THE DIGITAL SILK ROAD:

CHINA AND THE RISE OF DIGITAL REPRESSION IN THE INDO-PACIFIC

ARTICLE 19

First published by ARTICLE 19, March 2024

www.article19.org
72-82 Rosebery Ave
London EC1R 4RW
UK

ARTICLE 19 is an international think–do organisation that propels the freedom of expression movement locally and globally to ensure all people realise the power of their voices.

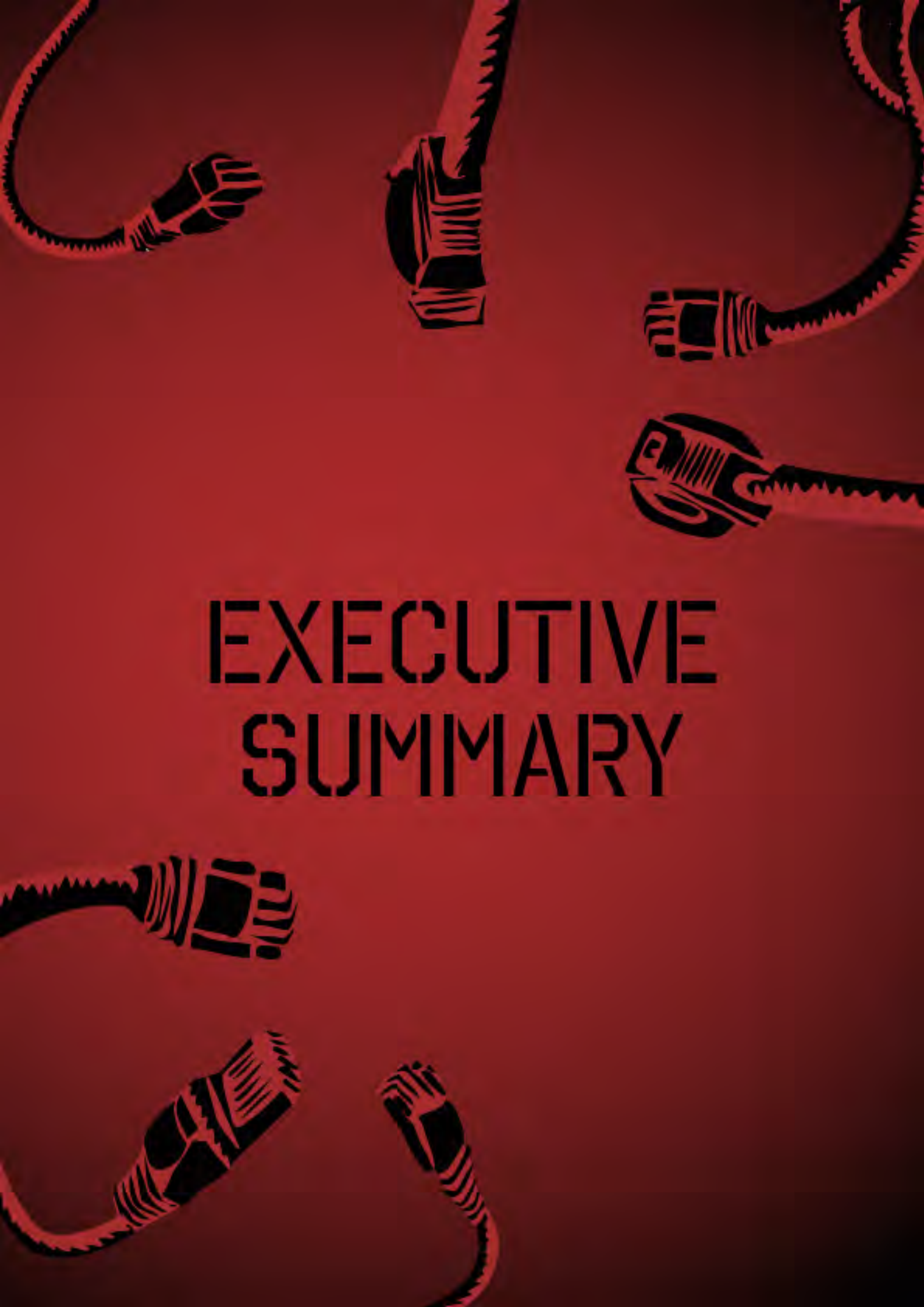
Together with our partners, we develop cutting-edge research and legal and policy analysis to drive change worldwide, lead work on the frontlines of expression through our nine regional hubs across the globe, and propel change by sparking innovation in the global freedom of expression movement. We do this by working on five key themes: promoting media independence, increasing access to information, protecting journalists, expanding civic space, and placing human rights at the heart of developing digital spaces.

Cover illustration by Badiucao

Table of Abbreviations

AAE-1	Asia–Africa–Europe 1
ADC	Asia Direct Cable Consortium
AI	artificial intelligence
AIS	Advanced Info Service
APEC	Asia-Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
BRI	Belt and Road Initiative
CCA	Computer-Related Crimes Act
CCP	Chinese Communist Party
CCS	China Communication Services Corporation Limited (China Comservice)
CFOCN	Cambodian Fibre Optic Cable Network
CGWIC	China Great Wall Industry Corporation
CII	critical information infrastructure
CMA	Communications and Multimedia Act
CSIC	Customer Solution Integration and Innovation Experience Centre
CSM	Cyber Security Malaysia
DFTZ	Digital Free Trade Zone
DNB	Digital Nasional Berhad
DSR	Digital Silk Road

FDI	foreign direct investment
HRIA	human rights impact assessments
ICCPR	International Covenant on Civil and Political Rights
ICT	information and communications technology
IoT	Internet of Things
ISOC	Internal Security Operations Command
MCT	Malaysia–Cambodia–Thailand
MDES	Minister of Digital Economy and Society
MIIT	Ministry of Industry and Information Technology
MOU	memorandum of understanding
MPTC	Ministry of Post and Telecommunications
NBTC	National Broadcast Telecommunications Commission
NDRC	National Development and Reform Commission
NIG	National Internet Gateway
NT	Nepal Telecom
PRC	People's Republic of China
SEATEL	South East Asia Telecom
TM	Telekom Malaysia
UDHR	Universal Declaration of Human Rights
UNGP	United Nations Guiding Principles on Business and Human Rights
XUAR	Xinjiang Uyghur Autonomous Region



EXECUTIVE SUMMARY

In this report, ARTICLE 19 examines the Digital Silk Road (DSR) as a platform for advancing China's model of digital authoritarianism, and seeks to equip civil society and other stakeholders with the necessary background and context to inform advocacy and policymaking. The report outlines internet freedom and human rights concerns associated with the DSR, especially those related to the right to freedom of expression and information and the right to privacy, through cases studies from the Indo-Pacific, where China has prioritised much of its DSR activity.

The report defines the DSR as an umbrella concept for evolving digital policies and priorities under China's larger Belt and Road Initiative (BRI), rather than a distinct policy on its own. It is a critical element of China's ambition to become a global technological superpower by developing the technology and policy to reshape global norms.

The Indo-Pacific will retain its strategic significance for China as it rolls out next-generation tech and seeks partners in normalising its authoritarian approach to digital governance. For this reason, assessing China's regional partnerships and what they mean for the deterioration of internet freedom and rising digital repression in the Indo-Pacific is important to an understanding of China's ambitions to rewire the world and rewrite the rules that govern the digital space.

The report begins by establishing a common understanding of China's domestic landscape for digital authoritarianism as a lens through which to see its approach to global digital infrastructure and governance. It focuses on how the Chinese Communist Party has systematically converted the tech sector – whose national champions, such as Huawei, ZTE, and Alibaba Group, have been at the forefront of DSR projects – into proxies for Party priorities. The Party capture of all sectors of society is emblematic of China's leader Xi Jinping's totalitarian government. Building on this, the report outlines legal frameworks in China, such as the National Intelligence and Cybersecurity Laws that impose obligations on individuals and institutions to perform censorship and surveillance functions, contrary to international human rights law.

The report then presents the evolution of China's domestic and foreign policy priorities and stated intentions under the DSR.

Through DSR partnerships, China has packaged its model as the prevailing best practice, often masked as support for innovation centres, exchanges, or broader digital diplomacy initiatives, especially on issues relating to cybersecurity. This is intended to tip the scales in global adoption to influence more states to employ Chinese norms, accelerating internet fragmentation. In the hands of authoritarian states, this has contributed to increasing restrictions on freedom of expression and information and the right to privacy, and other acts of digital repression.

China has often prioritised the Indo-Pacific under the DSR, with countries such as Cambodia, Pakistan, and Thailand among the first adopters. Six of the ten countries most globally exposed to China's malign influence, according to the Taiwan-based Doublethink Lab's China Index, are based in the Indo-Pacific. Regionally, the ARTICLE 19 Global Expression Report finds the state of expression in the region in stark decline over the past decade. Of the countries examined in this report, Malaysia and Nepal are ranked as 'restricted' while Cambodia and Thailand are 'in crisis'.

The protection and promotion of human rights compels states to develop transparency rules over the ownership of telecommunications infrastructure. The freedom of expression requires digital infrastructure that is 'robust, universal and regulated in a way that maintains it as a free, accessible and open space for all stakeholders'.

Each country in this report has benefitted from development assistance and DSR-related projects from China. The case studies examine infrastructure or digital governance partnerships in these countries, focusing on collaboration around 5G, submarine fibreoptic cable and satellite systems, digital economies, and cybersecurity-related laws and policies. Each case study is informed by open-source media reports and feedback from civil society experts in the respective countries to ensure that it highlights the areas of digital partnership with China that appear most prominent and concerning for civil society in that country.

Embracing China-style digital authoritarianism, since 2021 Cambodia has worked to impose its own version of the Great Firewall under a National Internet Gateway. Malaysia has not declined to this level of authoritarianism, but signs point to concerning ongoing partnerships with Chinese firms where policy changes could have serious consequences. In Nepal, development support from China in exchange for cracking down on Tibetan refugees has been ongoing, while recent changes in cybersecurity policy point to flirtations with a Chinese-style firewall. And in Thailand, since a military coup in 2014, the country's decline into digital dictatorship has been supported by cooperation agreements with China, leading to a range of cybercrime and cybersecurity legislation and interest in a China-style firewall. Uyghur refugees have also been caught in the crosshairs between China and host countries including Thailand. The report concludes with recommendations for various actors.

We consider the report a step in the right direction of supporting civil society, including journalists and other human rights defenders, and policymakers with the information necessary to inform future research, advocacy, and policymaking.

Key takeaways

- It is paramount that the rights to freedom of expression and information be promoted and protected, and that there be effective mechanisms for citizens to exercise their right to information on cooperation agreements with China and Chinese companies as part of any DSR project. Governments and private-sector partners should strive for transparency in all agreements signed with China or Chinese companies.
- Independent human rights impact assessments are a critical part of the procurement, design, development, and deployment of any digital infrastructure project, especially when it involves China or Chinese companies.
- More resources should be made available to support connectivity and internet development around the world. This support should be based on human rights law and internet freedom principles, to prevent China from exploiting internet development needs to position its services – and often by extension its authoritarian model – as the most accessible option.
- While confronting China's market dominance is important, democracies and tech companies should refrain from selling infrastructure or dual-use technologies to any government or deploying such technology on their behalf where the risks of human rights abuses, such as censorship or surveillance, are high.
- All governments and tech companies should actively dispel counterproductive narratives of 'if not us, then China', which have been used to excuse ongoing cooperation with states that abuse human rights, and should explore positive solutions to providing digital transformation support grounded in the protection of human rights and fundamental freedoms.
- Governments and other actors in international fora should ensure that multistakeholderism is the norm rather than multilateralism, which privileges a state-centric approach.
- All stakeholders should resist efforts to normalise concepts of digital sovereignty that promote internet fragmentation and relativism in contrast to the universality of human rights and internet freedom principles, and should seek to promote a free, open, and interoperable internet.
- Governments that claim to uphold principles of democracy, the rule of law, and human rights cannot merely critique China's authoritarian model of internet governance or sanction Chinese actors. They must also guarantee that they will not implement any China-style cybersecurity or other internet laws and policies that are not grounded in the strictest rights-based principles of internet freedom.

EXECUTIVE SUMMARY 5

Key takeaways 8

INTRODUCTION 10

THE DIGITAL SILK ROAD 15

Defining the Digital Silk Road 16
Institutions and Chinese ICT law 17
The party-state and 'private' digital industry 17
Information communication technology law in China 20
Situating the Digital Silk Road 24

REGIONAL CASE STUDIES 28

CAMBODIA **31**
Digital infrastructure 32
Fibreoptic and submarine systems 33
BeiDou in the spotlight **34**
China's 'digital diplomacy' in Cambodia 35
Networking authoritarianism 35

MALAYSIA **38**
Digital infrastructure 40
Digital economy 41
Networking authoritarianism 42

NEPAL **45**
Digital infrastructure 46
Tibetans caught between China and Nepal **48**
Networking authoritarianism 50

THAILAND **52**
Digital infrastructure 53
Fibreoptic and submarine systems 54
BeiDou Navigation Satellite System 55
Digital economy 56
Networking authoritarianism 57
Surveillance in the deep south **58**

Taiwan: Another way? **63**

INTERNATIONAL LAW 65

International human rights law 66
Right to freedom of expression and information 66
Right to privacy 67
United Nations Guiding Principles on Business and Human Rights 68
Human rights and internet infrastructure 69

RECOMMENDATIONS 70

Recommendations to the Government of Cambodia 71
Recommendations to the Government of Malaysia 72
Recommendations to the Government of Nepal 73
Recommendations to the Government of Thailand 74
Recommendations to the Internet freedom community 75
Recommendations to the United States 76
Recommendations for new strategic partnerships with Taiwan 77
Recommendations to global private tech sector organisations 78


INTRODUCTION

Since it was launched in 2015, the Digital Silk Road (DSR) has become an increasingly focal component of China's grandiose Belt and Road Initiative (BRI). It now appears slated for increased prioritisation by the Chinese Communist Party (CCP, or the Party) following the third Belt and Road Forum in October 2023. At this forum, China's leader Xi Jinping signalled his intention to downgrade the big-ticket legacy projects under the first decade of the BRI in favour of 'small yet smart' projects, which includes high-tech activities focused on digital infrastructure and governance norms.

This will play out as the Party focuses domestic and foreign policy priorities on creating a China-centric global alternative to current technological standards and digital governance norms, positioning its authoritarian model as an alternative to ultimately supplant the tenets of internet freedom and rights-based principles of global digital governance.

Globally, China has pursued opaque partnership agreements on telecommunications infrastructure such as fibreoptic and satellite systems, 5G, cloud computing, digital economy, smart cities, and other emerging technologies. Such infrastructure can be exploited to gain access to user data or to filter or block online content. China's domestic digital ecosystem and information and communications technology (ICT) legal frameworks thus provide a template for would-be digital dictatorships.

China has packaged its model of digital governance as the prevailing best practice, often masked as support for innovation centres, technology exchanges, or broader digital diplomacy initiatives, especially on issues relating to cybersecurity. The combination of infrastructure and policy, in the hands of authoritarian states, has contributed to increasing restrictions on freedom of expression and information and the right to privacy, and other acts of digital repression.

In its own words, China has often prioritised the Indo-Pacific region under the DSR, with countries such as Cambodia, Pakistan, and Thailand among the first adopters of Chinese technology. Even as it seeks to expand its influence elsewhere, the region will retain its strategic significance for China as it rolls out next-generation technologies and seeks global partners in normalising its authoritarian approach to internet governance. Six out of the ten countries most globally exposed to China's malign influence, according to the Taiwan-based Doublethink Lab's China Index, are based in the Indo-Pacific. The ARTICLE 19 Global Expression Report finds the state of expression in the region is in stark decline over the past decade. Of the countries examined in this report, Malaysia and Nepal are ranked as 'restricted' while Cambodia and Thailand are 'in crisis'.

Each country in this report has benefited from development assistance and DSR-related projects supported by China. The case studies examine what kinds of infrastructure or digital governance partnerships have taken place, with a focus on collaboration around 5G, submarine fibreoptic cable, and satellite systems; digital economies; and cooperation on cybersecurity-related laws and policies under broader digital governance partnerships. Each case study is informed by open-source media reports and then corroborated and ordered based on feedback from civil society experts in the respective countries, to ensure that it highlights those areas of digital partnership with China that appear most prominent and concerning for civil society in that country.

Assessing China's regional partnerships and what they mean for the deterioration of internet freedom and rising digital repression in the Indo-Pacific is important to understanding China's ambitions to rewire the world and rewrite the rules that govern the digital space.

In the most emblematic example of Cambodia's embrace of China-style digital authoritarianism, since 2021 Cambodia has worked to impose its own version of the Great Firewall under a National Internet Gateway. While Malaysia has not declined to the level of authoritarianism seen in Cambodia, signs point to concerning ongoing partnerships with Chinese firms where policy changes could have serious consequences. In Nepal, development support from China in exchange for cracking down on Tibetan refugees has been ongoing, while recent changes in cybersecurity policy point to flirtations with a Chinese-style firewall. And in Thailand, since a military coup in 2014 the country's decline into digital dictatorship has been supported by cooperation agreements with China, leading to a range of cybercrime and cybersecurity legislation and expressions of interest in a China-style firewall. Uyghur refugees have also been caught in the crosshairs between China and host countries including Thailand. The infographic on p. 14 highlights China's influence in these countries.

For these reasons, assessing China's regional partnerships and what they mean for the deterioration of internet freedom and rising digital repression in the Indo-Pacific is important to understanding China's ambitions to rewire the world and rewrite the rules that govern the digital space.

This report examines the DSR as a platform for advancing China's model of digital authoritarianism. In focusing on the actual and potential adverse influence on the rights to freedom of expression and privacy posed by DSR partnership, the report seeks to:

- ground the discussion of global DSR risks on a foundation of understanding of China's domestic approach to authoritarian digital governance;
- equip civil society with the necessary background and context to inform its advocacy;
- help policymakers to better prepare against the human rights implications of entanglement with the DSR; and
- explore the actual and potential human rights implications of DSR partnership in the Indo-Pacific region to understand the risks inherent in China's global ambitions.

The report is in no way exhaustive. While it aims to offer a clear evidence base for advocacy, it also presents opportunities for further research and investigation.

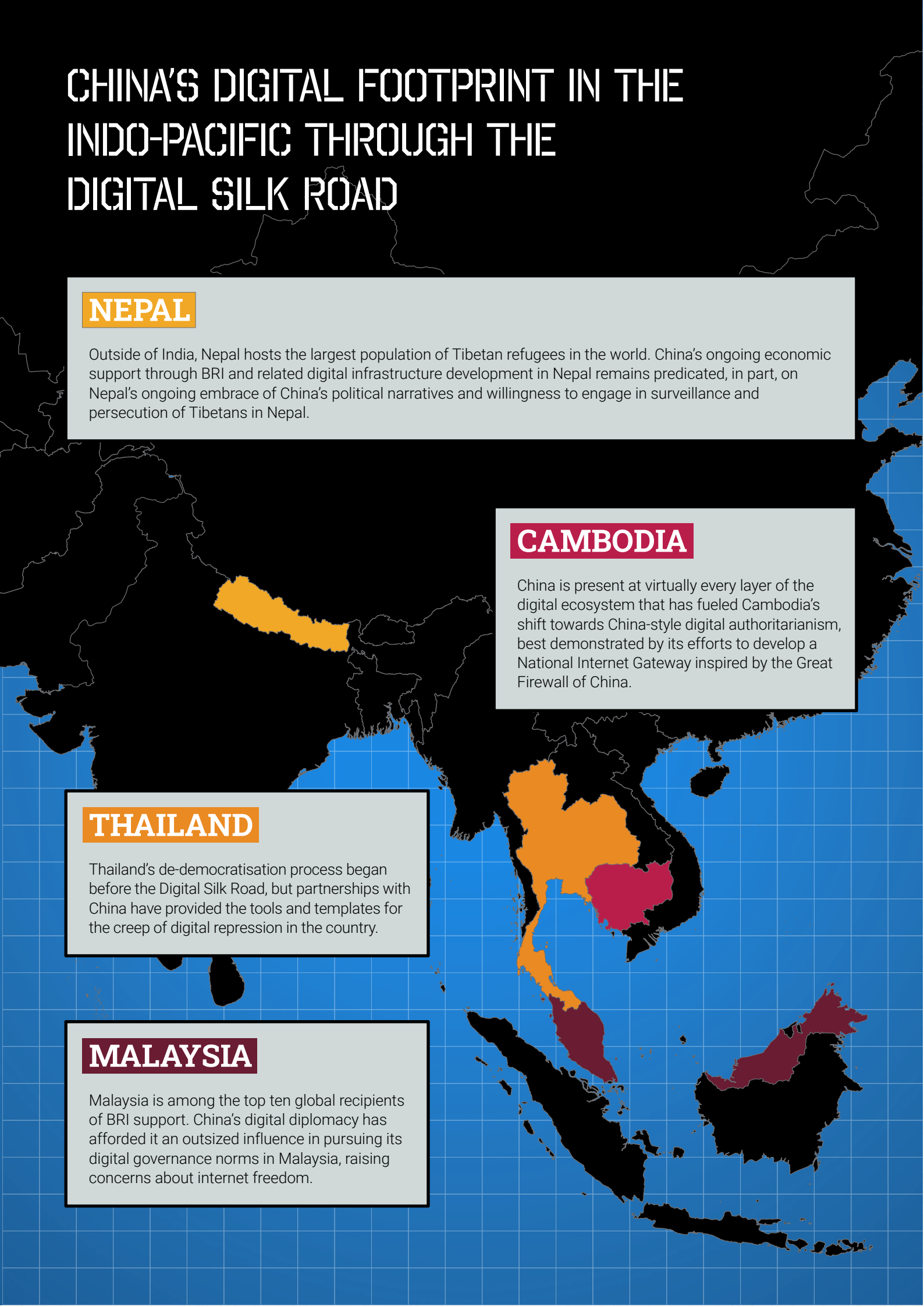
CHINA'S DIGITAL FOOTPRINT IN THE INDO-PACIFIC THROUGH THE DIGITAL SILK ROAD

NEPAL

Outside of India, Nepal hosts the largest population of Tibetan refugees in the world. China's ongoing economic support through BRI and related digital infrastructure development in Nepal remains predicated, in part, on Nepal's ongoing embrace of China's political narratives and willingness to engage in surveillance and persecution of Tibetans in Nepal.

CAMBODIA

China is present at virtually every layer of the digital ecosystem that has fueled Cambodia's shift towards China-style digital authoritarianism, best demonstrated by its efforts to develop a National Internet Gateway inspired by the Great Firewall of China.



THAILAND

Thailand's de-democratisation process began before the Digital Silk Road, but partnerships with China have provided the tools and templates for the creep of digital repression in the country.

MALAYSIA

Malaysia is among the top ten global recipients of BRI support. China's digital diplomacy has afforded it an outsized influence in pursuing its digital governance norms in Malaysia, raising concerns about internet freedom.


THE DIGITAL
SILK ROAD

Defining the Digital Silk Road

The Digital Silk Road is an umbrella concept for evolving digital policies and priorities under China's larger Belt and Road Initiative, rather than a distinct foreign policy on its own. It is a critical element of China's ambition to become a global technological superpower by developing the technology and policy to reshape global norms. This raises challenges for the future of internet freedom and broader technology and human rights issues.

For this report, we define the DSR by the following interrelated elements:

- **The DSR begins at home.** China is promoting and investing in the growth of homegrown industries towards technological independence, as a key feature of national security and to increase international adoption of technical standards that favour Chinese industry as the country's tech sector is increasingly integrated globally. 'Private' companies involved in new and emerging technologies are increasingly indistinguishable from the Party itself as their success becomes synonymous with the future of the Party. States along the DSR entering into public–private partnerships with Chinese technology companies are therefore effectively in partnership with the CCP.

- **The DSR is more than infrastructure.** The DSR is primarily dedicated to developing digital infrastructure, from terrestrial and submarine cables to satellite infrastructure, big data, the Internet of Things (IoT), and cloud computing. It also integrates device and application layers into promoting alternative economies through e-commerce and fintech applications. At the same time, China has engaged in digital diplomacy and content manipulation, for example through exchanges with state regulators, technicians, and journalists, either to soften partnership agreements or promote positive public narratives.

- **The DSR is a vehicle for China's networked authoritarian model of digital governance.** China is seeking to influence global norms through technical standards-setting bodies and other multilateral fora, including those purpose-built by China such as the World Internet Conference. This model emphasises digital sovereignty and the abandonment of multistakeholder internet governance, inclusive of civil society, in favour of a state-driven approach emphasising cybersecurity, censorship, and surveillance over a free, open, and interoperable internet.

Institutions and Chinese ICT law

In order to identify potential human rights implications associated with the DSR, we need to understand the interrelationship between the Party and ostensibly private technology sector institutions, as well as China's legal frameworks on ICT law, which are often at odds with international human rights norms.

The party-state and 'private' digital industry

Although Party guidance on industry in China is nothing new, the past decade has seen a dramatic consolidation of Party power over erstwhile private enterprises under Xi Jinping. This has effectively transformed industry into an extension of the Party, especially in the strategic technology sector. In part, this Party capture has been legitimised and institutionalised through the following laws and policies.

The 1993 Company Law of the People's Republic of China,[1] amended in 2018, requires Party organisations within companies to 'provide the necessary conditions to facilitate' Party activities. Party organisations are seen as a way to steer companies to support top-level Party policies. They generally lack transparency and accountability to outside regulators or judicial organs, answering only to higher-level CCP officials.

In March 2012, the General Office of the Party Central Committee issued its 'Opinions on Strengthening and Improving the Party Building Work in Non-Public Enterprises'[2] to 'comprehensively promote' Party-building within the private sector.

According to a study by the Chinese Private Enterprise Survey of the All-China Federation of Industry and Commerce, the Party group responsible for political development within the private sector, saturation grew on average 2 per cent per year from 2012 to 2018 (as discussed in a 2020 MacroPolo analysis). By 2018, nearly 93 per cent of China's top 500 companies had Party organisations within their corporate structures. Saturation is likely now at 100 per cent, especially in strategic industries such as the technology companies at the heart of China's global digital ambitions.

In 2018, the China Securities Regulatory Commission released a Code of Corporate Governance,[3] calling on state-owned enterprises to formally empower Party organisations in their corporate charters. While private companies were not required to revise their corporate charters, the number doing so had actually already spiked the year before.

1 中华人民共和国公司法

2 关于加强和改进非公有制企业党的建设工作的意见（试行）

3 中国证券监督管理委员会公告

Foreign companies have also been under increasing pressure to revise the terms of joint ventures and allow a greater role for the Party in decision-making. This has included strategic ventures with companies such as Samsung Electronics Suzhou Semiconductor: in 2018, all the company's executives and 74 per cent of its middle management or above were Party members. Since then, the pressure to permit greater CCP authority has been extended to wholly owned foreign companies and investment funds.

Thus, since around 2018, we see not only the growth of Party organisations within companies but also increasing Party power over management and decision-making. This is part of Xi Jinping's larger mission to consolidate CCP power over all institutions.

This emphasis on CCP supremacy is derived from a 14-point set of principles known as 'Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era' (Xi Jinping Thought), which calls for adherence to the leadership of the Party above all: 'Among the Party, the government, the military, the people, the academia and all circles, the Party leads all'.

Citing 'Xi Jinping Thought', in 2020 the General Office of the Party Central Committee issued a set of 'Opinions on Strengthening the United Front Work of the Private Economy in the New Era'[4] to strengthen and expand Party leadership over the private sector and harness the strengths of the private sector. The document calls for the Party's ability to plan and lead private industry from a political perspective to be improved; places a premium on ideological and political instruction to ensure consistency with Party priorities; and Party representation to be optimised among private-sector personnel in 'strategic emerging industries', including high-tech industries, in order that they 'unswervingly follow the Party'. This includes participation in major national strategic priorities, such as 'to actively participate in the Belt and Road construction, consciously safeguard national interests, and establish a good image of Chinese private enterprise'. Such efforts are part of China's united front work system to coordinate, among other things, global information manipulation and influence operations.

This Party capture is disproportionately felt in the technology sector. One emblematic case of the interplay between Party and non-Party roles for tech executives is that of former Huawei executive Zhou Daiqi,[5] who served an executive role within the company but more often represented Huawei in his capacity as Party Secretary, especially in high-level talks or the signing of strategic cooperation agreements, pointing to the significant role of the Party committee within the company. Following increased scrutiny of Huawei in recent years, the company has taken a more opaque approach to listing Party committee figures within the company.

4 中共中央办公厅印发 - 关于加强新时代民营经济统战工作的意见

5 周代琪

After Huawei, the e-commerce titan Alibaba Group has been perhaps the second-most important Chinese tech giant for DSR-related projects. For example, from 2018 to 2021 its cloud service revenue in the Indo-Pacific rose by 25 per cent, beating Amazon and Microsoft.

Alibaba Group co-founder and former CEO Jack Ma Yun[6] has had a contentious relationship with the Party, including when he disappeared for several months in 2021 after angering senior CCP leadership. In January 2023, under intense regulatory pressure, Alibaba Group announced that Ma would effectively be forced from his controlling position, a move that was completed in December 2023. This marks perhaps the most aggressive indicator of Party capture of the tech sector to date.

Before he fell out with the Party, Jack Ma was credited as an early influence on China's networked authoritarianism, an indicator of how the Party presumably views the utility of expanding such technologies along the DSR. In 2016, addressing the Central Political and Legal Affairs Commission (a powerful Party organ overseeing law enforcement and judicial actors), Ma promoted the surveillance potential of big data, explaining, 'The political and legal system of the future is inseparable from the internet, inseparable from big data … Bad guys won't even be able to walk into the square.'[7]

Under the umbrella of the DSR, Chinese technology firms operating abroad to build digital telecommunications services or provide guidance on technical standards and digital governance in the region and around the world, such as Huawei, Alibaba Group, or ZTE, claim that they are independent and pose no risk of collusion with the Chinese Government for the purposes of intelligence-gathering or promoting technologies for censorship. These are empty assurances, as not only are they increasingly guided by Party capture but China's ICT legal framework (outlined below) imposes precise censorship and surveillance obligations.

The shaping of China's technology companies to be extensions of the Party started almost from the beginning of Xi Jinping's time in power. Within weeks of assuming his position as General Secretary of the CCP in 2012, Xi Jinping's first inspection tour kicked off with a visit to Tencent's headquarters, Kuang-Chi Institute of Advanced Technology[8] (further discussed in the Cambodia case study), and other technology companies. At Tencent, Xi Jinping tellingly asked the company for advice on adapting the internet to manage society. Over the coming years, ICT legislation evolved to suit his networked authoritarian objectives.

6 马云

7 As reported by Josh Chin and Liza Lin (2022) Surveillance State: Inside China's Quest to Launch a New Era of Social Control, New York: St Martin's Publishing Group

8 深圳光启高等理工研究院

Chinese law has evolved to impose authoritarian obligations on individuals and institutions to act as extensions of the Party. This raises serious concerns about China's global digital ambitions.

Information communication technology law in China

In addition to the growing role of the Party in Chinese technology firms, Chinese law has evolved to impose authoritarian obligations on individuals and institutions to act as extensions of the Party. This raises serious concerns about China's global digital ambitions.

Article 22 of the Counter-Espionage Law (2014, revised 2023)[9] requires organisations and individuals to cooperate with state security organs gathering evidence and investigating espionage. The concept and definition of espionage in China has expanded to effectively cover any engagement with foreign entities, including those protected by international norms on the freedom of expression and information.

In 2021, China expanded counter-espionage priorities, with an editorial in the CCP-affiliated *Global Times* emphasising the threat of collusion through examples of Chinese journalists working with 'mainstream Western media outlet[s]' to 'stigmatize China'. This is a threat to press freedom, raising concerns about self-censorship and access to information, that does not end at China's borders. China is already 'the world's largest prison for journalists, and its regime conducts a campaign of repression against journalism and the right to information worldwide'.

The Counter-Espionage Law seemingly applies to Chinese media seeking to conduct their own investigative journalism into DSR or related infrastructure projects. It also means that Chinese news assistants and fixers are vulnerable to criminal prosecution for facilitating foreign news investigation or for covering Chinese infrastructure or related projects abroad. These types of fear tactics have a direct impact on journalism and the right to information for all.

9 中华人民共和国反间谍法

The updated law also places additional emphasis on cyber- and data security and anti-espionage expectations for digital spaces, adding a whole new definition of espionage to include 'network attacks … [on] critical information infrastructure'.

It is unclear exactly how China will seek to enforce these regulations outside of its borders. For example, it seems to raise the risk of Chinese media workers being accused of espionage as a result of activities unwanted by the Party. In defining 'acts of espionage' to include those carried out or funded by foreign entities or individuals to 'purchase or illegally provide state secrets, intelligence, and other documents, data, material, or items related to national security', virtually anything could be espionage. This includes public interest investigation of the human rights impact of the DSR.

The National Intelligence Law (2017)[10] effectively requires individuals and institutions to comply with state surveillance efforts. Article 7 requires that 'all organizations and citizens shall support, assist, and cooperate with national intelligence efforts'. This applies to Chinese tech companies operating abroad. Article 11 holds that those engaged in national intelligence work must 'collect and handle intelligence related to foreign institutions, organizations or individuals' vaguely deemed to be a threat to the 'national security and interests of [China]'.

The 2017 Cybersecurity Law[11] has become the backbone of China's restrictive 'digital sovereignty' model and has influenced similar laws around the world. It establishes provisions on data localisation, real-name identity verification, and network shutdowns, while actually weakening cybersecurity. It empowers the Cyberspace Administration of China to oversee inter-agency cooperation on cybersecurity efforts, especially in relation to critical information infrastructure.

Section 2 outlines a number of obligations specifically on critical information infrastructure (CII) operators, subjecting them to strict data control and government oversight. Article 31 holds that the state 'encourages' non-CII operators to also 'voluntarily' follow the same rules, effectively imposing a blanket requirement on all digital actors. While the law does not define CII, later regulations released in 2021 (discussed below) offer some clarity.

Among the more concerning provisions, Article 37 includes data localisation requirements that hold that CII operators must store 'important data' within mainland China. Data localisation requirements apply to foreign companies operating in China and to Chinese companies operating internationally through DSR projects.

Article 21 requires network operators to adopt measures to monitor and record network traffic data, and to store network logs for at least six months. Article 28 continues that they must provide vaguely defined 'technical support' to public and state security organs – or in other words, comply with the authorities in surveillance activities.

10 中华人民共和国国家情报法

11 中华人民共和国网络安全法

Article 24 holds that network operators must require users to provide real-name identification, especially for publication and instant messaging services, in a major blow to online anonymity. Encryption and circumvention tools are subjected to near total criminalisation in China.

The law also empowers censorship. Article 48 requires the broad categories of electronic information distribution and application service providers to censor prohibited information or programmes and report people to the government for disseminating or storing prohibited content.

In an attempt to legislate the internet shutdowns that are increasingly seen around the region, especially in Myanmar, Article 58 proffers a legal basis for targeted network interference 'to protect national security and the social public order'.

Since the Cybersecurity Law came into effect, additional rules and regulations clarifying and strengthening the state's censorship powers have come into force. The Provisions on the Governance of the Online Information Content Ecosystem (2020)[12] and the draft Provisions on the Management of Internet Post Comments Services (2022)[13] are emblematic. China's extensive censorship capabilities have increasingly extended beyond its borders, posing a significant threat to internet freedom.

The Data Security Law (2021)[14] empowers the Cyberspace Administration of China. Article 35 compels organisations and individuals to cooperate with public and state security authorities in obtaining data to 'safeguard national security or investigate crimes'. This language is similar to that of the cooperation requirements under the National Intelligence Law. It is equally vague and overbroad.

The law claims extraterritoriality in the name of data sovereignty. Article 2 states that when data is handled outside of China in a way that harms national security, public interest, or the 'lawful rights and interests of citizens or organizations of the PRC [People's Republic of China]', determines that China may pursue legal liability. This is again extremely vague and overbroad, allowing for 'harming national security' or 'public interest' to mean anything, and seems drafted for the purposes of political reprisal.

Article 26 notes, without definition, that if any country or region adopts 'discriminatory prohibitions, restrictions, or other similar measures against the PRC relevant to investment, trade, etc. in data, data development and use technology', China may take reciprocal measures. This is seemingly intended to justify reprisal should foreign regulators attempt to limit China.

12 网络信息内容生态治理规定

13 国家互联网信息办公室关于《互联网跟帖评论服务管理规定（修订草案征求意见稿）》公开征求意见的通知

14 中华人民共和国数据安全法

China's Personal Information Protection Law (2021)[15] is further relevant to assessing not only China's domestic ICT policy landscape but also how the integration of Chinese technology firms into the global ecosystem can impact privacy rights.

Article 35 of the law explains that officials have no notification duties when collecting personal information under certain undefined circumstances, such as where notification would impede fulfilment of official duties and responsibilities. Article 26 holds that personal identity recognition equipment, such as facial recognition cameras, may be used only for 'safeguarding public security' – but it is left entirely up to the security sector to define this. Biometric data is considered sensitive personal information, requiring strict protection measures under Article 28, except when there is a 'specific purpose'.

All exceptions such as those above are vague, overbroad, and left open to interpretation by the authorities implementing invasive data-driven policing and related surveillance practices. For example, in both the Tibetan and the Uyghur regions of China, mass forced biometric data collection has been linked to gross human rights abuses.

Article 36 requires that personal information collected by the state be stored within mainland China, except in extreme circumstances. Article 53 requires foreign entities to establish 'a dedicated entity or appoint a representative' within mainland China.

In Article 43, China claims the right to retaliatory measures against any country or region that adopts vaguely defined 'discriminatory prohibitions, limitations or other similar measures' against China relating to personal information. This provision could be read as a threat of retaliatory action should DSR partners enact limitations on Chinese technology companies handling personal data within related projects.

The Critical Information Infrastructure Security Protection Regulations (2021)[16] build on the 2017 Cybersecurity Law obligations on CII operators. They have been described by the Deputy Director of the Cyberspace Administration of China, Sheng Ronghua,[17] as a specific measure intended to implement Xi Jinping's 'important thought on cyber power', a euphemism for totalising Party control. The regulations are relevant for understanding China's involvement in digital infrastructure beyond its borders.

Article 2 offers a non-exhaustive set of definitions for CII, including 'public telecommunications and information services, energy, transportation, water, finance, public services, e-government, national defence science, technology, and industry'.

15 中华人民共和国个人信息保护法

16 关键信息基础设施安全保护条例

17 盛荣华

CII operators are to establish a responsible person and security management team, who must work closely with public security authorities. CII operators must comply with the vaguely worded Cybersecurity Review Measures (2022),[18] and must undergo a security review when such products and services may influence national security.

In August 2021, before the regulations came into force, Sheng Ronghua emphasised that foreign companies could also be considered CII operators in China, depending on their function, and would be bound by the regulations. The question is how far China will go in imposing jurisdiction over partnerships for the development of CII under DSR-related projects.

Situating the Digital Silk Road

The first real reference to a DSR[19] appears in the 2014 Ministry of Industry and Information Technology (MIIT) 'Plan for the Construction of Interconnected Infrastructure in Surrounding Countries',[20] which laid out China's ambition to achieve interconnectedness in data and information services and international communications services within the BRI.

This was the same year that China established the Cyberspace Administration of China,[21] which has played a significant role in developing and implementing China's digital authoritarianism and broader efforts to internationalise its model of internet governance, such as through the World Internet Conference in Wuzhen.

18 网络安全审查办法

19 数字丝绸之路

20 周边国家互联互通基础设施建设规划

21 国家互联网信息办公室

Throughout its evolution, the DSR has been just as much about promoting China's tech industry and developing digital infrastructure as it has about reshaping standards and internet governance norms away from a free, open, and interoperable internet.

In 2015, the National Development and Reform Commission (NDRC) formally introduced the DSR in its white paper '**Vision and Actions to Promote the Joint Construction of the Silk Road Economic Belt and the 21st Century Maritime Silk Road**',[22] calling for accelerated construction of cross-border backbone networks such as fibreoptic and submarine cables and satellite networks, and for the broad expansion of ICT exchange and cooperation.

It also stressed China's ambition to lead in technical standards-setting under the **China Standards 2035** policy, a '**blueprint** for the Chinese Government and leading tech companies to set global standards for emerging technologies, such as 5G, IoT, and artificial intelligence'. China has **outlined plans** to actively strengthen standardisation with APEC and to deepen standardisation cooperation in the Indo-Pacific. Since 2015, China has made technical standards part of bilateral agreements, signing memoranda of understanding (MOUs) on standardisation with Vietnam, Myanmar, and Indonesia. As with most such agreements, these are non-public.

In December 2016, the State Council published the **13th Five-Year Plan for National Informatisation**,[23] outlining ambitions for China to reform global internet governance. It also called for accelerated collaboration with the Association of Southeast Asian Nations (ASEAN).

The same year, the State Administration for Science, Technology and Industry and NDRC released the '**Guiding Opinion on Accelerating the Construction and Application of the Belt and Road Spatial Information Corridor**',[24] expressing China's vision of completing its space information corridor by 2026. South East and South Asia are listed as the first two priority regions. It further stresses support for BeiDou satellite infrastructure and navigation systems in ASEAN countries, namely Thailand, Laos, Indonesia, and Cambodia. China has signalled **plans** to build as many as 1,000 satellite ground stations throughout South East Asia.

In 2017 and 2019, China hosted the first and second Belt and Road Forums. The second **concluded** with 85 technical standards agreements with 49 countries, although these are marked by a lack of transparency. A **joint communiqué** issued by heads of state, including those of Cambodia, Indonesia, Malaysia, Myanmar, Nepal, Pakistan, and Thailand, stressed continued efforts towards digital infrastructure, including fibreoptics, e-commerce, and smart cities, through public–private partnerships and the strengthening of cooperation in the Indo-Pacific.

An infrastructure investment masterplan released in 2020 **highlighted** China's intention to invest USD 1.4 trillion over the following six years in digital infrastructure development, mobilising governments and private tech companies like Alibaba, SenseTime, and Huawei to 'lay 5G networks, install cameras and sensors, and develop AI [artificial intelligence] software that will underpin autonomous driving to automated factories and mass surveillance'.

---

22 推动共建丝绸之路经济带和21世纪海上丝绸之路的愿景与行动

23 国务院关于印发 "十三五"国家信息化规划的通知

24 国防科工局 发展改革委关于加快推进"一带一路"空间信息走廊建设与应用的指导意见

In March 2021, China launched its 14th Five-Year Plan (2021–2025) for National Economic and Social Development and Vision 2035 of the PRC.[25] This outlines plans to unlock the potential of big data and strengthen China's role in cyberspace, especially emerging technologies such as high-end chips, AI, cloud computing, and cybersecurity, as well as new approaches to governance through smart cities.

Elaborating earlier concepts, in November 2022 China's State Council Information Office issued a white paper, 'Jointly Build a Community with a Shared Future in Cyberspace',[26] emphasising China's goal of accelerating global digital infrastructure, including specific references to the Indo-Pacific. It promotes a greater rollout for BeiDou and China's objective for BeiDou to enter international standardisation organisations.

The white paper highlights regional joint initiatives relating to cybersecurity. It hails the expansion of partnerships under the National Computer Network Emergency Response Technical Team/Coordination Centre of China (CNCERT/CC)[27] to 81 countries and the establishment of MOUs with 33, such as Indonesia and Thailand. The partnership with ASEAN began in 2017 with the China–ASEAN Network Security Emergency Response Capacity Building Seminar, in which Cambodia, Indonesia, Laos, Myanmar, the Philippines, Thailand, and Vietnam participated.

Building on this, the paper calls for a China–ASEAN Network Security Exchange and Training Centre, exemplifying China's digital diplomacy to shape cybersecurity norms.

It is of concern that the approach is based on China's principle of digital sovereignty, under which 'all countries should be respected to independently choose their cyber development path, governance model, and equal participation in the international governance of cyberspace. All countries have the right to formulate public policies, laws and regulations related to cyberspace according to their own national conditions and drawing on international experience.' This is at odds with international human rights law and internet freedom principles.

Marking ten years of the BRI, in October 2023 China hosted a third Belt and Road Forum, ahead of which a white paper was published stressing its successes along the DSR. At the forum, China launched an AI Global Governance Initiative firmly rooted in principles of digital sovereignty, reiterated its ambition to lead in developing rules for global digital governance, and concluded several joint press statements, including with Pakistan, Indonesia, and Thailand, promising strengthened cooperation on areas such as 5G, smart cities, digital economy, and AI. Xi Jinping signalled intentions for China to move away from massive signature BRI infrastructure projects in favour of more 'small yet smart' projects, such as high-tech DSR activities.

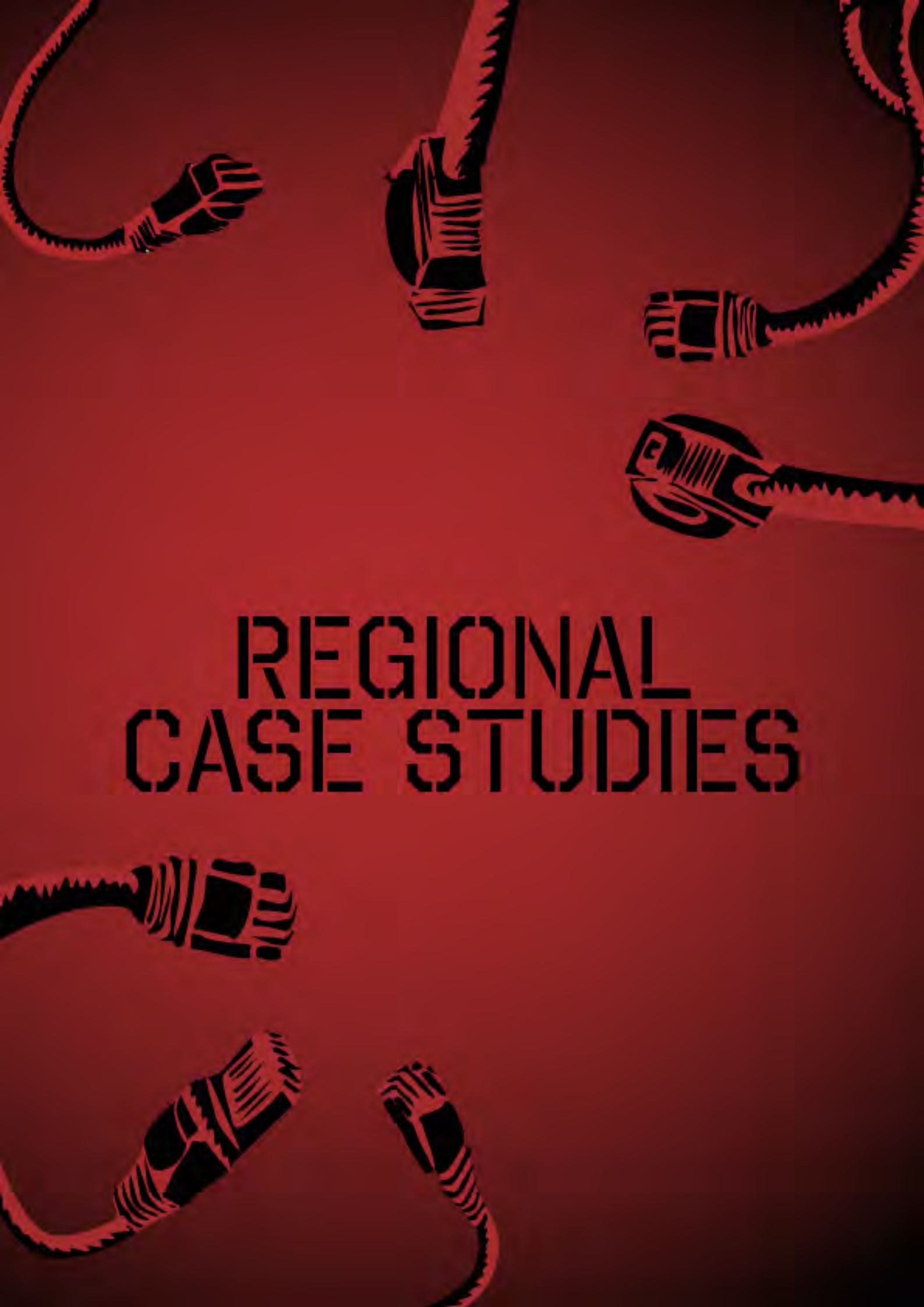
25 中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要

26 携手构建网络空间命运共同体

27 国家互联网应急中心

Projection of Xi Jinping at the World Internet Conference in Wuzhen on 23 November 2020. (Photo: Aly Song/ Reuters)

Throughout its evolution, the DSR has been just as much about promoting China's tech industry and developing digital infrastructure as it has about reshaping standards and internet governance norms away from a free, open, and interoperable internet in favour of a fragmented digital ecosystem, built on censorship and surveillance, where China and other networked autocracies can prosper. Although China's malign influence has not always been explicit in DSR-related partnerships, it has provided the infrastructure and a model of digital governance that has exacerbated the deterioration of internet freedom and the embrace of digital repression in the region.



REGIONAL CASE STUDIES

Six out of the ten countries most exposed to China's malign influence, according to the Taiwan-based Doublethink Lab's China Index, are based in the Indo-Pacific. Regionally, the ARTICLE 19 Global Expression Report finds the state of expression in much of region in stark decline over the past decade. Of the country case studies examined in this report, Malaysia and Nepal are ranked as 'restricted' while Cambodia and Thailand are 'in crisis'.

China has prioritised Indo-Pacific countries throughout the past decade of BRI and DSR policies and projects, from the development of connectivity and economic infrastructure to partnership on cybersecurity and other aspects of digital governance. While the majority of DSR partnerships across the region have been agreed with China's national technology champions, such as Huawei, ZTE, Alibaba Group, and Tencent, Party capture and ICT regulations have blurred the line between the state and such tech companies, increasing the need for enhanced transparency and human rights due diligence.

Huawei and ZTE have emerged as leading infrastructure providers across the region, out-competing others such as Samsung and Ericsson, especially in relation to 5G infrastructure. China's role in developing undersea cable systems in the region is also pronounced. With some 95 per cent of global internet traffic travelling via submarine cables, China's goal of gaining greater control of this infrastructure through the DSR raises questions about information flow and security.

China's BeiDou global satellite system has active agreements with the region, and China is also pursuing satellite internet infrastructure opportunities for the future. Such developments raise questions about more sophisticated surveillance and censorship at the infrastructure level.

Chinese fintech and e-commerce platforms such as with Alipay and Tencent's WeChat Pay have flourished across the Indo-Pacific, beginning with marketing to growing numbers of Chinese tourists, followed by a broader rollout for other users. Chinese companies have also expanded controlling stakes and the acquisition of national products, such Alibaba affiliate Ant Group's acquisition of Singapore-based Lazada, one of the largest e-commerce platforms in South East Asia. This digital economy expansion poses concerns over the right to privacy, providing Chinese companies, and consequently the Chinese Government, with considerable access to user data.

Digital economies collect vast amounts of data, as Jack Ma alluded to while head of Alibaba in noting the role of big data in training the surveillance systems of the future. Chinese technology companies are obligated under the law to grant data access to the authorities. It is plausible that China would share such data with allied authoritarian governments or exploit it as part of its influence operations over others. Without greater transparency and oversight, it is impossible to rule out these concerns.

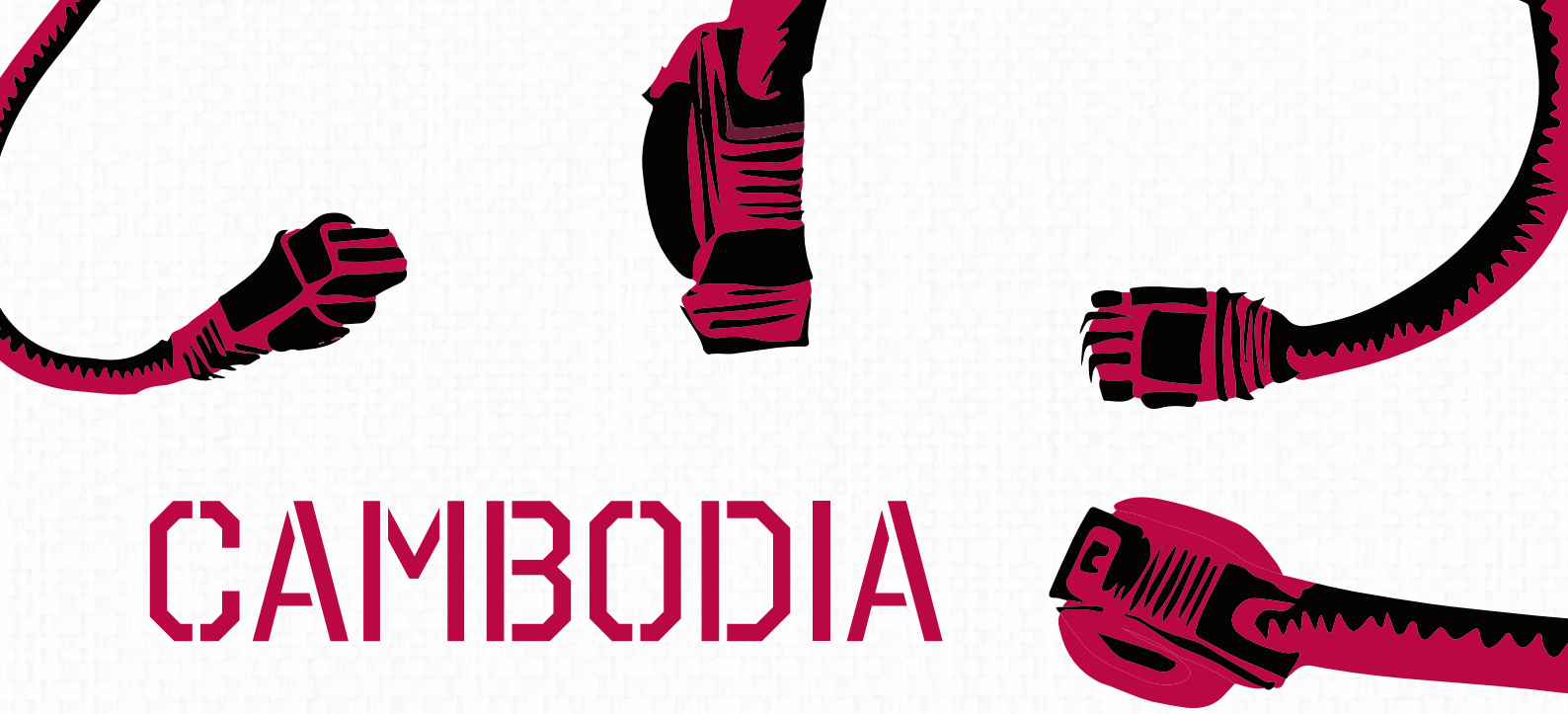
China has also vigorously courted countries in the Indo-Pacific through digital diplomacy and the establishment of innovation centres to promote Chinese technologies and the country's authoritarian model of internet governance. This is seen especially in relation to its form of digital sovereignty, at odds with the principle of multistakeholderism and of a free, open, and interoperable internet.

In some countries in the region, China's presence within the digital ecosystem is nearly universal, giving it tremendous influence over traditional and digital infrastructure and internet laws and policies. Such cooperation is often hidden behind opaque agreements, while access to information is further complicated through repressive legislation and the targeting of media or outright reprisal and physical violence against human rights defenders critical of China's role in the region. China's digital footprint, while embraced by the region's authoritarian or semi-authoritarian regimes, has nevertheless faced resistance from civil society.

For example, in June 2018, ahead of Vietnam's adoption of a Cybersecurity Law closely modelled on China's, tens of thousands of protesters gathered across the country against the law and against a planned Special Economic Zone bill that would have allowed foreign investors to take out 99-year leases. Protesters carried signs reading 'no land lease to China even for one day' and 'the cybersecurity law means silencing people', among other slogans. Despite the demonstrations, Vietnam enacted the law, which came into effect in January 2019.

Another case of apparent reprisal against those speaking out against China's footprint is that of Laotian human rights defender Anousa Luangsuphom, also known as Jack. In 2022, Jack launched 'Kub Kluen Duay Keyboard' (Driven by the Keyboard), a Facebook page focused on exposing corruption and human rights repression in Laos, including cases associated with China. On 29 April 2023, an unidentified gunman approached Jack in a café and `shot him in the face and chest. Barely surviving, Jack later recalled that all he knew was that on the day he was shot, he had explicitly posted online against China's level of control over Laos.

Throughout China's investments and partnerships in the region, the DSR has been a vehicle for expanding China's model of networked authoritarianism, leaving the actual adoption of the tools and templates of repression up to governments. The following case studies outline in depth how DSR-related cooperation between China and Cambodia, Malaysia, Nepal, and Thailand has affected internet freedoms and broader digital rights.



CAMBODIA

Globally, Cambodia ranks second only to Pakistan in the China Index, making it one of the countries most exposed to China's influence. China is Cambodia's largest foreign investor and development partner, and Cambodia is perhaps China's staunchest ally in South East Asia. In 2020 alone, Chinese direct investment accounted for more than half of all foreign direct investment (FDI) in Cambodia since 1993. The cooperation has many elements, including those relating to digital infrastructure and internet governance.

At the 2017 Belt and Road Forum, China and Cambodia signed 13 agreements, including agreements outlining the important role that Chinese tech companies should play in exporting telecommunications equipment to Cambodia and calling for greater bilateral cooperation in, for example, enhancing BeiDou and spatial information services. Cambodia signed a further eight agreements with China at the 2023 Belt and Road Forum, where Cambodian Prime Minister Hun Manet called for 'increased funding for the development of digital infrastructures including connectivity, data centres, security and other(s)'.

Huawei, ZTE, Alibaba, and Tencent, among others, have played a leading role in Cambodia. Alongside infrastructure-level cooperation, the shadow influence of China's internet governance model has loomed large over Cambodia's embrace of digital authoritarianism.

In early 2022, Cambodia launched its Cambodian Digital Government Policy 2022–2035, built on ten strategic pillars including the development of digital information and connectivity, payment systems, and security infrastructure, as well as organisation around digital governance. The preface refers to China as a positive case study in successful digital government, raising concerns about the further deterioration of internet freedom in Cambodia.

Digital infrastructure

Cambodia's digital ecosystem has developed in large part through significant input from China and Chinese companies, which have established market dominance over competitors like Viettel, Ericsson, or Nokia. This is in part the result of 'undisclosed subsidies from Chinese state institutions, such as the Silk Road Investment Fund and the Bank of China' – a feature across the whole DSR.

China's technology presence is noticeable at every layer of Cambodia's digital ecosystem. This includes 5G, terrestrial and submarine fibreoptic cable systems, data centres, and cloud computing (Huawei is the country's only authorised cloud service provider), among other areas.

Huawei is the largest Chinese technology company operating in Cambodia, with ZTE a close second. Others include Xiaomi, which focuses on mobile distribution through partnership with South East Asia Telecom (Cambodia) Co. Ltd (SEATEL Cambodia)' and Alibaba Group, which has been developing Cambodia as a logistics hub. In August 2023, Cambodian civil society activists told ARTICLE 19 on condition of anonymity that Cambodian internet service providers are increasingly requiring customers to purchase Huawei Wi-Fi routers, whereas previously customers could choose routers from other companies such as Linksys or Asus. This has especially been the case with Cambodian telecom EZECOM.

Huawei's dominance, especially in 5G, has accelerated since 2019 following an agreement with the Ministry of Post and Telecommunications (MPTC) and Smart Axiata, a Cambodian operator under the Malaysian parent company Axiata Group Berhad.

Addressing Huawei's perceived importance, in March 2022 Dong Yuanpeng,[28] the Chief Communications Officer of Huawei Cambodia, noted that the company had 'changed the landscape of digital infrastructure in Cambodia'. These remarks were made before the Cambodia Internet Startup Association, the Chinese association of internet companies in Cambodia, whose stated vision is 'to empower Cambodian Internet start-ups and build a brilliant milestone along the path of the Belt and Road Initiative' and which aims to bring more investment from China to the ecosystem of the Cambodian internet industry. Such exchanges are emblematic of China's soft power and digital diplomacy efforts in Cambodia, which contribute to China's dominant position in the digital ecosystem.

Some Cambodian civil society representatives have raised concerns with ARTICLE 19 about how support from China on digital infrastructure and governance will improve Cambodia's future capability to implement a China-style Great Firewall and tighter controls on internet freedom.

28 董元鹏

Fibreoptic and submarine systems

Since 2017, Cambodia has had two operational submarine cable landing stations, both in Sihanoukville. One is the Malaysia–Cambodia–Thailand (MCT) system administered by Cambodian Telcotech, a subsidiary of EZECOM and the Cambodian Royal Group. The MCT was originally built by Huawei Marine, which after acquisition by Hengtong Group[29] was rebranded as HMN Technologies Co. Ltd[30] in 2020. Huawei's sale of its submarine fibreoptic holdings was seen as a response to mounting international pressure over information security.

Cambodia's other submarine cable is the Asia–Africa–Europe 1 (AAE-1) system operated by Cambodian Fibre Optic Cable Network (CFOCN). An agreement to connect Cambodia to AAE-1, launched by Chinese state-owned telecommunications company China Unicom in 2013, was signed in 2016 between the MPTC and CFOCN. It went online the next year. CFOCN is a subsidiary of the Singapore-based HyalRoute Communication Group, one of whose major shareholders is Shenzhen Kuang-Chi Group,[31] a Chinese technology firm with interests in AI, smart cities, and telecommunications. Kuang-Chi Group's presence in the ownership structure, and potentially the governance, of a critical information network in Cambodia is concerning. Kuang-Chi Group' since 2020, has been on the US entities list and subject to export restrictions for enabling 'wide-scale human rights abuses within China' and for having 'facilitated the export of items by China that aid repressive regimes around the world'.

In February 2023, construction began on a third submarine cable system to link Cambodia to Hong Kong. While Huawei was reportedly originally planning to instal the new undersea cable, following the above changes the project now appears to be under the control of China Unicom. It is slated for completion in 2025.

Cambodia and China Great Wall Industry Corporation have been partnering since 2017 to roll out more advanced satellite systems, despite unaddressed human rights concerns. (Photo: Pascal Rossignol/Reuters)

29 亨通集团有限公司

30 华海通信技术有限公司

31 深圳光启高等理工研究院

BeiDou in the Spotlight

Since at least 2011, Cambodia has entertained notions of its own satellite internet, with the no-bid signing of a multi-million-dollar licensing agreement between Royal Blue Skies, a subsidiary of the Royal Group, and the MPTC. By 2016, with little progress made, in part due to the more advanced development of the MCT submarine fibreoptic system, then-Prime Minister Hun Sen encouraged the Royal Group to seek outside partners.

Cambodia's participation in the 2017 Belt and Road Forum led to a partnership between Royal Blue Skies and the China Great Wall Industry Corporation (CGWIC) (中国长城工业集团有限公司), a subsidiary of the state-owned China Aerospace Science and Technology Corporation (中国航天科技集团公司). In 2018, CGWIC and the Royal Group signed a framework agreement outlining that China would provide the Royal Group with 'end-to-end satellite services including satellite development, launch, ground station systems, and training and technology transfer'. Despite cooperation, the revised 2021 deadline for the launch of Cambodia's own satellite passed, while the country deepened its reliance on China's satellite infrastructure.

In November 2020, Cambodia's Ministry of Public Works and Transport signed an MOU with CGWIC to use the BeiDou Navigation Satellite System. The MOU is not publicly available. A spokesperson for the Ministry said that the BeiDou system would give new life to Cambodia's development, in line with China's BRI. Cambodia has reportedly already rolled out several hundred BeiDou GPS and remote sensing technologies.

China is also reportedly maintaining BeiDou ground station technology at a naval base in Sihanoukville, which will be reserved exclusively for use by China's military.

In addition to its imaging capabilities, BeiDou satellite infrastructure provides communications services, namely SMS messaging and user tracking. The BeiDou Smart Police Terminal system synchronises these functions, with digital ID verification and fingerprint recognition, along with providing police access to satellite-enabled personal, vehicle, business, and location data in real time that can be remotely uploaded to police command centres. In June 2020, China was reporting that more than 400,000 portable terminals were in use by public security across China and had been used for security at high-level events in Asia-Pacific. As of 2020, Chinese products based on BeiDou were in use in 120 countries.

Because of the high risk of surveillance and other human rights abusing use cases, and the lack of transparency, further deployment of BeiDou in Cambodia has been met with concern from local human rights organisations. Members of Cambodia's civil society have told ARTICLE 19 of concerns that infrastructure upgrades relating to the transmission and storage of high-capacity data point to plans to upgrade reliance on China's satellite systems for such use cases.

Cambodian civil society has expressed deep concerns that ongoing support from China on digital infrastructure and governance will supercharge Cambodia's capability to impose a China-style Great Firewall and tighter controls on internet freedom.

China's 'digital diplomacy' in Cambodia

China has engaged in significant digital diplomacy and capacity-building, arguably not just improving Cambodian network engineering ability but also providing the technical knowhow for Cambodia to better emulate China's digital authoritarian model.

Examples include a 2018 MOU establishing the Cambodia–China Technology Transfer Centre, a research institution to train Cambodians in science, technology, engineering, and mathematics. In 2020, officials from the MPTC were invited by the China Academy of Information and Communications Technology, under the MIIT, for 5G training in Beijing, to promote 'Chinese national policy for supporting 5G development' and related topics. In late 2023, the Cambodia–China University of Technology and Science opened in Phnom Penh, further systematising China's digital diplomacy.

Examples of Chinese companies fulfilling United Front obligations include a 2022 Huawei ICT training programme for Cambodian students to strengthen relations with China. At the launch, China's ambassador noted that 'China and Cambodia are now building a community with a shared future, and ICT increasingly becomes an important field of cooperation'.

Networking authoritarianism

In Cambodia, as elsewhere along the DSR, China's digital influence may not be the principal driver in the decline of internet freedom, but its support has provided the network and knowhow to improve Cambodia's capacity for digital repression. By building the infrastructure now, China is facilitating the hardware to support the additional policy changes underway in Cambodia.

Since 2015, China has provided at least 1,000 CCTV cameras for deployment in Phnom Penh, and in 2021 Cambodian police announced plans to extend this nationwide with China's support. Those familiar with this surveillance system have explained that all information collected is likely processed by the Ministry of Interior command centre at the national police headquarters, which itself was provided by China. Those who spoke with ARTICLE 19 on condition of anonymity stated that they believe the police have received training from Huawei and the Chinese Ministry of Public Security on the management of the surveillance system.

China has also supported information manipulation operations in Cambodia, for example through the Cyber War Team, established to monitor social media to 'protect the government's stance and prestige'. Many claim that Huawei has provided this team with the technical tools to monitor and censor content, and that it receives direct capacity-building support in China.

While the lack of public consultation and transparency in the legislative process, among other factors, makes it impossible to point conclusively to China's direct influence, Cambodia has drafted or enacted a number of internet governance policies that appear to emulate China.

This includes embracing data localisation, real-name identity verification, and increasing control over internet infrastructure, through the Telecommunications Law, DNS Management Law, draft Cybersecurity and Cybercrime Laws, and the Sub-Decree on the establishment of a National Internet Gateway (NIG). In terms of Cambodia's shift toward China-style digital authoritarianism, the NIG is the most emblematic.

Cambodia enacted this NIG Sub-Decree in February 2021. Article 6 requires telecommunications companies and internet service providers to reroute internet traffic through government-controlled and -monitored services 'to prevent and disconnect all network connections that affect national income, security, social order, morality, culture, traditions, and customs'. In addition to blocking online connections, Articles 14 and 16 allow government officials to retain traffic data for a year and issue overbroad penalties for non-compliance.

Sopheap Chak, former executive director of the Cambodian Centre for Human Rights, has observed that 'the proposed NIG mirrors that of the Chinese internet gateway'. In an effort to defend itself, Cambodia has claimed that it conducted an 'extensive study on infrastructure models from different countries around the world'. However, no official has provided clarity on which countries' internet models it studied. One can speculate that the Ministry learned from China.

The government has not disclosed who it is contracting to construct the NIG, but experts in Cambodian civil society believe it is Huawei or ZTE. The lack of transparency is alarming and complicates an effective human rights impact assessment.

In July 2023, Cambodia began the construction of a national data centre under the MPTC, expected to be completed by 2025. The new data centre will contribute necessary infrastructure to the implementation of the NIG. It will be certified Tier IV, the highest level of data centre certification and complexity, beyond the level at which Cambodia currently operates. Again, there has been no public disclosure about whom the MPTC is partnering with for construction.

In a similar effort to rein in internet freedom, Cambodia has put forward a Draft Cybersecurity Law. This draft legislation is part of a concerning trend in the region of masking human rights abuses online with the vocabulary of cybersecurity, which appears to trace its origin to provisions in China. The law is poised to crush digital rights and the exercise of online freedom of expression by creating a framework that would expose every part of society to searches and surveillance and would force private-sector compliance with government orders, while not allowing for any judicial oversight. It introduces a number of measures similar to those that exist in China's ICT law.

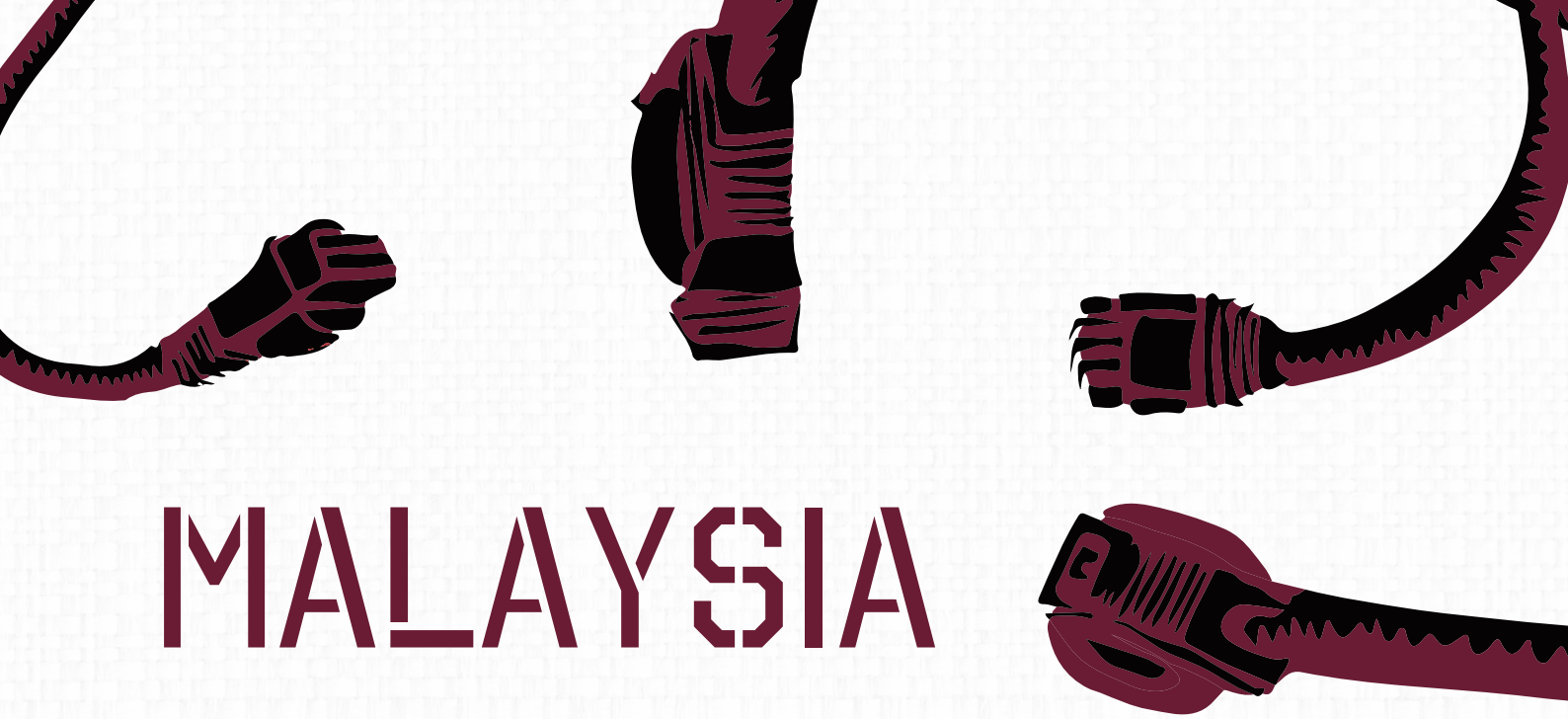
It calls for the creation of a committee under the MPTC, with seemingly limitless jurisdiction over 'any other necessary duties related to cybersecurity'. This committee may appoint cybersecurity inspectors to search and seize evidence, interrogate individuals, and enforce detentions. It may also suspend non-compliant parts of computer systems, which appears to authorise network interference or shutdowns. The law may also be used to mandate forced decryption.

The draft law also establishes jurisdiction over broadly defined 'critical information infrastructure', which, alarmingly, includes the media and conceivably parts of civil society. Article 7 allows the scope to be amended at will by the MPTC to include any provider of 'other essential services', a provision that is subject to abuse. Article 21 further allows for CII to be ordered to 'monitor and examine' a computer or computer system, which amounts to warrantless surveillance.

Furthermore, judicial harassment and new draft laws and regulations are creating a stifling environment for independent media in Cambodia, inhibiting them from investigating and reporting on sensitive matters, not least the matter of cooperation between Cambodia and China. In February 2023, Voice of Democracy, one of the longest-running independent media organisations in the country, which had done investigations in Khmer and English on development and digital cooperation projects between Cambodia and China, was arbitrarily shuttered in reprisal for its reporting on corruption within then-Prime Minister Hun Sen's family. This forced closure was a clear warning to civil society not to cover such off-limits topics.

Likewise, among the concerning provisions of Cambodia's Draft Cybercrime Law, it criminalises 'disinformation' through information technology. It specifies disinformation in vague and overbroad terms as information that is likely to 'diminish public confidence' in the government. As the government has routinely used such accusations against independent media, it is reasonable to expect that if enacted, the law is likely to further punish and criminalise critical reporting and restrict access to information.

These concerns point to not only deteriorating internet freedom but also the shrinking space for independent, investigative coverage of China's digital footprint in Cambodia, where they affect human rights and fundamental freedoms. It will further complicate efforts to document and assess the potential negative impact that China has on internet freedom in the region.



MALAYSIA

Malaysia is home to the second-largest Chinese overseas community in the world, after Thailand. According to the China Index, it is the country tenth-most exposed to China's global influence, and this is most pronounced in the domains of law enforcement and technology. Malaysia is also among the top ten global recipients of BRI support, making relations with China and its digital components common elements of Malaysian political discourse. In early 2023, China's ambassador to Malaysia, Ouyang Yujing,[32] remarked that 'Malaysia–China relations have been at the forefront of ASEAN–China relations' and called for deeper cooperation to accelerate technological innovation and connectivity and the digital economy.

In addition to funding directly from the Chinese Government and state-owned financial institutions such as China Construction Bank, Chinese technology companies such as Huawei and Alibaba Group have made substantial investments in Malaysia. China's state-owned Aerospace and Science Industry Corporation[33] has expressed plans to invest in Malaysia's high-tech drone industry, with Malaysia's Transport Minister in 2022 welcoming investment through the BeiDou Navigation Satellite System.

Huawei and Cyber Security Malaysia (CSM), the national cybersecurity agency under the Ministry of Communications and Digital, have cooperated on technical standards and through Huawei's support for a Cyber Security Malaysia Collaborative Partner programme. Another example is the National Computer Network Emergency Response Technical Team/Coordination Centre of China (CNCERT/CC), noted in the previous chapter. The training cooperation has covered technical skills and, in an effort to influence internet governance, China's approach to cybersecurity policy.

32 欧阳玉靖

33 中国航天科工集团有限公司

Other examples include the 2016 Huawei Customer Solution Integration and Innovation Experience Centre (CSIC) launched in Kuala Lumpur under former Prime Minister Najib Razak and later upgraded in 2021 under Prime Minister Ismail Sabri to design and test technology solutions. Alibaba has also announced plans to establish an Alibaba Cloud Innovation Centre to train some 30,000 Malaysian professionals in high-tech fields.

Huawei has facilitated other 5G-related projects. In December 2021, the Ministry of Communications and Digital launched a 5G Cybersecurity Test Lab, based on an MOU signed earlier that year with Huawei, CSM, and Celcom Axiata (now CelcomDigi). Speaking remotely at the Mobile World Congress 2021 in Shanghai, Malaysia's then-Minister of Communications and Multimedia Saifuddin Abdullah said that the lab would be a model for end-to-end cybersecurity covering 'a comprehensive 5G test bed ecosystem'.

Chinese technology cooperation has also been directed by Malaysian entities, albeit those which are actively targeted by Chinese soft power operations. For example, in 2022 the Malaysia–China Business Council hosted the Malaysia–China Digital Economy Forum, 'to promote mutual technology development and cooperation … between Malaysia and China'. At the event, Ambassador Ouyang Yujing remarked that 'China continues to deepen cooperation with its international partners in the digital economy. China has been actively contributing to international digital governance by getting involved in rules and regulations setting.'

Another example is Kairous Capital, headquartered in Kuala Lumpur, whose mission is 'to invest in Chinese tech companies' and export their 'technology and expertise from China to South-east Asia'. During the Malaysia–China Business Forum held in Beijing in April 2023, Kairous Capital signed two MOUs – with Digital Way Group and China Silk Road Group[34] – to establish the Malaysia–China Digital Cooperation Council and the Malaysia–China Digital Cooperation and Development Fund, worth USD 226.28 million.

While China Silk Road Group is listed as a Hong Kong-registered private company, its Chair Yan Lijin[35] has held a number of positions with government entities, including serving as Chair of the Silk Road International Foundation,[36] a special fund managed by the China Federation of Social Work under the Ministry of Civil Affairs, Co-Chair of the China–Pakistan Economic Corridor Committee, and Chair of the Law and Globalization Research Centre of the National People's Congress, in which capacity he contributed to influencing the government's BRI investment policy. Such partnerships point to the Chinese Government's ongoing strategic oversight of advancing digital cooperation in the region in support of the DSR.

There is also evidence that when soft power and digital diplomacy have failed, China has targeted Malaysian officials and companies who have signalled doubts about the relationship between the two countries, such as with cyberattacks in 2018, 2020, and 2022.

34 中國絲路集團有限公司

35 闫立金

36 丝路国际公益基金

Digital infrastructure

In 2022, Celcom Axiata and DiGi merged to form CelcomDigi, becoming the largest wireless network operator in Malaysia. As of July 2023, the company has confirmed partnerships with both Huawei and ZTE. CelcomDigi is an affiliated brand of the Axiata Group Berhad, which shares ownership with the Norwegian Telenor Group, marking a potential advocacy opening.

Prime Minister Mahathir Mohammed (May 2018–February 2020) supported integrating Chinese technology through the DSR and broader BRI-related projects. Notably, he was granted the highly symbolic role of presenting a speech during the opening ceremony of the 2019 BRI Forum in Beijing. A month later, responding to the US Government's suggestion that the use of Huawei equipment raised national security concerns, he announced that he wanted Malaysia to use Huawei technology 'as much as possible'.

Prime Minister Mahathir Mohammed speaking at the opening ceremony of the Second Belt and Road Forum in Beijing on 26 April 2019. (Photo: Florence Lo/Reuters)

Malaysia appeared to reverse course under Prime Minister Muhyiddin Yassin (March 2020 – August 2021), in a decision that likely had more to do with nationalism than countering China's influence. Yassin's government announced the establishment of the Digital Nasional Berhad (DNB) to create a state-owned agency responsible for 5G spectrum licensing. Malaysia's top four telecommunications firms all agreed to use DNB's state-owned 5G network. In early February 2021, DNB announced that Swedish telecommunications company Ericsson had won its bid to design and build its 5G network, out-competing Huawei and ZTE, along with other vendors Cisco, Nokia, Samsung, Fiberhome, and NEC.

From August 2021 to October 2022, under Prime Minister Ismail Sabri, Malaysia resumed a greater embrace of Chinese technologies and policies. This included an upgrade of the Huawei CSIC, involving not only 5G solutions but also coordination on cloud computing, especially between Huawei and Telekom Malaysia Berhad (TM Technology Services) to develop Alpha Edge, a Malaysian-owned cloud and AI infrastructure focused on data sovereignty. By the end of 2022, 5G coverage in Malaysia had reached 50 per cent. Under Prime Minister Anwar Ibrahim, the government has set a target of 80 per cent coverage by the end of 2024.

Under Prime Minister Ibrahim, Malaysia appears to be reaffirming its adoption of China's approach to digital governance. In late 2022, the Prime Minister called into question the DNB–Ericsson agreement, in part following intense lobbying from Huawei and ZTE to regain a market hold on 5G. In June 2023, Communications Minister Fahmi Fadzil announced that Huawei would roll out a second 5G network to rival Ericsson's.

This change in policy appears influenced by additional soft power persuasion from China. The announcement followed a March state visit in which Prime Minister Ibrahim met with Xi Jinping, Premier Li Qiang, and other high-level Party officials. The Prime Minister again travelled to China in September 2023 for the China–ASEAN Expo and Business and Investment Summit, where he again met with Li Qiang. Following the visit, he noted that Malaysia and China welcomed the development of cooperation under the BRI and agreed to improve cooperation, including among high-tech companies and the digital economy.

Digital economy

The dominant players for online payment applications in the region are Tencent's WeChat Pay and Alibaba Group's Alipay. Alibaba has made major investments in e-commerce platforms in Thailand, Bangladesh, South Korea, Singapore, the Philippines, India, and Pakistan, and has partnered with platforms in Indonesia, Vietnam, and Malaysia. CIMB, Malaysia's second-largest bank, and Kenanga Investment Bank, the largest investment institution in the country, have both signed MOUs with Alibaba Group.

In August 2018, Malaysia granted a licence to Tencent to roll out WeChat Pay for local transactions in Malaysia – the first time Tencent was able to introduce WeChat Pay to markets outside of China. It is now available in 49 countries, including Cambodia, Sri Lanka, Thailand, and Indonesia.

Chinese companies have also invested heavily in other e-commerce platforms in South East Asia. In 2017, Didi Chuxing and SoftBank invested USD 2 billion in Grab, a Singapore-headquartered 'super app' that operates in Malaysia as well as Cambodia, Indonesia, Myanmar, the Philippines, Singapore, Thailand, and Vietnam. Alibaba holds an 80 per cent stake in Lazada, one of the largest e-commerce operators in South East Asia.

In November 2017, the Malaysia Digital Economy Corporation and Alibaba established Malaysia's Digital Free Trade Zone (DFTZ), to develop an internet ecosystem to drive innovation in e-commerce and the digital economy. In November 2021, Alibaba announced that the DFTZ would be its electronic World Trade Platform (eWTP) hub for the South East Asia region. Following its launch, reliance on Lazada and Alipay-integrated Malaysian banks such as Maybank increased. CIMB Group experienced significant growth, and FDI in Malaysia rose. Within months, Chinese companies had invested over USD 295 million in Malaysia. The DFTZ is thus about not only advancing digital economy but also promoting China's influence. The market control of Chinese e-commerce platforms raises concerns over monopolies and data privacy.

Networking authoritarianism

China's digital diplomacy has afforded it an outsized influence in pursuing its digital governance norms in Malaysia, raising concerns about internet freedom. Malaysia has signalled support for China's model of digital governance, for example in an October 2020 joint statement by the foreign ministers of the two countries declaring that they stood 'ready to work together to promote the growth of digital economy and advance global digital governance'.

During the 2022 International Telecommunications Union Plenipotentiary Conference, the Malaysian Ministry of Communications and Multimedia signed an MOU with China's MIIT, outlining cooperation on policy, standards, training, and awareness on cybersecurity. Malaysia's Minister of Communications and Multimedia Annuar Musa remarked that China's sharing of best practice and expertise would improve Malaysia's cybersecurity ecosystem. While the MOU is not publicly available, in the light of China's model of cybersecurity the adoption of such models in Malaysia is alarming, especially considering other signals of the move towards digital repression.

China's digital diplomacy has afforded it an outsized influence in pursuing its digital governance norms in Malaysia, raising concerns about internet freedom.

In one example, in 2018 the Auxiliary Force Sdn Bhd, a company that trains auxiliary police officers, began a partnership with Chinese AI company Yitu Technology,[37] for which the company provided body-worn cameras with facial recognition technology. The dataset of faces was provided by the Malaysian police.

Any partnership with Yitu Technology for law enforcement in Malaysia is concerning in the light of its role in 'human rights violations and abuses in the implementation of China's campaign of repression, mass arbitrary detention, and high-technology surveillance against Uyghurs, Kazakhs, and other members of Muslim minority groups' in the Xinjiang Uyghur Autonomous Region in China, known for techno-authoritarianism. Yitu is listed on the United States Federal Register of prohibited entities, which also includes SenseTime.

Under Prime Minister Mahathir, in 2019 Malaysia signed an agreement to develop a USD 500 million AI park with SenseTime.[38] The MOU, signed between G3 Global Berhad, Malaysia's leading AI company, SenseTime, and China Harbour Engineering Company, a subsidiary of the state-owned China Communications Construction Company,[39] lapsed in 2022 but G3 Global Berhad has expressed continued interest in the partnership. Partnership with SenseTime raises concerns in the light of the company's cooperation with the Chinese police in the past to enhance facial recognition surveillance capabilities, and the fact that it has supplied facial recognition technology for the surveillance and mass internment of Uyghurs and other minorities in China. SenseTime maintains an office in Malaysia

Malaysia has taken steps to crack down on freedom of expression online, especially under the Communications and Multimedia Act (CMA). Since it was adopted in 1998, the CMA has emerged as one of the greatest threats to freedom of expression in Malaysia. Authorities have repeatedly used Section 233 of the law to target online expression, often in conjunction with other laws, such as the Sedition Act, but also at times as a standalone offence. It was reported in early 2023 that 444 cases had been opened for investigation under Section 233 of the CMA between 2020 and 23 January 2023. Approximately 38 cases were prosecuted, 31 cases include convictions, and seven more cases are still under trial. In 2021, the Malaysian Government enacted a 'fake news' law, which criminalised publishing or sharing over social media any 'wholly or partly false' information about the COVID-19 pandemic or the state of emergency then in place. The law was overbroad and risked severe infringing on freedom of expression online. According to Freedom House, the Ministry of Higher Education funded an academic paper to examine China's 'anti-fake news laws' to determine whether Malaysia should emulate the Chinese model. The law was revoked at the end of 2021.

Meanwhile, Malaysia still has no national legislation on the right to information, making it difficult for the media and civil society to access information on, among other things, agreements for digital cooperation with China or other actors.

37 上海依图网络科技有限公司

38 商汤科技

39 中国交通建设

Malaysia's approach to digital sovereignty has also resulted in greater judicial harassment of internet intermediaries and social media platforms. For example, in June 2023 the Malaysian Communications and Multimedia Commission announced its intention to take legal action against Meta for a perceived lack of action to remove allegedly harmful content, such as materials relating to race, royalty, and religion, the so-called 3Rs often used as pretext for censoring expression otherwise protected under international law. This is not to say such efforts are directly influenced by partnership with China, but the parallel with China's model is noteworthy in this instance since it was announced in the same month that Hong Kong authorities attempted to press for a legal injunction against internet intermediaries to stop them providing access to the 'Glory to Hong Kong' protest anthem.

In April 2024, the Malaysian Parliament passed a Cybersecurity Bill that seeks to normalise broad control over internet infrastructure in line with a more authoritarian model of digital governance. Similar to the Cambodia draft noted above, the Malaysian bill alarmingly deems 'communications', and hence media, as 'critical information infrastructure' opening up the potential for disproportionate regulations that could negatively impact freedom of expression and information. It requires prior licensing for a broad range of activities and empowers Malaysian authorities with search and seizure powers not subject to judicial or independent review. Although there doesn't appear to have been any direct link between China and Malaysia during the drafting process, Malaysia's approach to information infrastructure appears to increasingly resemble China's model.

NEPAL

Nepal hosts the largest population of Tibetan refugees outside of India, making the control of the Tibetan community a core priority in China's relationship with the country. In March 2008, months before Beijing was to host the Olympics Games, Tibetans in Lhasa and Kathmandu gathered in peaceful protest to mark 'Tibetan National Uprising Day', the anniversary of the 1959 Tibetan uprising against Chinese occupation. China responded with violence. Police in Nepal also responded with excessive force. The incidents raised international attention on China's persecution of the Tibetan community and the diaspora. A year later, China redoubled development support in Nepal in exchange for assistance in addressing so called 'anti-China or separatist activists' within its borders. China's increasingly dominant position in Nepal has arguably contributed to restrictions on Tibetans' right to freedom of expression and assembly, and to broader deteriorating internet freedom in Nepal.

Since 2014, China has been a major source of FDI in Nepal. In 2020, it accounted for around 71 per cent of all FDI and in 2022, Chinese media reported Chinese investors' commitment to further increasing FDI.

Nepal joined the BRI in 2017, and since then the two countries have collaborated to develop Nepal's transportation and digital infrastructure. In September 2021, Xi Jinping stressed the need for cooperation between Nepal and China to, among other things, 'advance on a priority basis cooperation on … digital economy and connectivity'. In March 2023, Nepali Prime Minister Pushpa Kamal Dahal urged development partners, including China, to support Nepal's aspirations to graduate from Least Developed Country status by 2026. To achieve this, he announced, Nepal would seek to strengthen trade and investment opportunities with China.

People in Nepal have protested against this cooperation and called for the cancellation of BRI projects, concerned about the risks of debt and use of Chinese companies in virtually every project. Moreover, there is anger over proposed infrastructure projects that would displace large numbers of people. Civil society has also expressed concerns in interviews with ARTICLE 19 over China's potential malign influence over Nepal's internet freedom.

Nepal police arrest a Tibetan Buddhist nun protesting the Chinese crackdown in Tibet near the Chinese Embassy in Kathmandu on 5 May 2008. (Photo: Gopal Chitrakar/ Reuters)

Digital infrastructure

State-owned Nepal Telecom (NT), Ncell, and Smartcell – Nepal's three largest telecoms – all use equipment manufactured by Chinese technology companies.

In 2019, NT partnered with China Communication Services or Comservice[40] (CCS) and ZTE to expand its 4G network and improve high-speed internet. CCS supplied equipment procured from Huawei. In 2021, in conversation with ZTE, Ncell's CEO acknowledged that over a decade of partnership, ZTE had met 60 per cent of the company's wireless network needs, and that 'ZTE and Ncell will continue to strengthen the collaboration … to the further development of Nepal's telecommunications industry'. All three of Nepal's major telecoms have contracted with Huawei to upgrade their existing 4G networks to 5G. In February 2023, NT announced the start of its long-anticipated 5G trial. This trial will be conducted only among the company's employees, and it is not yet known when the 5G network will go live for the general public.

In January 2018, the Nepal–China Optical Fibre Link Project began operations, based on an initial agreement between NT and the state-owned China Telecom in 2016. The fibreoptic network connects the two countries, allowing Nepal to purchase internet from Chinese firms and ending its sole dependence on India for internet bandwidth. China's ambassador to Nepal at the time, Yu Hong,[41] commented that the bandwidth project would play a crucial role in enhancing partnership between the countries.

40 中国通信服务股份有限公司

41 于红

China's ongoing economic support through BRI and related digital infrastructure development in Nepal remains predicated on Nepal's ongoing embrace of China's political narratives and willingness to engage in surveillance and persecution of Tibetans in Nepal.

In an interview with Chinese state media outlet China Global Television Network, China Telecom Global General Manager Deng Fiaofeng[42] stated: 'We want to build a grand corridor and a big platform for telecommunications. I'd call this an "information-centred high-speed link" along the Belt and Road routes.'

In addition to network infrastructure development, ZTE and Huawei have taken a lead in developing data storage systems and constructing data centres in Nepal. For example, at the Huawei Connect 2022 conference held on 20 December 2022 in Kathmandu, Nicholas Ma, president of Huawei for Asia-Pacific, affirmed the tech company's support for Nepal's digital economy by agreeing to support the country with cloud and data centre infrastructure, in addition to ensuring digital connectivity.

In February 2023, Ncell announced the launch of its new data centre in Lalitpur. The centre, which, according to Ncell, is the largest in Nepal, cost USD 15.1 million to produce and was constructed in collaboration with Huawei.

42 邓小锋

Tibetans caught between China and Nepal

Since 2008, Nepal has signed a number of security and 'intelligence-sharing' agreements with China, in particular relating to targeting the Tibetan community. Nepal has incrementally embraced a China-style surveillance infrastructure in part to surveil and monitor Tibetans, under direct pressure from China.

As of 2019, the police operated 1,249 CCTV cameras across Nepal, although some have speculated to ARTICLE 19 that many likely do not function. There is a high concentration of CCTV cameras around Buddhist sites, fuelling speculation that Tibetan Buddhists are their main target. According to an internal police study, there is a plan to install more than 21,000 CCTV cameras across the Kathmandu Valley in the coming years. There is some evidence that this surveillance equipment has been provided by China, but procurement records are not public and there is no public reporting beyond speculation.

Pointing to the appearance of China's involvement, one journalist who visited the CCTV control room at the Metropolitan Police headquarters described a room 'dominated by an enormous screen which … beamed text in Chinese that we could not read, headed by the phrase "China–Nepal" in English'.

Tibetans living in Nepal have faced restrictions on their right to freedom of expression, both online and offline. Tibetans in Nepal are also prohibited from advocating for Tibetan independence or greater freedoms. Even reporting on the Dalai Lama in Nepal has at times been restricted. For example, in 2019, under pressure from China's embassy in Kathmandu, Nepal's Minister of Communications and Information Technology ordered an investigation into three journalists with state media agency Rastriya Samachar Samiti who had written about the Dalai Lama. One of the members of the committee formed to investigate the journalists pointed directly to China's influence, telling Radio Free Asia at the time that 'our investigation will be guided by Nepal's relationship with China, by the One-China policy, and by Nepal's foreign policy'.

China's threat to withdraw financial support for failure to control Tibetans has raised concern about China's coercion over Nepali legislation. In mid-2019, Pradeep Yadav, a member of parliament, was handed a six-month suspension after he attended a 'Free Tibet' event co-organised by the International Network of Parliamentarians on Tibet in Latvia. The suspension followed strong objections from the Chinese embassy in Kathmandu.

Tibetans caught between China and Nepal

Later the same year, in October 2019, following a state visit from Xi Jinping, the two countries concluded a number of agreements. A statement released by Nepal's Foreign Ministry outlining the agreements referred to continued implementation of BRI projects and other infrastructure projects, such as fibreoptics, and promised to 'further strengthen cooperation on information and communications for mutual benefit'. It also emphasised continued efforts between the two countries to strengthen cooperation on law enforcement in information exchange.

In September 2023, Nepal's Prime Minister Pushpa Kamal Dahal, in the same meeting with Xi Jinping noted above where he requested China's ongoing development assistance, promised Nepal's 'firm and unshakeable' adherence to the One China policy and position on Tibet. He praised Xi Jinping as a 'visionary global leader and a good friend of all Nepalese people'.

China's ongoing economic support through BRI and related digital infrastructure development in Nepal remains predicated, in part, on Nepal's ongoing embrace of China's political narratives and willingness to engage in surveillance and persecution of Tibetans in Nepal.

Networking authoritarianism

Especially in the targeting of the Tibetan community, some of Nepal's censorship and surveillance efforts have appeared to be in response to China's influence and in part aimed at maintaining economic support.

China has sought to shape Nepal's free flow of information in favour of pro-Beijing narratives. This includes the soft power projection of Chinese-sponsored junkets and training for Nepalese journalists. As one foreign affairs correspondent for the *Kathmandu Post*, Anil Giri, put it, such sponsored events are 'why probably we don't see lots of criticism about China's growing investment in Nepal, China doing business in Nepal and China's growing political clout in Nepal'.

China also exerts sharp power. Soon after Nepal signed up for the BRI, Nepali journalists reported that they had been instructed to avoid covering Tibetan issues. This extended to broader critical coverage of China, and the Chinese embassy in Kathmandu has a history of harassing and threatening Nepali media. In at least one case, this has led to speculation over the killing of a journalist investigating China-backed projects in Nepal.

In early August 2020, Balaram Baniya, an editor with one of Nepal's most widely read newspapers and a frequent critic of Chinese infrastructure and influence in Nepal, was found dead after having vanished a few days earlier. He had reportedly last been seen in police custody. Two months prior to his mysterious death, Balaram had been suspended over a critical story on China's annexation of the village of Rui in Nepal into Chinese-controlled Tibet. Following its publication in June, the Chinese embassy had called on the Nepali Government to issue a statement condemning the article and to demand Balaram retract the piece.

Legislatively, in step with its evolving digital infrastructure pursued through Chinese support, Nepal has passed a number of digital governance laws, some of which do not comply with the country's obligations under international human rights law.

For example, the government uses the 2006 Electronic Transaction Act to silence those critical of the government. A proposed piece of legislation, the Information Technology Bill, would grant the government the authority to censor online content it deems offensive and arrest those who post it. The proposed 2021 Social Media Bill, updated in January 2024, would compel social media companies to register in Nepal or face operational restrictions, and to remove content the state deemed illegal. Such bills point to a growing embrace of a more repressive model of internet governance that privileges digital sovereignty over the protection of human rights and favours localisation and fragmentation over a free, open, interoperable internet.

Emblematic of this shift, in September 2023 Nepal's cabinet approved a National Cybersecurity Policy. Among its most concerning provisions, in a clear echo of a China-style Great Firewall, 'Strategy 11.25' proposes a government-owned intranet and the establishment of an NIG.

ARTICLE 19 has raised alarm over the policy, noting that if Nepal's NIG is modelled on China's or Cambodia's, it would centralise control of all internet traffic in and out of the country through a government-appointed operator, potentially supercharging surveillance and censorship capabilities while leaving open very serious questions about data privacy and protection and the risk of criminal penalties for telecommunications companies. Increasing internet censorship and control in Nepal under a China-style firewall would also run the risk of greater digital repression targeting Tibetans.

THAILAND

Thai Chinese make up the largest overseas Chinese community in the world. The country ranks fourth in the China Index for exposure to China's malign influence, which is most pronounced in the domains of military, law enforcement, and technology cooperation. Thailand has been a long term partner for China. Thai Government officials have lauded cooperation with China as facilitating its digital economy, broader digital infrastructure, and governance. In 2021, then-Minister of Digital Economy and Society (MDES) Chaiwut Thanakamanusorn expressed his hopes for increased collaboration between the Thai Government and Huawei. In 2022, Arthayudh Srisamoot, Thailand's ambassador to China, stated, 'from the installation of 5G stations to smart hospitals and a digital currency trial, these are concrete outcomes from the beneficial cooperation between Thailand and China'.

China has long been the one of the largest sources of FDI in Thailand. In 2022, it accounted for nearly 20 per cent of Thailand's total FDI, with much of it focused on electric vehicles, data centres, electronics, and related digital areas. Some of China's growing investment in Thailand's tech sector has admittedly also been the result of Beijing's recent response to international pressure to shift elements of its supply chain, in part responding to sanctions over information security and human rights abuses. To this end, Thailand has been among the most popular choices, along with Vietnam and to a lesser extent Malaysia and Indonesia, for China's offshoring of its own tech sector.

In addition to FDI, China has been Thailand's largest trading partner for nearly a decade, with the spike in its trade presence arguably coinciding with the 2014 military coup in Thailand. This presence further increased following a 2018 agreement to double bilateral trade in the fields of science and technology, digital, and finance by 2021. Thailand and China have agreed to work closely on cybersecurity, e-commerce, 5G technology, and digital infrastructure, including fibreoptics. Thailand has embraced a number of policies that appear closely aligned with China's digital governance priorities under the DSR. One example is that MDES, which is closely aligned with Chinese tech companies, has been the only Thai ministry attending meetings of the International Telecommunications Union, a forum where China has invested considerable resources to shape technology standards.

The Thailand 4.0 Policy, a holistic framework to promote industrial growth and innovation, covers five groups of technology and targeted industries. While the policy has no doubt been designed to benefit Thailand, it is stark in its apparent emulation of similar policies in China, which is indicative of China's indirect influence. Describing Thailand 4.0 in a 2020 op-ed, Archanun Khohpaiboon, an economics professor at Thammasat University, wrote that 'six out of the ten industries under Thailand 4.0 are similar to those proposed under the Made in China 2025 initiative'. And at a 2023 seminar on Thailand–China relations, China's ambassador to Thailand, Han Zhiqiang,[43] praised Thailand 4.0 for its alignment with the BRI.

In November 2022, during the APEC (Asia-Pacific Economic Cooperation) Summit in Bangkok, the two countries issued a joint statement in which they agreed to 'expand investment in high-tech industries such as … artificial intelligence' and that 'Thailand and China share broad common interests … [and] will explore cooperation under the framework of the Global Security Initiative [A Chinese initiative announced in April 2022 as an effort to position a post-Western security order] and maintain close communication and coordination in addressing … cybersecurity'.

China's support for Thailand's digital infrastructure and governance has taken place amid the gradual adoption of tactics of digital repression in Thailand, especially following the 2014 military coup. As is the case elsewhere, while China's digital infrastructure and governance support and influence may not be the direct source of Thailand's trajectory towards digital authoritarianism, China has happily provided the tools and templates as part of its ongoing partnership.

Digital infrastructure

As a long-time member of the DSR, Thailand has received heavy investment from the Chinese Government and technology companies to develop its digital infrastructure, supporting the advanced development of Thailand's 5G networks. China has also been active in developing fibreoptic and submarine cable connectivity in Thailand.

At the end of 2022, over 85 per cent of Thailand's population had access to 5G coverage. Much of the infrastructure that allowed this was built by, or in collaboration with, Chinese companies.

In February 2019, Thailand launched Huawei's first 5G testbed in South East Asia, in spite of US warnings over Huawei surveillance risks. Again, as a reminder that China is not the only influence on digital repression, it is worth acknowledging that Thailand has purchased surveillance equipment from other countries, including the Pegasus spyware from the Israeli NSO Group, to target human rights defenders.

In 2020, Thailand's Advanced Info Service (AIS), the largest mobile operator in the country, became the first company to receive spectrum licences to launch a 5G network nationwide. AIS had earlier signed an MOU with Huawei to build the necessary infrastructure. By the end of 2022, half of all 5G users in the country used AIS's 5G network.

43 韩志强

Thailand's True Corporation, through its partnership with ZTE, also provides 5G service. In 2014, Chinese state-owned China Mobile purchased an 18 per cent stake in True Corporation, but it has since sold off shares, leaving it with slightly less than an 8 per cent stake in the Thai company as of March 2023 – still a significant hold on a major telecommunications provider in Thailand. In early 2023, True Corporation completed its planned merger with DTAC, a subsidiary of the Norwegian Telenor Group – the largest telecom merger in South East Asia by value.

At the June 2022 Thailand 5G Summit, then-Prime Minister Prayuth Chan-o-cha announced the Thailand 5G Alliance, a public–private partnership between Huawei, AIS, and True Corp, as well as the National Broadcast Telecommunications Commission (NBTC), the Federation of Thai Industries, the Office of the Digital Economy and Society Commission, the Thai IoT Association, and the Telecommunications Association of Thailand. The alliance empowers MDES to develop frameworks to promote 5G and manage the necessary infrastructure.

Similarly, in September 2022, AIS signed a strategic partnership MOU with ZTE to support 5G digital infrastructure through a 5G Innovation Centre. They agreed to upgrade Thailand's 5G network, enhance capabilities under the Thailand 4.0 Policy, and deliver a range of other 5G services.

As with other critical infrastructure, the data centre market in Thailand is experiencing rapid investment and is expected to grow steadily for at least the next five years. Chinese tech giants Tencent, Huawei, and Alibaba all have data centres in Thailand. In addition, several new entrants, including Chinese firms OneAsia Network [44] and Chindata Group,[45] have recently established data centres in the country.

Fibreoptic and submarine systems

China has supported Thailand's connectivity through fibreoptic and submarine cable systems. As elsewhere, China's stated focus on gaining dominance in submarine infrastructure foreshadows the potential for China to maliciously exert or opportunistically export the tools for greater information control to countries relying on fibreoptic cable systems under China's purview. Of the eight submarine cables currently landing in Thailand, more than half are at least partly Chinese owned, such as AAE-1 mentioned above.

44 亚洲脉络

45 秦淮数据集团

In June 2020, Thailand's state-owned telecommunications infrastructure company CAT Telecom announced that the Asia Direct Cable Consortium (ADC), of which it is a member alongside China Telecom, China Unicom, and others, planned to build an advanced 9,400 km submarine fibreoptic line to connect Thailand to China, Japan, the Philippines, Singapore, and Vietnam. Then-CAT Telecom president Colonel Sanpachai Huvanandana expressed aspirations that the high-capacity cable would support Thailand's plans for advanced technologies including 5G, AI, cloud services, and smart cities, which are all bandwidth intensive. At the time of writing, the cable has landed in Vietnam and Hong Kong but has not yet reached Thailand. In 2021, CAT Telecom and Telecom of Thailand merged, becoming the National Telecom Public Company Limited (NT).

Other projects include the South East Asia Hainan–Hong Kong Express Cable System (SEA-H2X) to connect Hong Kong, China, the Philippines, Malaysia, Singapore, and Thailand. At 160 terabits per second, SEA-H2X will support higher bandwidth than the ADC, further supporting the adoption of big data technologies and capabilities for advanced surveillance and internet controls. Admittedly, the new cable's capacity would still lag behind that of Google's transatlantic Dunant submarine cable, which supports upwards of 250 terabits per second.

The consortium behind SEA-H2X is made up of China Mobile, China Unicom, Malaysia's PPTelecom, and the Philippines' Converge ICT Solutions. The cable is being constructed by HMN Technologies, the company which resulted from the Huawei Marine Networks rebranding noted above. SEA-H2X is slated to go online in 2024.

BeiDou Navigation Satellite System

In 2013, Thailand became BeiDou's first overseas partner. Under the agreement, China agreed to build a national remote sensing system for Thailand as well as a satellite ground station and industrial park for the development and production of BeiDou receivers for sale in South East Asia. By August 2022, China's State Council was reporting more than 120 countries using the BeiDou-3 satellite system.

While China has invested in the development of its own satellite internet technologies and applied to the International Telecommunications Union for major spectrum allocation, to date it is not involved in internet infrastructure in Thailand. According to Thai experts, the main cooperation between BeiDou and Thailand thus far has been for geo-information. This could still raise Thailand's surveillance capabilities, as noted in the Cambodia case study.

Digital economy

Thailand's e-commerce market is expected to grow to nearly USD 120 billion by 2025, five times larger than in 2022. In addition to support from the Chinese state, technology companies Ant Group, formerly Ant Financial and a subsidiary of Alibaba Group, and Tencent have invested heavily in Thailand's e-commerce market, providing funding, infrastructure, and technical expertise to develop Thailand's digital economy. As with other countries receiving considerable investment from China in the development of their digital economies, there is a risk of becoming overly dependent on China and of vulnerability to influence in exchange for ongoing investment and economic development.

AliPay has been in use in Thailand since 2015, and in 2016 Ant Group bought a 20 per cent stake in Thai e-payment company Ascent Money with the option to buy an additional 10 per cent. As part of the deal, Ant Group sent a team to help Ascend to develop its digital platform. In return, Ascend Money helped to open doors for Ant Group in Thailand. Ascend Money developed the mobile payments app TrueMoney, the most popular financial application in Thailand, with a 53 per cent market share. In September 2021, Ascend Money became Thailand's first fintech unicorn with a valuation of USD 1.5 billion. Tencent's WeChat Pay has also been operating in Thailand since 2016, beginning with mobile third-party payment services for Chinese tourists. WeChat Pay and AliPay are now widely available across the country, supported by Thai banks such as Bangkok Bank and the state-owned Krungthai Bank.

Ant Group's presence in Thailand is likely to further grow following additional collaboration with the Tourism Authority of Thailand. Such partnerships and increasing digital economy presence carry with them access to major troves of data, which under Chinese law Ant Group is required to store in servers in China accessible to Chinese authorities. This raises concerns over the right to privacy not only for Thai nationals relying on Chinese e-commerce platforms but also for Chinese tourists travelling to Thailand and others using these platforms.

The Chinese Government's embrace of a digital currency and its efforts to position its own cross-border interbank payment system is likely informed by a desire to limit the impact of accountability mechanisms such as international sanctions under the Global Magnitsky Human Rights Accountability Act, which relies on SWIFT.

The governments of Thailand and China have worked together to promote e-commerce between the two countries. On 19 November 2022, they signed an MOU that reportedly outlines that the two countries 'will establish an e-commerce cooperation mechanism and promote high-quality product trade between them'. Furthermore, on 29 September 2022, China, Thailand, Hong Kong, and the United Arab Emirates completed a central bank digital currency trial focused on cross-border transactions using China's digital yuan. This is significant in that the Chinese Government's embrace of a digital currency and its efforts to position its own cross-border interbank payment system is likely informed by a desire to forestall accountability under international financial sanctions, such as the Global Magnitsky Human Rights Accountability Act, which relies on SWIFT. While recent accounts put China well behind establishing a truly competitive alternative system, the more countries like Thailand become integrated into China's alternative digital economy, the more it may be able to evade accountability for human rights abuses such as those in Xinjiang.

A demonstration of the Megvii facial recognition system at a media tour in Beijing on 10 February 2022. (Photo: Florence Lo/Reuters)

Networking authoritarianism

China's role in the deterioration of internet freedom and other digital rights in Thailand does not exist in a vacuum. As mentioned above, Thailand has also purchased repressive surveillance tools like Pegasus from the Israeli NSO Group, and it has met with Russia's facial recognition company NtechLab, sanctioned by the European Union, to discuss smart city projects. Thailand's de-democratisation process began before the DSR, but China's involvement has provided inspiration for the creep of digital authoritarianism in the country.

Surveillance in the deep south

Thailand has developed a powerful surveillance apparatus, including the use of facial recognition and biometric data, in the Malay Muslim-majority southern border provinces, where a nearly two-decade-long insurgency has claimed over 7,000 mostly civilian lives, with widespread reports of enforced disappearances, extrajudicial killings, torture, and arbitrary detention by Internal Security Operations Command (ISOC) forces.

While the conflict and its associated human rights abuses predate any DSR partnerships, in recent years Thailand has undoubtedly adopted increasingly China-style techno-authoritarian security measures in the deep south, leading to comparisons to China's system of repression in the Xinjiang Uyghur Autonomous Region (XUAR).

In 2020, the UN Special Rapporteur on freedom of religion or belief acknowledged reports of surveillance targeting Muslim groups, including the use of AI. While Thai authorities have denied the use of AI-enabled facial recognition surveillance systems in the deep south, they have experimented with it elsewhere in the country and have publicly rolled out other policies in the deep south contrary to international human rights law.

In 2019, ISOC and Thailand Broadcasting and Telecommunications Commission (NBTC) issued a mandatory identification policy for all mobile subscribers in the deep south to re-register SIM cards with fingerprint and facial recognition data, in a discriminatory policy targeting the region's ethnic and religious minorities. Anyone failing to comply by mid-2020 risked having their mobile services suspended. The policy amounted to arbitrary network interference akin to targeted internet shutdowns based on an individual's identity. Elsewhere in the country, SIM card registration requires only the customer's ID or passport. Such privacy-invasive identity verification requirements for mobile subscribers in the deep south is part of the larger system of surveillance imposed over the region's minorities.

For example, Cross Cultural Foundation, a Thai human rights organisation that works in the deep south, has documented the widespread forced collection of DNA targeting Malay Muslims, often carried out at checkpoints or during search operations. This practice has also been criticised by the United Nations Committee on the Elimination of Racial Discrimination.

Concerns that Thailand may intensify the use of more advanced facial recognition in the deep south are not mere speculation. In 2020, then-Deputy Prime Minister General Prawit Wongsuwan, in a visit to the region, instructed local police to accelerate the advance of CCTV surveillance systems with enhanced AI technologies.

Surveillance in the deep south

While there is no evidence that Thailand has directly modelled its systematic surveillance of Malay Muslim minorities in the deep south on China's persecution of Uyghurs, Kazakhs, and other Muslim minorities in XUAR, there are mounting similarities. While establishing concrete influence is hamstrung by the lack of transparency, there are indications that point to China's role in at least part of Thailand's developing surveillance infrastructure.

Since around 2018, the Chinese AI company Megvii Technology Limited (旷视), which counts Alibaba Group among its largest shareholders, has been expanding in South East Asia, opening a distributor in Thailand and marketing its Face++ facial recognition platform to the police in Thailand. The company has also explored operations in Malaysia. Megvii is among the AI companies supplying technologies to China's Ministry of Public Security, and among other concerns it has been linked, alongside Huawei, with facial recognition systems used to profile Uyghurs.

In the light of its role in biometric surveillance and tracking of ethnic and religious minorities in China, the US Commerce, Treasury, and Defence Departments have imposed varied sanctions on Megvii. The 2019 inclusion on the Commerce Department Entity List entailed heightened export restrictions, while in 2021 the Treasury Department prohibited US citizens from purchasing or selling securities related to the company. In January 2023, the US Defence Department added Megvii to its list of Chinese companies that it says work directly with China's military.

In its listing announcement, in 2021 the Treasury Department noted that Megvii 'operates or has operated in the surveillance technology sector of the economy of the PRC … has developed and created customised software designed to conduct surveillance activities of ethnic minorities, including Uyghurs … Megvii has exported its facial recognition software to third countries, including Thailand and Pakistan.'

Thailand has also been complicit in the persecution of Uyghurs within its own territory. In 2014, several hundred Uyghur refugees fleeing China arriving in Thailand's southern Songkhla province in the hope of registering with the UN Refugee Agency were detained by Thai authorities. Some 109, mostly men and boys, were forcibly returned to China, in a blatant violation of the principle of non-refoulement and Thailand's obligations under international law, while Thailand sent some 173 people, mostly women and children, to Turkey. To date, some 50 Uyghurs remain arbitrarily detained in Thailand. In 2023, two Uyghur detainees died in immigration detention in Bangkok, raising fears of serious mistreatment rising to the level of torture. The continued detention of Uyghur refugees in Thailand represents a serious test of relations between Thailand, China, the United States, and others.

China's vision of digital sovereignty has also received consideration in Thailand, in suggestions for the establishment of its own internet firewall.

Since the 2014 military coup, Thailand has increasingly restricted internet freedom through the embrace of digital authoritarian tactics at times similar to China's vision of internet governance.

Thailand first enacted the Computer-Related Crimes Act (CCA) in 2007, but 2017 amendments came after Thailand had joined the DSR and embraced China's support in developing its digital infrastructure and governance. In response to the amendments, parts of Thai civil society alleged that the CCA had been 'inspired and informed – if not enabled – by China's "Great Firewall" and other domestic digital policies and practices'.

The CCA, as ARTICLE 19 has previously articulated, allows the government 'nearly unfettered authority to restrict free speech, engage in surveillance, conduct warrantless searches of personal data, and undermine freedoms to utilise encryption and anonymity' and is generally rife with broad powers that are open to abuse and likely to punish legitimate expression.

In 2016, Thailand established the Ministry of Digital Economy and Society, previously the Ministry of Information and Communication Technology. It has been a driving force in tightening digital cooperation between China and Thailand. Under the CCA, in particular, Thailand's MDES is empowered with broad discretion to act, often amounting to censorship powers, and has flirted more overtly with imposing a China-style firewall.

China's vision of digital sovereignty has also received consideration in Thailand, in suggestions for the establishment of its own internet firewall. First proposed a little over a year after the 2014 military coup, in August 2015 under then-Prime Minister Prayut Chan-o-cha, the government approved a plan instructing the Ministry of Information and Communication Technology to establish a Single Internet Gateway 'as a tool to control access … and the influx of information from abroad'. Amid widespread opposition, with some dubbing it the 'Great Firewall of Thailand', in October 2015 the policy was scrapped.

In early 2022, Chaiwut Thanakamanusorn, the former MDES Minister mentioned at the start of this section for his embrace of Huawei, raised the possibility of resuming plans to establish a national internet gateway and of amending the CCA 'to better control the flow of illegal information online' – or in other words, to better control and restrict access to online content from outside the country.

While his successor, Prasert Jantararuangtong, has not publicly taken a position on the NIG conversation, he has not abandoned the MDES's embrace of Chinese technology companies. In September 2023, attending the Huawei Connect forum in Shanghai, the new Minister noted that he had met with more than 20 Chinese tech companies which he had invited to open offices in Thailand to generate cooperation in new technologies.

One area where the two countries have increasingly struck partnerships is on cybersecurity. In 2019, the military-appointed parliament unanimously passed Thailand's Cybersecurity Act, which contains a number of provisions contravening Thailand's international human rights obligations. Again, while it is not necessarily modelled on China's law, it is similar in its focus on state control over human rights safeguards.

The 'Cybersecurity Act fortified the State's online monitoring and mass surveillance powers'. It grants the authorities further sweeping powers to monitor internet traffic, access data and networks, and copy or seize information or devices without court orders in the vaguely defined interests of 'national security' or to protect 'critical information infrastructure', which is not defined. It goes so far as to establish that in critical situations, the National Security Council may override other procedures within its own jurisdiction. It empowers the National Cybersecurity Committee to summon individuals and enter private property without judicial oversight in the interest of vaguely defined 'serious cyber threats'.

Thailand and China have entered several opaque partnership agreements on strengthening cooperation on cybersecurity. In July 2022, the Thai Ministry of Foreign Affairs and MDES signed an MOU to enhance cybersecurity collaboration between the Thai National Cyber Security Agency and the Cyberspace Administration of China. The agreement reportedly focuses on the exchange of information, skills, experience, and technical innovation. The announcement was published in the *Royal Gazette*. In late July, despite ARTICLE 19's efforts through an intermediary to obtain more information about the agreement, Thailand's Ministry of Foreign Affairs denied the existence of the MOU. In the light of China's approach to cybersecurity in particular, the lack of transparency about this collaboration is problematic.

In August 2023, Thailand's then-Deputy Prime Minister Prawit Wongsuwon hosted China's Vice Minister of Public Security, Xu Ganlu,[46] to discuss cooperation on transnational cybercrime and related law enforcement coordination. Hinting at China's potential impact beyond digital affairs, the Prime Minister remarked that Thailand's foreign policies have 'always been strongly influenced by Thai–Chinese diplomatic relationships'.

46 许甘露

THE DIGITAL SILK ROAD FACILITATES BUSINESS OPPORTUNITIES FOR SANCTIONED CHINESE TECHNOLOGY COMPANIES

THAILAND

Since around 2018, **Megvii Technology Limited (旷视)**, which counts Alibaba Group among its largest shareholders, has been expanding in South East Asia. In 2019, Megvii and Thailand-based NVK Co. Ltd., which specializes in the distribution and service of computer systems, established a partnership on facial recognition and smart city technology. Megvii is listed as a prohibited entity by the US Government because it 'operates or has operated in the surveillance technology sector of the economy of the PRC… [and] has developed and created customized software designed to conduct surveillance activities of ethnic minorities, including Uyghurs'.

CAMBODIA

Since 2017, Cambodian Fibreoptic Cable Network (CFOCN) has managed the Asia–Africa–Europe 1 submarine cable landing station in Sihanoukville, one of the only two currently operational submarine cable lines providing broadband to Cambodia, and a likely crucial node in implementing designs on a National Internet Gateway. CFOCN is a subsidiary of the Singapore-based HyalRoute Communication Group, whose major shareholder **Shenzhen Kuang-Chi Group (深圳光启高等理工研究院)**, since 2020, has been on the US restricted entities list over 'wide-scale human rights abuses within China' and for having 'facilitated the export of items by China that aid repressive regimes around the world'.

MALAYSIA

In 2018, Malaysia's Auxiliary Force Sdn. Bhd., a member of the Royal Malaysian Police Cooperative, announced a partnership with **Yitu Technology (上海依图网络科技有限公司)** to provide body-worn cameras equipped with facial recognition technology. While the project has not been fully rolled out, the partnership raises human rights concerns. Since 2019, the US Government has listed Yitu as a prohibited entity for its role in 'human rights violations and abuses in the implementation of China's campaign of repression, mass arbitrary detention, and high-technology surveillance against Uyghurs, Kazakhs, and other members of Muslim minority groups' in China.

In 2019, under former Prime Minister Mahathir Mohamad, Malaysia's leading AI company G3 Global Berhad signed an MOU with China's **SenseTime (商汤科技)** and China Harbour Engineering Company to develop an artificial intelligence park. The MOU lapsed in 2022 but G3 Global Berhad has expressed continued interest in the partnership with SenseTime, despite the fact the US Government lists the company as a prohibited entity for providing Chinese police with facial-recognition technology for the surveillance and mass internment of Uyghurs, Kazakhs, and other minorities in China.

Taiwan: Another way?

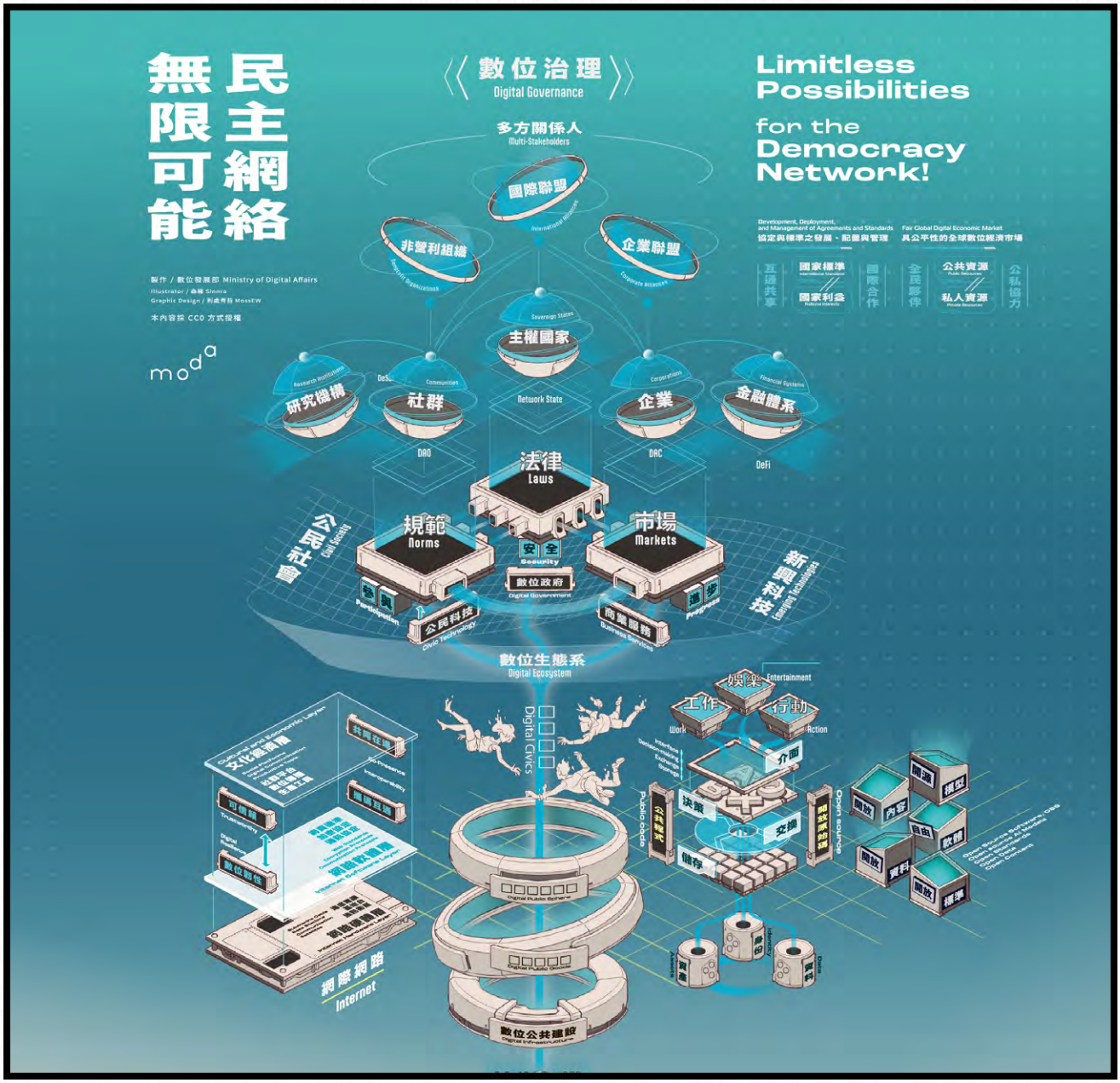
Contrary to China's approach to infrastructure and digital governance, Taiwan's model is based on radical transparency and civic engagement. While not the focus of this report, Taiwan offers a positive example of digital democracy as a counterweight to the digital authoritarianism being promoted by China through the DSR. We briefly provide the example of Taiwan's alternative digital governance practices here as an invitation for further research and advocacy.

In 2019, Taiwan's Executive Yuan approved a Smart Government Action Plan based on three core goals: to promote open and transparent data, to link governance networks to optimise decision-making, and to innovate smart government services. In 2020, the National Development Council followed up with the launch of a Digital Government Program 2.0 of Taiwan (2021–2025).

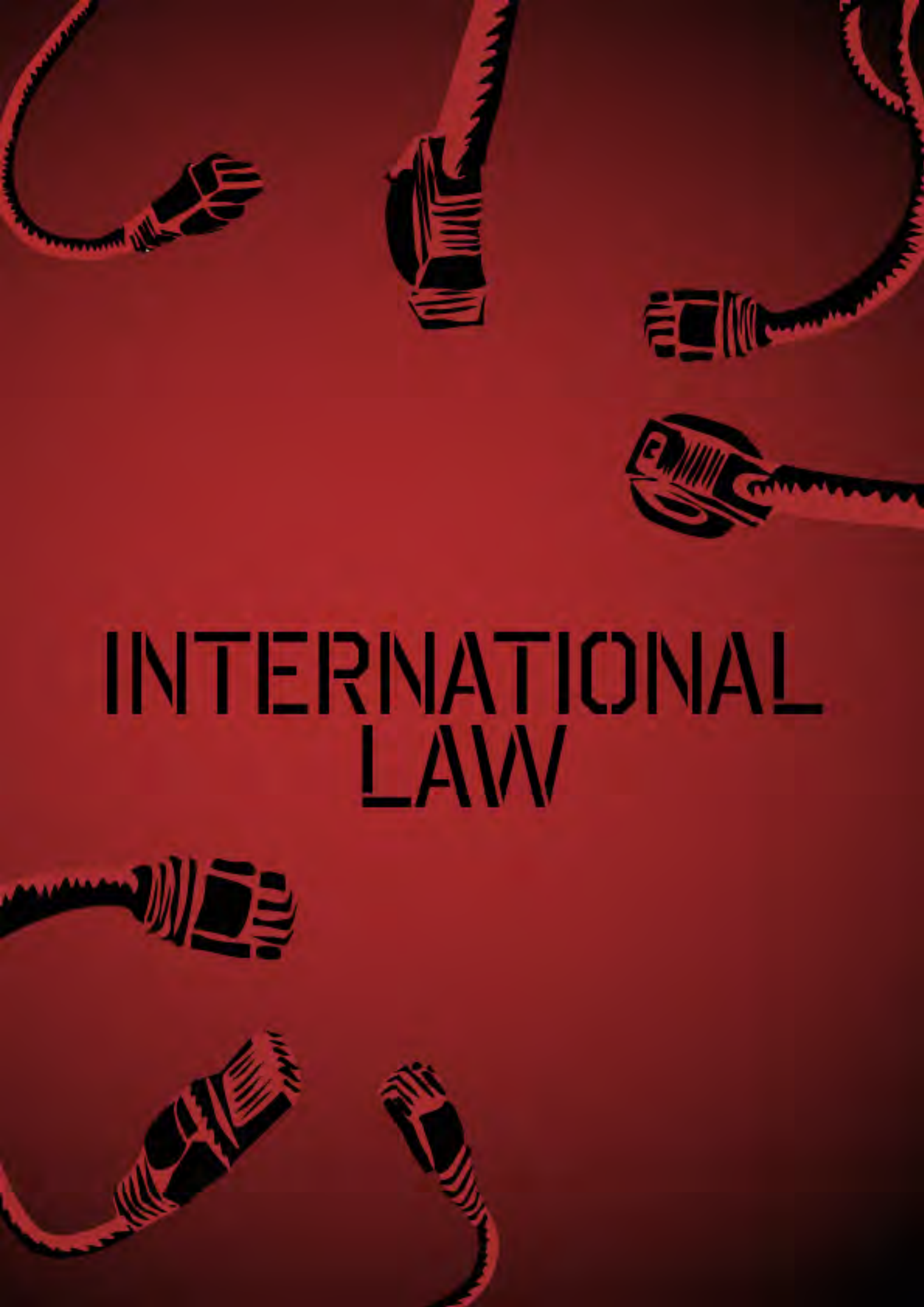
In stark contrast to China's approach to the value of big data in digital governance as a tool for social control, Taiwan's digital governance programme focuses its data-driven approach on enhancing civic engagement, noting that 'through Big Data, the needs of the public are collected; government openness and transparency are promoted through Open Data … to provide services that fully meet people's needs'. This emphasis on open data and open-source technology is foundational to Taiwan's approach and critical to an understanding of building digital public infrastructure that serves democratic and rights-based aims. By putting transparency first and committing to public participation, this model offers a more rights-based approach to the design, development, and deployment of digital infrastructure and digital governance norms.

Taiwan's commitment to these principles is further enumerated in its Open Government National Action Plan (2021–2024), which lists the promotion of 'open data and freedom of information' first among five categories of commitment. It lays out a path to radical transparency and open-source technology, acknowledging the importance of multistakeholderism and harnessing technology to transform public opinion into creative policies to deepen democratic literacy. This is continued in the Open Parliament Action Plan (2021–2024), the objectives of which are likewise transparency, openness, participation, digitisation, and literacy.

Through such policies, Taiwan is demonstrating its commitment to open information and digital governance, and promoting a collaborative approach between civil society, the tech sector, and government in the drafting and implementation phases towards developing a rights-based model of digital public infrastructure. This open data, open governance, multistakeholder approach has been developed in part through the bottom-up initiatives of Taiwan's civic tech community, such as the Open Culture Foundation and g0v (pronounced Gov Zero).



Taiwan's vision for digital democracy.
(Photo: Department of Democracy Network, Ministry of Digital Affairs Taiwan)


INTERNATIONAL
LAW

International Human Rights Law

Right to freedom of expression and access to information

The right to freedom of expression is protected under international human rights law, in particular Article 19 of the Universal Declaration of Human Rights (UDHR), and given force in Article 19 of the International Covenant on Civil and Political Rights (ICCPR).

General Comment No. 34, adopted by the UN Human Rights Committee in 2011, explicitly recognises that Article 19 of the ICCPR protects all forms of expression and the means of their dissemination, including all forms of electronic and internet-based modes of expression. State parties to the ICCPR are also required to consider the extent to which developments in information technology, such as internet and mobile-based electronic information dissemination systems, have dramatically changed communication practices around the world.

The UN Human Rights Council affirmed in 2018 that the 'same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice'.

In a 2019 Joint Declaration on challenges to freedom of expression in the next decade, the four special mandate holders on the right to freedom of expression reiterated that 'the exercise of freedom of expression requires a digital infrastructure that is robust, universal and regulated in a way that maintains it as a free, accessible and open space for all stakeholders'. States should 'recognise the right to access and use the Internet as a human right as an essential condition for the exercise of the right to freedom of expression', 'refrain from imposing Internet or telecommunications network disruptions and shutdowns', and 'avoid measures that risk fragmenting the Internet and limiting access to the global Internet'.

While the right to freedom of expression is a fundamental right, it is not absolute. Freedom of expression and access to information may only be limited under strict circumstances. Restrictions must be:

> **Provided for by law:** Restriction must be formulated with sufficient precision so that any individual may regulate their conduct accordingly. Vague or overbroad restrictions are never permissible.
>
> **In pursuit of a legitimate aim:** Legitimate aims for restricting the freedom of expression are expressed in Article 19(3)(a) and (b) of the ICCPR. Restrictions are permitted only for (a) respect of the rights or reputation of others and (b) the protection of national security or of public order (ordre public), or of public health or morals. International norms hold that where rights are restricted based on the justification of national security they are illegitimate unless their genuine purpose and effect is to protect country's existence or territorial integrity against the threat of force, and as such, restrictions may never be

permitted where they are intended rather to protect the government from embarrassment or the exposure of information. This is further elaborated in the Johannesburg Principles on National Security, Freedom of Expression and Access to Information and the Global Principles on National Security and the Right to Information (Tshwane Principles).

Necessary and proportionate: Restrictions must be based on a direct and immediate connection between the expression and the protected interest. Proportionality requires that they must be not overbroad but specific, tailored, and the least intrusive means capable of achieving the same limited result.

The right to information is likewise recognised under Article 19 of the UDHR and ICCPR, including the right to seek and receive information. General Comment No. 34 holds that states should proactively disseminate information in the public interest and ensure that access is 'easy, prompt, effective and practical'. It enjoins states to enact 'necessary procedures' such as right to information legislation. ARTICLE 19's Principles on Right to Information Legislation hold that any such legislation should be guided by the principle of maximum disclosure. The UN Special Rapporteur on the freedom of expression has reiterated that internet access is a leading prerequisite for the enjoyment of the freedom of expression and access to information. Finally, access to information laws contribute to effective business practices. Public bodies hold a great deal of information, much of which relates to matters useful for private enterprises. Open data facilitates both accountability and encourages innovation and economic opportunity.

Right to privacy

Similarly, the right to privacy, particularly relevant in the context of protection against arbitrary surveillance, is enshrined in Article 12 of the UDHR, and Article 17 of the ICCPR holds that 'no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence' and that 'everyone has the right to the protection of the law against such interference or attacks'.

The UN Human Rights Committee, in its General Comment No. 16 on the Right to Privacy, explains that 'even with regard to interferences that conform to [the ICCPR], relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted'.

The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has argued that restrictions of the right to privacy under Article 17 should be interpreted as subject to the three-part test of legality, legitimacy, and necessity and proportionality.

In the 2018 Right to Privacy in the Digital Age report presented to the UN Human Rights Council, the High Commissioner for Human Rights recommended that all states adopt strong and comprehensive privacy legislation, including on data privacy, in accordance with international human rights law covering safeguards, oversight, and remedy.

The protection of anonymity, furthermore, is a critical element for the enjoyment of the right to freedom of expression, the right privacy, and other human rights. A fundamental feature enabling anonymity online is encryption.

United Nations Guiding Principles on Business and Human Rights

The United Nations Guiding Principles on Business and Human Rights (UNGP) were endorsed by the UN Human Rights Council in 2011 as a set of guidelines for states and companies to limit and address the adverse human rights impacts associated with business operations, including business actors within digital infrastructure and internet governance.

As applies specifically to states benefitting from China's digital infrastructure development projects or internet governance support, the UNGPs reiterate that states must prevent human rights abuses within their territory by third parties, including businesses. This imposes a requirement to 'prevent, investigate, punish and redress such abuses'. States must also ensure that laws and policies do not constrain but rather enable business respect for human rights.

This applies to both private-sector actors and state-owned or -controlled enterprises, of particular relevance to the opaque relationship between the CCP and ostensibly private Chinese technology companies. The UNGPs hold that states should take additional measures to protect against human rights abuses by state-owned or -controlled enterprises, or those which receive significant support from the state.

States should furthermore ensure oversight of all business enterprises with which they enter into contracts to provide services that may impact human rights.

The UNGPs' Pillar II outlines the corporate responsibility to respect human rights. Companies should establish 'a human rights due diligence process to identify, prevent, mitigate and account for how they address their impacts on human rights'.

The Guiding Principles also introduce a heightened human rights due diligence process based on the concept of proportionality: the higher the risk, the more complex the risk assessment. Although initially envisioned for situations of armed conflict, this concept could be extended, for example to ensure an expectation of higher standards in situations where companies are operating within or with support from authoritarian states where gross human rights abuses are widespread or systematic, or where their technologies are built on or used to perpetuate these gross human rights abuses and criminal acts under international law.

The UNGPs conclude with Pillar III's emphasis on access to remedy, holding that states must ensure that when abuses occur, those affected have access to an effective remedy.

While the UNGPs are voluntary, they have increasingly been normalised in the ICT sector through the adoption of corporate human rights policies. Some companies, such as Meta, have explicitly pointed to the human rights concerns around operation in Asia as part of the impetus in developing their human rights policies in line with UNGP duties.

Human rights and internet infrastructure

Internet infrastructure consists of the physical technologies that make up the internet and the logical technologies that govern how data moves across them. The design, development, and deployment of these technologies determines the extent to which the internet enables or threatens the full expression of human rights both online and offline. These technologies are often under-scrutinised, despite their implications for who can access and share content and how individuals and communities associate and represent themselves online.

However, there has been increasing recognition of the impact internet infrastructure has on human rights. In his 2017 report to the UN Human Rights Council, David Kaye, the then-UN Special Rapporteur on the protection and promotion of the right to freedom of expression, recognised the impacts that internet infrastructure providers such as internet service providers, internet exchange points, content delivery networks, and network equipment vendors have on human rights, including freedom of expression, particularly in the context of surveillance and censorship.

In their 2019 Joint Declaration on challenges to freedom of expression in the next decade, the four special mandate holders on the freedom of expression noted that in order to create enabling environments for the protection and promotion of the freedom of expression, states should, among other actions, develop rules on transparency of ownership of the media and telecommunications infrastructure, and that the freedom of expression requires a digital infrastructure that is 'robust, universal and regulated in a way that maintains it as a free, accessible and open space for all stakeholders'. States must ensure that developments, including but not limited to transitions to 5G and the expansion of the IoT, 'respect human rights, particularly through robust human rights due diligence in the development of infrastructure, network service, interoperability, and privacy-by-design'.

In its 2023 report to the UN Human Rights Council, Human Rights and Technical Standard-Setting Processes for New and Emerging Digital Technologies, the Office of the United Nations High Commissioner for Human Rights recommended that states 'refrain from and prevent the development of standards that could foreseeably facilitate human rights violations and abuses when participating in standard-setting processes'; that 'standards-setting organisations review their operations in order to assess how they affect the enjoyment of human rights'; and that technology vendors 'meet their responsibility to respect human rights and strive for coherence of their engagement in standard-setting processes and their commitment to human rights when participating in standard developing processes'.

RECOMMENDATIONS

Recommendations to the Government of Cambodia

- Repeal the Sub-Decree on the Establishment of a National Internet Gateway and take no further steps to implement a China-style firewall and related measures leading to internet fragmentation.
- Make publicly available the contents of cooperation agreements and MOUs signed in relation to digital infrastructure or internet governance cooperation between Cambodia and China and consider establishing a national transparency database for easy access to all such agreements.
- Ensure open, public consultation on all digital infrastructure and governance policymaking, especially as relates to actual or planned partnerships with China or Chinese technology companies.
- Amend or repeal Cybercrime, Cybersecurity, DNS Management, Data Protection, and other internet governance policies in line with Cambodia's obligations under international human rights law.
- End persecution or threats of reprisal against independent journalists and other civil society for investigation or expression relating to China in Cambodia.

Recommendations to the Government of Malaysia

- Make publicly available the contents of cooperation agreements and MOUs signed in relation to digital infrastructure or governance cooperation between Malaysia and China, and consider establishing a national transparency database for easy access to all such agreements.

- Conclude the drafting and consultation process for a Right to Information Law in Malaysia; ensure all provisions are in line with international human rights standards; disseminate information about the law; and begin effective implementation, including by supporting individuals receiving access to information related to partnerships with China and Chinese companies.

- Conduct HRIAs on public–private partnerships and commit to ending any partnerships with Chinese institutions or individuals with documented records of exporting technologies used in the commission of human rights abuses, including those on existing sanctions or special entities lists such as Yitu and SenseTime.

- Commit to open, transparent procurement in all current and future development of 5G and other digital infrastructure and ensure safeguards are in place to prevent foreign influence or non-competitive practices that may privilege certain actors, i.e. Huawei.

- End arbitrary restrictions on internet intermediaries and reverse trend towards digital sovereignty in favour of commitments under international human rights law.

Recommendations to the Government of Nepal

- Ensure the rights and fundamental freedoms of all Tibetans are protected in Nepal.
- Nepal deserves to graduate from Least Developed Country status, which in part will require greater connectivity and digital infrastructure, but it should seek development cooperation from partners who embrace transparency and a rights-based approach, which must not premise digital development on a promise of embracing anti-human rights policies.
- Make publicly available the contents of cooperation agreements and MOUs signed in relation to digital infrastructure or governance cooperation between Nepal and China, and consider establishing a national transparency database for easy access to all such agreements.
- Amend or repeal draft provisions such as the Social Media Bill, Information Technology Bill, and others that do not align with internet freedom principles, in part for expanding the censorship powers of the state in ways similar to those advocated by China under the Cyberspace Administration of China. Any social media regulation must comply with international human rights law, the Manila Principles on Intermediary Liability, and others.
- Amend or repeal the National Cybersecurity Policy in line with international human rights law, and in particular do not proceed with plans for a government intranet and National Internet Gateway.

Recommendations to the Government of Thailand

- Make publicly available the contents of cooperation agreements and MOUs signed in relation to digital infrastructure or governance cooperation between Thailand and China, and in particular those relating to cybersecurity, and consider establishing a national transparency database for easy access to all such agreements.

- Take concrete, transparent, actionable steps to guarantee that the Ministry of Digital Economy and Society and others will not pursue, privately or in public, any efforts to research, draft, or explore the feasibility of establishing a China-style single internet gateway, and commit to no other policies that risk internet fragmentation in Thailand.

- Conduct HRIAs on public–private partnerships and commit to ending any partnerships with Chinese institutions or individuals with documented records of exporting technologies used in the commission of human rights abuses, including those on existing sanctions or special entities lists such as Megvii. Recognising that China doesn't exert influence in a vacuum, Thailand should also investigate and end partnerships with other non-Chinese companies known for exporting human rights abusing technologies such as Russia's NtechLab or Israel's NSO Group.

- Repeal or amend the Cybersecurity Law, Computer Crimes Act, and others in line with Thailand's obligations under international human rights law.

- Put an immediate end to the persecution of Muslim minority ethnic Malays in the deep south and launch a full investigation into human rights abuses carried out through the conflict including the actual or planned implementation of China-style techno-authoritarian tactics of surveillance and censorship.

- Commit to immediately releasing the remaining Uyghur detainees in Thailand.

Recommendations to the internet freedom community

- Recognise the power and importance of coalitions by ensuring that the Freedom Online Coalition, among others, works closely with regulators in Europe, North America, and elsewhere to identify the threats to internet freedom posed by China's DSR and empowers resources and multistakeholder networks to conduct research and advocacy towards informed, rights-based policy.

- Promote a positive environment for alternative infrastructure providers based on development needs. The UN and governments of the Freedom Online Coalition community can create the environment in which positive technologies and digital governance norms are deployed.

- Positive narratives and investments are needed to counteract the appeal of China's relatively cheap technological solutions, to prevent the seeds of digital authoritarianism from taking hold through economic reasoning.

- Ensure greater financial investment and resources into open-source and digital public infrastructure, emphasising the value of decentralised and human rights-grounded technologies.

- Continue to ensure interoperability, and multistakeholderism over multilateralism and China's approach to digital sovereignty.

- Actively engage with colonial legacies and power asymmetries that fuel China's disinformation narratives around their model of digital sovereignty.

- Promote internet freedom and human rights-grounded internet governance at international fora, and especially where China is active in rewriting international norms on internet governance.

- Invest more financial resources, capacity-building, and time in cooperation with civil society and other actors, especially from the Indo-Pacific, to engage in international technical standards-setting bodies in ways that push back on China's efforts.

Recommendations to the United States

- Efforts such as the Digital Connectivity and Cybersecurity Partnership initiative under the US Agency for International Development could be expanded to include greater financial resources and capacity support for civil society in affected countries to more effectively monitor and persuade their governments away from China-style adoption.

- Expand the support for digital infrastructure and internet freedom and for strengthening regional partnerships outlined in the Indo-Pacific Strategy of the United States, to more strategically counteract China's regional influence on the development of digital infrastructure and internet governance norms.

- Ensure that any common approach places equal emphasis on universal human rights law and internet freedom principles as it does national security, trade promotion and other recommendations made throughout this report.

- In deepening regional treaty alliances with Australia, Japan, the Republic of Korea, the Philippines, and Thailand, hold treaty partners accountable for upholding rights-based practices, such as with Thailand in the ways outlined in this report.

- In strengthening relationships with other regional partners, including India, Indonesia, Malaysia, Taiwan, Vietnam, the Pacific Islands, and others laid out in the strategy, (1) ensure that partnerships highlight human rights benchmarks and commitments as outlined above; (2) recognise that one-size-fits-all engagement will fail and employ different strategies with countries already more directly influenced by China, such as Malaysia; and (3) note that while greater regional cooperation is necessary, uncritically embracing countries with their own records of digital dictatorship, such as Vietnam, will ultimately be counterproductive.

- Invest more in exploring the specific threats and best practices of other regional partners in confronting China's digital authoritarian influence and promoting new strategic partnerships or creative alternatives, such as Taiwan.

Recommendations for new strategic partnerships with Taiwan

- Explore Taiwan's civic tech community expertise as a counterweight to China's influence in the Indo-Pacific and global technology space.
- Support the communication and coordination between civic tech communities and governments to inform a coherent regional approach to digital public infrastructure for democratic participation and collaboration as a means of confronting China's malign influence. Taiwan's model of integrating civic technology initiatives with government efforts has proven successful in countering China's influence in the digital space and can provide valuable insights for the Indo-Pacific region.
- Provide more financial resources and partnership opportunities for Taiwanese civil society to develop and integrate more meaningfully with regional and international civil society, and especially through opportunities to engage at international technology standards and digital governance fora.
- Explore deepening government-to-government partnerships with the government of Taiwan as well as multistakeholder fora for engagement with the government of Taiwan, the civic tech community, and Taiwanese private technology sector.

Recommendations to global private tech sector organisations

- Commit to adhering to corporate responsibilities to respect human rights outlined in the UN Guiding Principles on Business and Human Rights, acknowledging where this is at odds with partnerships with China and taking concrete steps to resolve these contradictions.
- Commit to identifying trusted partners with whom important information relating to actual or potential Chinese infrastructure and digital governance cooperation can be shared, recognising that the sector is often privy to more information from the government on possible infrastructure bids or has access to corporate or Party structure information that is not publicly available.
- In line with UNGP responsibilities, include the risks of partnership with China or Chinese companies within HRIAs and make these publicly available, while also committing to sharing this information with civil society in lieu of completed HRIAs.

- Where tech companies who claim to adhere to UNGP responsibilities currently have partnerships, either directly or through subsidiaries, with Chinse tech companies, there are particular opportunities which should be explored. This includes, for example Norway's Telenor, which holds equal ownership with Axiata Group Berhad over Celcom Digi in Malaysia, noted for collaboration with Huawei, or elsewhere in which Telenor or related companies partnerships, joint-ownerships, or shareholder involvement creates in roads.

- Refrain from entering into partnerships with China or Chinese companies that would raise human rights concerns, such as the now abandoned Google Dragonfly censored search engine or Facebook-Google Hong Kong undersea cable projects.

- Where China is active in promoting its technical standards to normalise Chinese digital infrastructure and next-generation technologies, ensure transparency and accessibility for civil society in the Indo-Pacific and elsewhere to engage in the regional and global standards development and adoption process.