens in Pakistan: "Iron Brother Friendship" or an iron cage', Centre of Excellence for Himalayan Studies, Shiv Nadar University, April 2026, [online](#); Tenzin Dalha, 'Nepal: Belt and Road to Big Brother surveillance tech in China's sphere of influence', Tibet Policy Institute, 16 January 2026, [online](#).
- 77 Hattotuwa, 'Are Chinese telecoms acting as the ears for the Sri Lankan government?'
- 78 Thomas Hader, Benjamin Jensen, Divya Ramjee, Jose M Macias III, 'China's gray zone infrastructure strategy on the Tibetan Plateau: roads, dams, and digital domination', CSIS, 4 June 2025, [online](#).
- 79 Sandeep Bhardwaj, 'BIMSTEC: dysfunctional regionalism, South Asia style', Institute of South Asian Studies, National University of Singapore, 20 April 2025, [online](#).
- 80 Amaia Sanchez-Cacicedo, 'India's digital public infrastructure: success story', Institut Montaigne, 16 December 2024, [online](#).
- 81 Constantino Xavier, 'India as a democratic tech power in the liberal international order', Council on Foreign Relations, 11 May 2026, [online](#).
- 82 PACTS succeeded and replaced the 2020 Framework Arrangement on Cyber and Cyber Enabled Critical Technology Cooperation.

Acronyms and abbreviations

AI	artificial intelligence
BRI	Belt and Road Initiative
CCP	Chinese Communist Party
CCTV	closed-circuit television
CERT	computer emergency response team
DPI	digital public infrastructure
DSR	Digital Silk Road
GDP	gross domestic product
ICT	information and communications technology
IoT	internet of things
IT	information technology
ITU	International Telecommunication Union
OTT	over-the-top
PACTS	Australia–India Partnership on Cyber, Critical Technologies and Supply Chains
SARIC	South Asia Regional Infrastructure Connectivity



25
YEARS
2001-2026