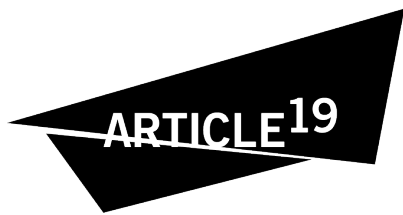




Cybersecurity with Chinese characteristics:

**Digital governance in the Indo-Pacific
and the Taiwanese alternative**



First published by ARTICLE 19, 2025

www.article19.org

© ARTICLE 19, 2025 (Creative Commons License 4.0)

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.

This work is provided under the Creative Commons Attribution-NonCommercialShareAlike 4.0 license.

You are free to copy, distribute, and display this work and to make derivative works, provided you:

- give credit to ARTICLE 19;
- do not use this work for commercial purposes;
- distribute any works derived from this publication under a license identical to this one.

To access the full legal text of this license, please visit:

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

ARTICLE 19 would appreciate receiving a copy of any materials in which information from this report is used. ARTICLE 19 bears the sole responsibility for the content of the document.

Contents

Abbreviations	4
Executive summary	5
Background	9
Cybersecurity governance in the PRC	
Key findings	12
Laws and regulations	13
Institutions	13
Digital governance norms	15
Cybersecurity and the Digital Silk Road	17
Case studies from the Indo-Pacific	
Key findings	20
Indonesia	23
Pakistan	29
Vietnam	34
Taiwan's cybersecurity strategies: Balancing security and freedom	
Key findings	40
Cybersecurity strategies	42
Cybersecurity legal framework	43
Innovation through community engagement	49
Conclusion	52
Priorities for dislodging China's grasp on cyber norms-setting	54
Appendix: PRC cybersecurity regulations affecting human rights	56

Abbreviations

ACS	Administration for Cyber Security
AI	Artificial intelligence
ASEAN	Association of Southeast Asian Nations
BSSN	Indonesia's National Cyber and Crypto Agency
CAC	Cyberspace Administration of China
CCP	Chinese Communist Party
CII	Critical information infrastructure
CNCERT/CC	National Computer Network Emergency Response Technical Team/ Coordination Center of China
CPD	Central Propaganda Department
CSMA	Cyber Security Management Act
CSO	Civil society organisation
DDoS	Distributed Denial of Service
DPP	Democratic Progressive Party
HITCON	Hacks in Taiwan Conference
ICT	Information and communications technology
MIIT	Ministry of Industry and Information Technology
MODA	Ministry of Digital Affairs
MoU	Memorandum of Understanding
MPS	Ministry of Public Security
NTCERT	National Telecom CERT
PDP	Personal Data Protection Law
PECA	Prevention of Electronic Crimes Act
PKCERT	National Cyber Emergency Response Team of Pakistan
PRC	People's Republic of China
PTA	Pakistan Telecommunication Authority
SIIO	State Internet Information Office
SPCAI	Sino-Pakistan Center for Artificial Intelligence
TAHR	Taiwan Association for Human Rights
VCP	Vietnam Communist Party
VPN	Virtual Private Network
WMS	Web Management System



Executive summary

In this report, ARTICLE 19 examines the People's Republic of China's (PRC) influence over cybersecurity norms through Digital Silk Road-related cooperation in 3 Indo-Pacific countries: Indonesia, Pakistan, and Vietnam. Our findings demonstrate how the PRC's digital development initiatives are aggressively integrating its governance norms in ways that pose profound challenges to international human rights, internet freedom, and democratic institutions, demanding urgent, contrasting digital governance norms. ARTICLE 19 further documents Taiwan as a more rights-based alternative to the PRC authoritarian model.

The report begins with establishing a baseline understanding of digital governance in the PRC, especially relating to cybersecurity norms. Because the Indo-Pacific region retains its strategic importance for the PRC as it continues to position itself as a global norms-setter in digital governance, understanding its normative diffusion in this region is key to comprehending its audacious global ambition: to fundamentally rewire the world's digital infrastructure and rewrite the rules governing digital space.

The report continues with 3 country case studies in the Indo-Pacific. We selected each country to show how PRC authoritarian models are spreading through their cybersecurity laws, policies, and institutions, which restrict freedom of expression and the right to privacy. These laws often relate to the management of critical information infrastructure, data localisation and identity verification requirements, digital surveillance, opacity, and comprehensive government control through 'China-style firewalls'.

Our findings point to the prevalence of PRC influence mechanisms through bilateral cooperation agreements that conflate digital development cooperation with digital governance norms adoption. Public-private partnerships with Chinese tech companies enhance bilateral cooperation. These exchanges, framed as non-political capacity-building efforts, aim to promote the PRC's digital authoritarian governance model as the best practice.

Through such influence mechanisms, our findings demonstrate PRC norms diffusion. Governments often pass stringent cybersecurity and data localisation laws under the guise of national security or digital economy development. In Indonesia, Pakistan, and Vietnam, the PRC's emphasis on cyber sovereignty has played a pivotal role in shaping domestic digital governance frameworks.

Another defining feature of the PRC's influence is the adoption of state-driven surveillance and censorship mechanisms. Indonesia has embraced cyber sovereignty and aligned further with PRC regional leadership through technical capacity exchanges and cooperation

agreements. In Pakistan, the development of a China-style firewall and the integration of surveillance technologies from Chinese companies such as Huawei is emblematic. Vietnam has incorporated real-name registration and strict content moderation measures into its cybersecurity laws. Our findings also point to capacity-building programmes, often led by Chinese companies, as creating dependencies that have further entrenched PRC norms and practices in the region.

Critically, this report presents Taiwan as a compelling alternative model for cybersecurity governance. By emphasising multi-stakeholderism over the PRC's restrictive multilateralism, Taiwan demonstrates a more transparent, civil society-engaged approach to digital governance. The fundamental separation of content regulation from critical information infrastructure governance stands in stark contrast to the PRC's securitisation strategy.

While acknowledging Taiwan's model is not without challenges, we argue that increased global engagement with Taiwan would contribute significantly to developing rights-based digital governance alternatives. This report serves not just as an academic investigation, but as an urgent call to action for policymakers, technologists, and human rights advocates worldwide.

By exposing the adverse characteristics of the PRC's digital model and its pervasive diffusion in the Indo-Pacific, we hope this report will provide a critical roadmap for identifying, understanding, and ultimately countering the profound human rights implications of the PRC's digital norm-setting ambitions.

Priorities for dislodging China's grasp on cyber norms-setting

For the international community

1. Stand with Taiwan

Advocate for Taiwan's participation in global cybersecurity and digital governance discussions to strengthen the international coalition against digital authoritarianism.

2. Support multi-stakeholderism

Encourage governments to involve citizens, civil society, and industry stakeholders in policymaking, mandating public consultations for draft legislation and ensuring Taiwanese stakeholders can engage meaningfully in international forums by creating inclusive mechanisms that amplify democratic voices.

3. Empower rapid response

Mobilise regional networks to gather evidence concerning digital tools and policies, working closely with local civil society to spotlight these issues – while protecting against reprisal – and foster an alliance against rising digital authoritarianism with Taiwan at the centre.

For the Taiwanese Government

4. Prioritise digital human rights within cybersecurity

Taiwan should continue to promote transparency, data protection, and public accountability with laws explicitly safeguarding privacy, free expression, and access to information as the cornerstone of its cybersecurity norms-setting.

5. Lead in global advocacy for rights-based cybersecurity governance

The Taiwanese Government should leverage Taiwan's democratic credentials to promote human rights-centric digital governance internationally, combined with digital diplomacy outreach for capacity-building to support Indo-Pacific nations in developing robust cybersecurity policies aligned with democratic values.

For Taiwanese civil society and private sector

6. Facilitate international monitoring of the PRC's digital influence

Taiwan civil society can work collaboratively with regional partners to document and publicise the negative human rights impacts of PRC-driven initiatives under the Digital Silk Road, especially by leveraging its expertise of PRC threats and influence tactics to help identify new problematic technologies, policies, and practices.

7. Engage in international norms-setting

Taiwan's private sector, and broader civic-tech community, should take advantage of all opportunities to participate in international forums, especially those on internet governance and technical standards-setting.

Background

In an era of unprecedented digital transformation, the People's Republic of China's (PRC) technological ambitions have achieved global reach through its strategic Belt and Road Initiative and its digital component, the [Digital Silk Road](#). This report arrives at a critical moment when the PRC's digital influence is rapidly reshaping geopolitical landscapes and digital norms across the Indo-Pacific region and beyond.

The accelerating technological competition and the PRC's systematic approach to digital infrastructure export have far-reaching implications. Developing nations are increasingly integrating Chinese technological ecosystems, setting the stage for profound normative transformations. The Digital Silk Road is more than mere infrastructure – it serves as a strategic instrument for projecting technological and governance models that challenge existing international digital and human rights frameworks.

The PRC's vision of digital governance, centred on centralised Communist Party control, cyber sovereignty, and multilateral promotion, poses significant challenges to international human rights, internet freedom, and democratic institutions. The normalisation of comprehensive government control, invasive digital surveillance, and restrictive data localisation practices threatens to fundamentally restructure the global digital environment.

Against this backdrop, Taiwan emerges as a critical counter point. At the same time, the PRC continues to actively isolate Taiwan internationally, seeking to suppress its engagement on the global stage. ARTICLE 19 argues that Taiwan's alternative approach to cybersecurity governance, however imperfect, remains an important, more rights-respecting alternative model globally, particularly in the Indo-Pacific, in countering PRC cybersecurity governance norms. Taiwan's rights-respecting approach to cybersecurity governance emphasises multi-stakeholderism, transparency, and the potential for civic participation. This alternative approach demonstrates the potential for democratic governance even under intense cyberthreats.

The primary objective of this report is to provide a comprehensive, evidence-based analysis that empowers policymakers, civil society organisations, and international stakeholders to understand, anticipate, and effectively counter the PRC's digital governance model. By exposing the mechanisms of normative diffusion, mapping the strategic landscape of digital infrastructure export, and highlighting alternative governance approaches, we aim to catalyse strategic responses that preserve digital rights, promote democratic values, and prevent the unchecked spread of authoritarian technological practices. Our research seeks

to transform understanding into actionable insights, supporting efforts to develop resilient, rights-respecting digital ecosystems in the Indo-Pacific and beyond.

As the PRC continues to expand its digital influence, this evolving situation demands both critical examination and decisive action. Policymakers, civil society, and international stakeholders must recognise, understand, and actively resist the normative transformation of digital spaces through authoritarian technological models. The future of global digital governance hangs in the balance, with profound implications for human rights and democratic values worldwide.

The top half of the cover features three stylized eyes. Each eye is a black almond shape with a yellow circular pupil and a thin red line for the upper eyelid. They are arranged in a triangular pattern, looking towards the center.

Cybersecurity governance in the PRC

The bottom half of the cover features three more stylized eyes, identical in design to the ones at the top. They are arranged in a triangular pattern, looking towards the center, mirroring the top section.

Key findings

Cybersecurity and digital governance norms in the PRC

- Centralised control under the Chinese Communist Party (CCP), cyber sovereignty, securitisation of development.
- Multilateralism versus multi-stakeholderism.
- Key laws such as the 2017 Cybersecurity Law and 2021 Data Security Law enforce party control through data localisation, censorship, and surveillance.

Digital Silk Road integration

- Launched in 2015 under the Belt and Road Initiative to develop digital infrastructure and expand information and communications technology (ICT) cooperation.
- Focus on promoting the PRC as a leader in digital governance, influencing global norms.
- Partnerships with the Association of Southeast Asian Nations (ASEAN) countries through initiatives like the ASEAN–China Strategic Partnership Vision 2030 and cybersecurity training programmes.

Technical standards, cybersecurity diplomacy, and strategic goals

- Secured 85 technical standards agreements with 49 countries by 2019, advancing PRC goals in digital governance.
- Expanded partnerships with 81 countries under the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), with a Memorandum of Understanding (MoU) established in ASEAN states.
- Cybersecurity linked to national security and development, embedding restrictive governance models in partner countries.

The PRC builds its cybersecurity governance through the following key laws, institutions, and norms.

Laws and regulations

- The 2017 [Cybersecurity Law](#) (中华人民共和国网络安全法) (see Appendix 1) forms the foundation of the PRC's cyber sovereignty model, mandating data localisation, real-name identity verification, and network control measures. It imposes strict obligations on critical information infrastructure (CII) operators and encourages non-CII operators to follow similar rules, effectively extending state control over all online service providers. Subsequent regulations have further strengthened these provisions.
- The 2017 [National Intelligence Law](#) (中华人民共和国国家情报法), alongside the amended [Counter-Espionage Law](#), mandates that individuals and organisations, including tech firms abroad, must assist in intelligence efforts, allowing for broad intelligence collection, recruitment, and surveillance, which raises concerns about privacy and state overreach.
- The 2021 [Critical Information Infrastructure Security Protection Regulations](#) (关键信息基础设施安全保护条例) expand the definition of CII to include 'public telecommunications and information services'.
- The 2021 [Data Security Law](#) (中华人民共和国数据安全法) extends PRC jurisdiction extraterritorially, holding foreign entities liable for data practices deemed harmful to the PRC's interests.
- The 2021 [Personal Information Protection Law](#) (中华人民共和国个人信息保护法) grants the state broad authority over personal data, permitting the use of identity recognition technologies under vaguely defined security pretexts.

All these laws raise significant concerns about privacy, freedom of expression, and international data governance tensions.

Institutions

Xi Jinping's statement, 'Government, the military, society, and schools ... the Party leads them all' exemplifies the hierarchical structure that also applies to digital governance institutions. The **Central Committee of the Chinese Communist Party** (中国共产党中央委员会) is the highest decision-making body in the country. The Standing Committee leads it, with Xi Jinping at the helm. The Central Committee sets political ideology and leads national policies and priorities. Meanwhile, the **State Council** (中华人民共和国国务院), the highest

organ of state power, is subordinate to the CCP and acts on the direction set by the Central Committee, including in areas like cybersecurity. Within China's Party-State system, several institutions may have both a public-facing state name and a Party designation, known as 'one institution with two names' (一个机构两块牌子). Acknowledging this distinction is important because, in cooperation agreements, countries who do not recognise this dual structure may believe they are entering partnerships with the government when in fact they are entering partnerships with the CCP.

The preeminent institution for cybersecurity, content-control regulations, and broader internet governance policies in China is the [Cyberspace Administration of China](#) (CAC) (国家互联网信息办公室). It has served as a '[supra-ministerial regulator](#)' under the Central Committee since 2018. It oversees censorship under the Great Firewall and leads in policies on emerging technologies including artificial intelligence (AI). The CAC also [supervises](#) the National Computer Network and Information Security Management Centre, which is responsible for the National Computer Network Emergency Response Technical Team/Coordination Centre of China (CNCERT/CC), discussed later.

The CAC's evolving authority points to the increasing importance of digital governance under Xi Jinping and is useful in understanding China's cooperation abroad. The State Council Information Office (国务院新闻办公室), also known as the Office of External Propaganda within the Central Propaganda Department (CPD), [established](#) the CAC as the State Internet Information Office (SIIO) in 2011.

The CAC's association with the CPD has [remained](#) core to its mission. Although often misunderstood, this distinction illustrates the interrelationship between internet governance and information control within China's digital norms. Top leaders often serve in both CAC and CPD roles, for example Zhuang Rongwen (庄荣文) who, as of December 2024, is [serving](#) as both the CAC Director and Deputy Director at the CPD.

In 2014, China reclassified the SIIO as the more authoritative Central Cybersecurity and Informatization Leading Small Group (中央网络安全和信息化领导小组), chaired by Xi Jinping, elevating CAC authority.

The same year, the CAC also hosted the [first](#) World Internet Conference (世界互联网大会) in Wuzhen, an event that has grown in stature and represents a key platform where the PRC has sought to influence international cyber norms. This is especially so following the 2022 [establishment](#) of the World Internet Conference International Organisation (世界互联网大会国际组织), which Xi Jinping [praised](#) for, among other things, its important role in 'the development and governance of the global internet'.

In March 2018, during a significant restructuring of Party-State institutions, the Central Cybersecurity and Informatisation Leading Small Group underwent an upgrade to become the Central Cyberspace Affairs Commission (CAAC) (中共中央网络安全和信息化委员会). The change effectively [elevated](#) the CAC to a Central Committee institution.

Key State Council institutions responsible for digital governance include:

- **National Development and Reform Commission** (中华人民共和国国家发展和改革委员会). This is the [most powerful](#) ministry under the State Council, overseeing development planning and producing the Five-Year Plan. It promotes technical innovation and strategic industries and plays a strategic role in developing digital policy frameworks. It also manages the [National Data Administration](#), which coordinates economic data applications with the CAC on smart cities and digital governance. The National Data Administration is part of the Digital China policy to lead global digital development by 2035 while enhancing cybersecurity.
- **Ministry of Industry and Information Technology** (MIIT) (中华人民共和国工业和信息化部). This State Council institution [regulates](#) telecommunications, software and information technology manufacturing industries, and provides technological support to the CAC for infrastructure and innovation. It also frequently represents the PRC in international organisations, such as the International Telecommunications Union (ITU), which plays a role in global cybersecurity norms.
- **Ministry of Public Security** (MPS) (中华人民共和国公安部). The MPS is the PRC's top police agency, originally responsible for the Golden Shield Project (Great Firewall). Although oversight has expanded to include the CAC and MIIT, MPS still [manages](#) public network security and enforces the Multi-Layer Protection Scheme. It handles cybersecurity tasks like regulating VPNs and [collaborates](#) with CNCERT/CC. Alongside the Ministry of State Security, MPS performs [surveillance](#) functions related to [foreign intelligence](#) and [transnational repression](#).

Digital governance norms

Cyber sovereignty

Arguably, the foundation of the PRC's digital governance norms is its notion of cyber sovereignty, first introduced in the 2010 [white paper on the internet in China](#). The concept asserts that internet governance falls under national sovereignty, allowing states to impose policies within their borders as they see fit. The PRC has actively promoted this vision

through various international forums and initiatives:

- At the 2012 Budapest Conference on Cyberspace, the PRC proposed [5 principles](#) for international cyber cooperation, with cyber sovereignty as the primary focus.
- The 2016 [National Cyberspace Security Strategy](#) (国家网络空间安全战略), launched by the CAC ahead of the passage of the Cybersecurity Law, reiterated this position and sought to force the global embrace of the PRC's norms-setting by claiming an international consensus on respecting cyber sovereignty.
- In 2018, launched in partnership with the CAC and others, the Belt and Road Initiative Digital Economy International Cooperation Initiative [encouraged](#) cooperation based on cyber sovereignty and multilateral internet governance.
- A 2022 State Council white paper, '[Jointly Build a Community with a Shared Future in Cyberspace](#)' (携手构建网络空间命运共同体), reaffirmed, among other norms-setting, cyber sovereignty as the 'natural extension of national sovereignty in cyberspace'.

The cyber sovereignty concept fundamentally conflicts with universal [human rights principles](#), which are universal, indivisible, and interdependent regardless of frontiers. It raises concerns about freedoms of expression, information, and privacy. Despite [China's Position on Global Digital Governance](#) released in 2023 by the Ministry of Foreign Affairs to oppose internet fragmentation, its cyber sovereignty norm encourages national regulations that risk precipitating a fragmented digital landscape.

Multilateralism and rejection of the multistakeholder model

The PRC's emphasis on multilateralism, consistent since the 2010 white paper, aligns with its emphasis on centralised authority under the CCP.

The PRC's vision systematically promotes multilateral cooperation through the UN and other state-led forums, emphasising cyber sovereignty that allows states to determine their own cyber development paths and regulations. The Ministry of Foreign Affairs exemplifies this in its 2021 [Position on International Rules-making in Cyberspace](#), urging states to 'formulate new international norms and rules'. By focusing on security and development in cyberspace governance, the PRC constructs a framework that fundamentally challenges existing international internet governance norms. This approach contrasts sharply with the [multistakeholder model](#), which traditionally includes civil society, industry, and academic perspectives.

By privileging state actors and limiting broader participation, the PRC's model raises significant concerns for human rights and internet freedom globally. Despite these concerns, the PRC's cyber sovereignty narrative is gaining traction, particularly among countries in the Global South seeking alternatives to US technological hegemony.

The implications are profound: the PRC is not merely proposing a technical governance model; it is actively constructing an alternative global digital ecosystem that prioritises state control over individual rights, transparency, and transnational collaboration.

Securitised digital development

The PRC views cybersecurity and informatisation as integral to national security and development. The 2017 International Strategy of Cooperation on Cyberspace highlights cybersecurity as crucial for sovereignty, security, and development. The PRC promotes multilateral cybersecurity cooperation through forums like the ASEAN Regional Forum, Shanghai Cooperation Organisation, Forum on China–Africa Cooperation, and elsewhere, supporting capacity-building in developing countries. One of the human rights concerns raised by this normative approach is seeing digital development as synonymous with securitisation of the online information space, a point [noted](#) by Xi Jinping. This approach risks influencing laws, policies, institutions, and infrastructures that infringe on the freedom of expression and right to privacy by modelling the PRC's approach with digital development partners along the Digital Silk Road. These concerns will be tested in the case studies from the region.

Cybersecurity and the Digital Silk Road

The first real reference to the Digital Silk Road concept was in MIIT's '[Plan for the Construction of Interconnected Infrastructure in Surrounding Countries](#)' (周边国家互联互通基础设施建设规划) in November 2014.

In March 2015, the National Development and Reform Commission followed suit with its white paper '[Vision and Actions to Promote the Joint Construction of the Silk Road Economic Belt and the 21st Century Maritime Silk Road](#)' (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). The paper called for the acceleration of the construction of cross-border backbone networks and broader expansion of ICT cooperation. It also stressed the PRC's global ambition to lead in technical standards-setting under the [China Standards 2035](#) policy. Since 2015 the PRC has sought to make the adoption of its technical standards part of its bilateral agreements, including in Indonesia and Vietnam.

The PRC published its [13th Five-Year Plan for National Informatization](#) (国务院关于印发‘十三五’国家信息化规划的通知) in December 2016. It announced its goal of reforming global internet governance and called for accelerated collaboration with ASEAN. This goal was further developed during the November 2016 ASEAN–China Summit, which concluded with the [ASEAN–China Strategic Partnership Vision 2030](#). It formed the basis of the first [ASEAN–China Cyber Dialogue](#) in 2020 on cybersecurity cooperation.

In 2019, the PRC [concluded](#) the second Belt and Road Forum with some 85 technical standards agreements with 49 countries, including Indonesia and Pakistan. The PRC held a third Belt and Road Forum in October 2023, during which it [reaffirmed](#) its ambitions to lead in developing rules for global digital governance, including cybersecurity governance. This goal has explicitly evolved in tandem with broader Digital Silk Road priorities. For example, the PRC’s [14th Five-Year Plan \(2021–2025\) for National Economic and Social Development and Vision 2035 of the PRC](#) (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), launched in March 2021, emphasised ambitions to strengthen its role in cyberspace, with attention to cybersecurity norms.

In November 2022, the State Council Information Office elaborated on several themes in the Five-Year Plan in its white paper ‘[Jointly Build a Community with a Shared Future in Cyberspace](#)’ (携手构建网络空间命运共同体). It highlighted regional joint initiatives on cybersecurity, including the expansion of partnerships under the CNCERT/CC to 81 countries and the establishment of MoUs with 33 countries, including Indonesia and Thailand. It also lauded the partnership with ASEAN, which 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 white paper calls for a China–ASEAN Network Security Exchange and Training Centre, exemplifying the PRC’s digital diplomacy to shape cybersecurity norms.



Case studies from the Indo-Pacific



Key findings

Case study 1: Indonesia

Digital dependency: Indonesia's growing reliance on Chinese digital technologies highlights governance gaps in cybersecurity governance, such as inadequate legal frameworks and resource-strapped institutions like the Ministry of Information and Communications (Kominfo) and the National Cyber and Crypto Agency (BSSN).

Chinese MoUs and policy shifts: Agreements like the 2017 MoU between the PRC's CNCERT/CC and Indonesia's BSSN have solidified the PRC's role in shaping Indonesia's cybersecurity policies and normalised PRC practices under the guise of capacity-building and bilateral cooperation that only benefits Indonesian cybersecurity norms.

Surveillance infrastructure expansion: Partnerships with Huawei and participation in the China–ASEAN Network Security Seminar have entrenched Chinese models in Indonesia with capabilities of real-name registration systems and stricter content moderation policies, raising privacy and freedom of expression concerns.

Case study 2: Pakistan

The PRC as a strategic lever: Pakistan's digital development under the China–Pakistan Economic Corridor has made it a testing ground for the PRC's influence, while partnerships with Chinese firms like Huawei and ZTE foster dependency.

Authoritarian legal frameworks: Laws like the Prevention of Electronic Crimes Act (PECA) borrow heavily from the PRC's 2017 Cybersecurity Law, which enables censorship, mandatory data localisation, and state surveillance while restricting dissent and free speech.

'Great Firewall' implementation: Pakistan's adoption of Chinese technologies for its Web Management System mirrors the PRC's Great Firewall, signalling a move towards centralised control over internet access and content moderation.

Case study 3: Vietnam

Cyber sovereignty as a shared character: Vietnam has facilitated the adoption of China-style cybersecurity policies over the years despite previous conflicts, including data localisation, censorship laws, and surveillance measures.

Cybersecurity law and its parallels with PRC norms: Vietnam's law mirrors the PRC's in several respects, such as mandating real-name registration and requiring platforms to provide backdoor access to government authorities.

The Digital Silk Road has emerged as a pivotal component in advancing the PRC's global influence through digital technologies and governance norms. Central to this initiative is the promotion of PRC-centric cybersecurity frameworks that prioritise cyber sovereignty, centralised control, and state-led internet governance. This initiative also extends to the Indo-Pacific region, as previously noted in ARTICLE 19's 2024 [The Digital Silk Road: China and the rise of digital repression in the Indo-Pacific](#), drawing on cases in Cambodia, Malaysia, Nepal, and Thailand.

While this report examines 3 cases from the region, the spread of the PRC's authoritarian approach to cybersecurity governance extends far beyond these examples. For instance, ARTICLE 19 has previously [highlighted](#) that online monitoring and mass surveillance became prevalent following the 2014 military coup in Thailand. Thailand has discussed establishing a national internet gateway to centralise state control over online content, further aligning its policies with the PRC authoritarian model. Similarly, the PRC's influence is stark in Cambodia across multiple domains, including digital infrastructure and internet governance. Chinese investment and cooperation have deeply embedded the PRC authoritarian model of cybersecurity governance, culminating in the [Digital Government Policy 2022–2035](#), which explicitly frames the PRC as a positive example. Cambodia has also sought to establish a China-style firewall in the form of the National Internet Gateway.

This report presents 3 new case studies – Indonesia, Pakistan, and Vietnam. Each case illustrates distinct yet interconnected pathways through which PRC norms are reshaping digital ecosystems and affecting cybersecurity governance and human rights in the Indo-Pacific. These countries demonstrate how bilateral agreements, partnerships with Chinese technology firms, and capacity-building initiatives have entrenched authoritarian practices in digital governance. From Indonesia's reliance on Chinese technologies and policy

frameworks to Pakistan's implementation of surveillance systems modelled on the Great Firewall, and Vietnam's replication of China-style cybersecurity laws, the case studies reveal a concerning trend: the gradual institutionalisation of authoritarian norms that prioritise state control over individual freedoms and civil society engagement.

Expanding on its previous research, the case studies are emblematic of broader trends in the diffusion of PRC digital governance norms and their adverse impact on the freedom of expression and other human rights. The case studies point to the significant need for alternative models for more rights-based cybersecurity governance in the Indo-Pacific.

Indonesia

Indonesia is a [key partner in the PRC's Digital Silk Road strategy](#), which aligns with the country's growing digital economy and its need for advanced digital infrastructure. It ranks seventh overall in global influence in Doublethink Lab's [China Index](#). The PRC has also focused on building influence through educational initiatives. Huawei, for instance, has [partnered](#) with Indonesian universities and government bodies to provide training in fields like cloud computing, AI, and the Internet of Things. The PRC has also [used diplomatic channels](#) to strengthen its ties with Indonesia. In 2021, both countries [signed an MoU](#) on internet security and technology cooperation, marking a significant step towards closer collaboration in digital governance. This agreement facilitates joint efforts between Indonesia's National Cyber and Crypto Agency (Badan Siber dan Sandi Negara) (BSSN) and the PRC's CAC, particularly in areas like data security and digital sovereignty.

Cybersecurity governance

Indonesia's cybersecurity governance is a crucial but underdeveloped aspect of its broader national security framework. As a rapidly digitising country with a growing reliance on digital infrastructure, Indonesia faces significant challenges in safeguarding its cyberspace.

Institutional framework for cybersecurity

In Indonesia, 2 key institutions, Kominfo and the BSSN, [manage](#) cybersecurity governance.

Established in 2001, Kominfo oversees internet governance, telecommunications, and cybersecurity. It has faced mounting [criticism](#) for its data management and lack of preparedness against cyber threats. It has also promoted content regulation policies that severely [infringe](#) on the freedom of expression.

BSSN, established in 2017, is responsible for overseeing cybersecurity policies, ensuring the protection of critical digital infrastructure, and enhancing the overall cybersecurity of the nation. BSSN has [struggled](#) with resource constraints and lacks the technical expertise necessary to address complex cyber threats effectively.

Indonesia's cybersecurity challenges extend beyond governance to a critical shortage of skilled professionals. The Minister of Communication and Information Technology Budi Arie Setiadi [highlighted](#) the global demand for cybersecurity talent, estimating a shortfall of 4 million professionals by 2023. National experts have informed ARTICLE 19 that, while private enterprises generally implement better data protection measures in Indonesia, state

institutions often neglect essential cybersecurity practices, such as regular data backups and updates to security protocols. This disparity exposes millions of Indonesian citizens to the risks of identity theft, fraud, and other cybercrimes, with severe implications for national security.

By addressing resource gaps, strengthening coordination between Kominfo and BSSN, and adopting advanced cybersecurity technologies, Indonesia can enhance its resilience against evolving cyber threats. Any models that Indonesia adopts will significantly impact human rights safeguards, so prioritising these is essential as the country develops its digital governance ecosystem.

Indonesia's fragmented cybersecurity regulations have led to human rights abuses. The 2008 [Electronic Information and Transactions Law \(ITE Law\)](#) sets a framework for managing digital communications and transactions, but [critics](#) argue that it is too vague and raise significant concerns over enforcement. Efforts to pass more comprehensive data protection legislation culminated in the 2022 [Personal Data Protection \(PDP\) Law](#). However, even this law has [faced delays](#) in its full implementation, with key provisions, such as the establishment of a dedicated data protection oversight agency, still pending. In general, Indonesia struggles with ineffective leadership in its cybersecurity governance, and it lacks a rights-based approach.

The PRC's influence on the cybersecurity landscape

Indonesia's cybersecurity governance challenges have prompted reliance on external solutions, including those from the PRC. Chinese firms have provided advanced cybersecurity technologies, particularly for critical infrastructure and data security, and with them the PRC's authoritarian governance norms.

2017 China–ASEAN Network Security Seminar: Indonesia's participation and subsequent policy changes

An important milestone in the development of Indonesia–PRC cybersecurity relations was when Indonesia participated in the [2017 China–ASEAN Network Security Seminar](#), hosted by CNCERT in Qingdao, PRC. This seminar brought together cybersecurity experts and officials from ASEAN countries, including Indonesia, to discuss the evolving challenges of cyber threats and share knowledge on how to improve cybersecurity resilience in the region. Indonesia's BSSN representatives actively engaged with their ASEAN counterparts and those from the PRC to learn about the PRC's approach to cybersecurity governance and emergency response. This interaction had policy implications for Indonesia, prompting a closer examination of its cybersecurity framework. The discussions at the seminar

highlighted the importance of coordinated responses to cyber incidents and the need for stronger regional cooperation, spearheaded by the PRC.

In particular, the event [pushed for greater engagement](#) with ASEAN and the PRC on cybersecurity matters, which eventually led to the signing of subsequent agreements, such as the MoU with CNCERT/CC in 2017. Moreover, the seminar underscored the need for Indonesia to upgrade its national cybersecurity capabilities, including establishing more robust emergency response systems and strengthening the coordination between various governmental bodies and private sector stakeholders. As a result of this PRC-led regional focus, the Indonesian Government took steps to formalise its role in regional cybersecurity organisations and started to prioritise the establishment of stronger cybersecurity protocols in line with standards promoted by the PRC.

MoUs between the PRC and Indonesia

The PRC shapes Indonesia's cybersecurity policies through various MoUs, international forum participation, and partnerships with players like Huawei. This section examines key examples of the PRC's influence, focusing on the MoU between Indonesia's BSSN and the PRC's CAC and the collaboration with Huawei to enhance Indonesia's cybersecurity infrastructure.

MoU with CNCERT/CC: Content, timeline, and implications for governance

One of the pivotal moments in the PRC–Indonesia cybersecurity cooperation [was in 2017](#) when Indonesia's BSSN and the PRC's CNCERT/CC signed an MoU. The MoU established a formal framework for cybersecurity cooperation aimed at enhancing both nations' capabilities in handling cyber threats and promoting the secure use of digital technologies. In line with the PRC's norms-setting, it emphasised, among other points, respect for cyber sovereignty and data security.

The MoU specifically laid out guidelines for joint efforts to improve cybersecurity awareness, capacity-building, and the sharing of best practices, which translates to adopting the PRC's practices. [It called](#) for regular exchanges of information on emerging cyber threats, training programmes for cybersecurity professionals, and the establishment of a cooperative framework for responding to cyber incidents. The first major activities after the MoU adoption included joint workshops and training sessions.

The implications for Indonesia's cyber governance were significant. The MoU marked a shift in its approach to cybersecurity, moving towards more reliance on the PRC and cooperation with non-Western powers. Several factors prompted this alignment.

First, there is [a growing sentiment](#) among some Indonesian officials and private sector leaders that Western technologies, often perceived as heavily influenced by geopolitical interests, may not fully align with Indonesia. Second, countries partner with non-Western powers like the PRC to gain [access](#) to advanced technologies and training, often without the strict human rights compliance expectations or regulatory conditions that typically come with Western aid.

This partnership has placed Indonesia in a position of increasing reliance on the PRC, raising questions about the balance of power and gradual adoption of the PRC's more authoritarian model of cyber governance.

MoU between BSSN and CAC: Huawei's role in the framework and its impact on cybersecurity practices

Another significant example of the PRC's influence on Indonesia's cybersecurity landscape is the MoU that BSSN [signed](#) with CAC, which led to its partnership with Huawei. The MoU is part of a broader effort to establish a systematic approach to cybersecurity focused on capacity-building, technology sharing, and the development of cybersecurity infrastructure, aligned with PRC approaches.

Huawei has played a central role in this framework, actively partnering with Indonesia to enhance its cybersecurity since it first signed the MoU in 2019, which was [renewed](#) in 2021. The company has [supported](#) BSSN in delivering a wide range of training programmes, including workshops on 5G security, cyber incident response, and the creation of [cybersecurity standards](#).

The collaboration between BSSN and Huawei has focused on developing Indonesia's national cybersecurity strategy, promoting greater engagement with the private sector, and encouraging a more proactive stance in cybersecurity governance. The renewal of the MoU between BSSN and Huawei in 2023 further cements this partnership.

However, Huawei's significant involvement has [raised](#) concerns, particularly about national security and data security. Critics have [pointed](#) to the risks of over-reliance on a company closely aligned with the CCP, especially given the sensitive nature of cybersecurity work and requirements incumbent upon Chinese ICT actors regarding CCP access and oversight. In other words, close collaboration between BSSN and Huawei could lead to potential backdoor access to Indonesia's digital infrastructure, which creates serious freedom of expression and right to privacy concerns. Reliance on the PRC authoritarian model for cybersecurity and broader digital governance may also inspire stricter content regulations, as seen in

recent [regulations](#) from Kominfo.

Evidence of policy shifts linked to the PRC's engagement

As Indonesia deepens its cooperation with the PRC, significant shifts are visible in the country's approach to cybersecurity, digital governance, and data sovereignty.

One example is Indonesia's commitment to cyber sovereignty, as demonstrated by the country's passage of the [Personal Data Protection \(PDP\) Law](#) in 2022. This legislation enforces stricter controls on data handling and foreign access to personal data. While the law is in line with global trends towards stronger data protection, it also signals a response to the growing influence of foreign companies, including the PRC's tech giants. The MoUs with CNCERT/CC and the CAC further illustrate Indonesia's evolving stance on data localisation.

However, the PDP Law does not necessarily represent a direct shift towards embracing the PRC's cybersecurity model without reservations. It is also a response to the challenges posed by foreign influence in Indonesia's digital landscape, such as concerns over data sovereignty and [security](#), including but not limited to threats from the [PRC](#). That said, the law still reflects Indonesia's goal of emulating the PRC's broader approach to cyber sovereignty in internet governance.

Another indicator is strategic digital alliances. Indonesia's continued partnership with Chinese tech giants has also influenced its broader digital strategy. The country's focus on cyber sovereignty and infrastructure modernisation aligns closely with the PRC authoritarian model of state-controlled internet governance and the promotion of national security within digital development. The development of 5G networks, AI, and cloud computing in collaboration with Chinese companies fits within Indonesia's broader goal of becoming a digital economy by 2035.

This engagement has influenced Indonesia's cybersecurity governance and strategic direction. Evidence of policy shifts further demonstrates the growing influence of this relationship on Indonesia's domestic policies.

[Official visits and diplomatic engagement](#)

Official visits and diplomatic agreements have served as critical channels for the growing cybersecurity and digital infrastructure collaboration between the PRC and Indonesia. These high-level engagements fostered the signing of key MoUs and set the stage for broader bilateral cooperation.

For example, in his January 2021 foreign visit, Chinese Foreign Minister Wang Yi [discussed](#)

expanding the nations' technological and cybersecurity cooperation. The result was the signing of an MoU between the CAC and Indonesia's BSSN. This agreement marked the [first cybersecurity](#) cooperation pact the PRC had signed with any foreign country. The MoU included provisions for improved internet security, data governance, and enhanced cooperation in cyberspace while upholding principles of cyber sovereignty. This agreement exemplified the PRC's increasing influence on Indonesia's approach to cybersecurity and wider digital governance.

Another example here is Huawei, which has also played a significant role in digital diplomacy in Indonesia, notably through its expansion of digital infrastructure and joint ventures with local firms. Huawei's commitment to building 5G networks and data centres in Indonesia, alongside collaborative efforts with the Indonesian Government and tech companies, underscores its strategic role in the bilateral relationship. Huawei has also been central to the Indonesian Government's digital transformation efforts, from developing AI capabilities to expanding cloud computing infrastructure. These joint ventures strengthen Indonesia's reliance on Chinese technology, aligning with broader Chinese geopolitical goals.

Training programmes and capacity-building

The soft-power aspects of the PRC's influence are equally significant, especially in terms of training programmes and capacity-building. Through these efforts, the PRC embeds its governance framework into Indonesian digital infrastructure. Again, Huawei has been a key player.

Through initiatives like the ICT Academy and the [Seeds for the Future](#) programme, Huawei has actively engaged Indonesian students and professionals, providing training in areas such as AI, cloud computing, big data, and 5G. [Huawei's collaboration with Indonesia's Presidential Staff Office](#) on a 5-year vocational training course for 100,000 Indonesian officials highlights the depth of the PRC's involvement in shaping the future of Indonesia's digital workforce.

Huawei's focus on digital skills extends beyond vocational training. The company has [worked](#) closely with Telkomsel, Indonesia's largest telecommunications operator, to provide 200 days of training for its employees in areas like 5G technology, cloud computing, AI, and customer experience management. By providing these learning opportunities, Huawei not only helps Indonesia build a technically capable workforce but also influences the strategic direction of Indonesia's digital infrastructure development. This capacity-building effort mirrors the PRC's broader regional influence through the Digital Silk Road, reinforcing Chinese tech companies' roles in regional digital development while entrenching Chinese technologies and alignment with the PRC's digital norms.

Pakistan

The PRC as Pakistan's strategic leverage

Pakistan ranks first in global influence in Doublethink Lab's [China Index](#). In the ICT sector, Chinese technology companies, notably Huawei, ZTE, China Mobile Communication Company Limited, and Alibaba have made considerable investments in developing Pakistan's digital infrastructure as part of the China–Pakistan Economic Corridor, established in 2015, and broader Digital Silk Road partnerships. Digital cooperation between the PRC and Pakistan predates the establishment of the Digital Silk Road. For example, in 2013, Pakistan became the first foreign country to adopt the Chinese navigation satellite system [BeiDou](#). More recently, in May 2024, in a joint cooperation between the PRC and Pakistan, the PRC [launched](#) the multi-mission communications Paksat-MM1 satellite, [capable](#) of providing broadband satellite internet among other services.

Alongside the adoption of Chinese technology and digital infrastructure, Pakistan is gradually incorporating PRC's digital standards. These developments in Pakistan's digital ecosystem demonstrate significant expansion in bilateral partnerships and between PRC companies and Pakistan counterparts. While these investments have resulted in modernisation and increased connectivity, they have also raised [apprehensions](#) about digital governance and technology norms, controls, and the spread of authoritarian standards. Pakistan's close cooperation with and learning from the state and Chinese ICT companies has facilitated the transformation to a more stifled and filtered internet environment. Current Prime Minister Shahbaz Sharif has [praised](#) the 'Chinese modernisation' as a model for Pakistan's future development of information technology.

How the cybersecurity landscape in Pakistan is adopting a PRC framework

Pakistani institutions leaning towards the PRC authoritarian model

The National Cyber Emergency Response Team of Pakistan (PKCERT) is the principal institution of Pakistan's cybersecurity architecture established under the [National Cybersecurity Policy 2021](#). PKCERT is responsible for responding to cyber incidents and strengthening cyber resilience. Similar to the nearly unfettered powers conveyed upon the CAC, the 2023 [Rules](#) grant the PKCERT comprehensive information collection and monitoring power in relation to proactively responding to cyber threats to CII; however, there is no clear definition of what constitutes the CII. The Rules also [mention](#) establishing

the National Telecom CERT (NTCERT) and its Security Operation Centres by the Pakistan Telecommunication Authority (PTA). Among others, the role of NTCERT will be critical in terms of its broad mandate to oversee the entire telecom constituency and data in the country. PKCERT, though still in its infancy, has started an active role in activating its local and international collaborations through different forums, particularly its cooperation with the PRC.

For example, PKCERT Director General Haider Abbas, who participated as a keynote speaker at the Beijing Cybersecurity Conference 2024, [expressed](#) PKCERT's intentions to collaborate with its Chinese counterpart in mutually addressing the 'cybersecurity threats and enhancing global cyber resilience'. Such comments point to Pakistan's readiness to further align its cybersecurity norms and expand its existing legislative frameworks seemingly modelled on the PRC's.

Legal frameworks governing cybersecurity

Historic anti-democratic events, including military interventions in democratic governments, have shaped Pakistan's legal framework governing digital spheres. The digital regulatory frameworks in Pakistan have also witnessed an evolution in the last decade. In 2014, the government issued a National Action Plan to respond to terrorism. The plan [stressed](#) taking 'measures against misuse of internet and social media for terrorism'. The [Prevention of Electronic Crimes Act \(PECA\) 2016](#) is the primary legislative instrument governing technology-facilitated offences.

The [PECA \(Amendment\) Bill 2018](#), introduced under PECA 2016, [established](#) the authority of the Federal Investigation Agency to monitor, investigate, and prosecute cybercrimes, including access and manipulation of unauthorised data, cyber frauds, cyberterrorism, hate speech, cyberbullying, child pornography, etc.

Pakistan's PECA has strong resemblances with the PRC's Cybersecurity Law. PECA 2016 makes it mandatory for the service providers to retain data for a minimum of 1 year, similar to the PRC's law. It also criminalises critical expression under the guise of 'false information' and reputational defamation, which is against international human rights norms that oppose criminal [defamation](#) laws. PECA 2016 also restricts any expression critical of the 'security or defense of Pakistan', which is again similar to the PRC's Cybersecurity Law, which prohibits online activities that may endanger national security.

Under the PECA (Amendment) Bill 2018, the regulator PTA has the power to arbitrarily take down critical expression online or request social media companies to do so by labelling

them as ‘unlawful content’. These provisions and subsequent rules are similar to the PRC’s Cybersecurity Law, legitimising censorship in the country. The PTA uses the framework established by PECA 2016 to block ‘unlawful content’. This provision has often targeted social media platforms (such as X, formerly known as Twitter), critical media outlets (such as FactFocus), and the websites of political parties, including the Pakistan Tehreek-i-Insaf and the Awami Workers Party. These actions often infringe arbitrarily on the freedom of expression. As of August 2024, the PTA had [blocked](#) over 2,300 websites and 180 mobile apps, in part relying on deep packet inspection technology.

The PTA is also [proposing](#) real-name identity verification for network operators in Pakistan in the [Digital Nation Pakistan Bill, 2024](#). The proposed system mandates mobile operators to verify users’ identities, relying heavily on biometric verification. The PTA may in the future leverage a [centralised database](#) to ensure precise identity authentication and enhance accountability within the digital ecosystem. These measures mirror the PRC’s internet governance norms on identity verification, raising concerns for privacy and the freedom of expression in Pakistan.

The misuse of PECA provisions on defamation, cyberterrorism, and blocking unlawful content has repressed civil society and media, silencing dissenting voices. Journalists have faced [harassment](#) by the Federal Investigation Agency for critical expressions on platforms like X, Facebook, and YouTube. Political controversies during the elections have [blocked](#) X since February 2024. These domestic restrictions align with Pakistan’s position in [supporting authoritarian](#) policies in international forums like the UN’s proposed Cybercrime Treaty, where it has advocated in line with the PRC and Russia for centralised, multilateral governance norms that emphasise cyber sovereignty and censorship under the guise of combating cyberterrorism and information threats.

In August 2024, in a related embrace of cyber sovereignty, resembling similar measures by the PRC’s MIIT, the PTA [announced](#) plans for a policy to limit unsanctioned VPN use. The policy would [establish](#) an allowed list of accepted VPNs. It is not the first time the PTA has [announced](#) such plans. Responding to a similar policy proposal in 2020, Pakistan-based digital rights group Bolo Bhi [warned](#) that registering VPNs and blacklisting non-compliant providers would result in a range of consequences from fuelling internet fragmentation to supporting surveillance.

On 23 January 2025, Pakistan’s National Assembly passed additional amendments to PECA, [widening](#) its scope to restrict control content at the expense of the freedom of expression, [including](#) greater emphasis on spreading ‘false information’.

The 2023 Personal Data Protection Bill, still awaiting approval final approval by the Senate, mandates [data localisation](#) similar to the PRC's laws, empowering the government to monitor and control personal and corporate data. PECA 2018 [Rules](#) already compel social media companies to store user data within Pakistan. While the government engaged civil society and big tech in the legislative process, the move faced significant opposition over right to privacy concerns. However, Pakistan appears aligned with the PRC's authoritarian approach to digital governance, emphasising state control over data under the guise of cybersecurity and combating cybercrime.

Emerging surveillance tech under the PRC's influence

The joint statement issued after Prime Minister Shehbaz Sharif visited the PRC and met with his Chinese counterpart Li Qiang confirmed Pakistan's dependency and trust on Chinese technologies. Cementing the PRC's role in Pakistan's digital transformation, major areas of attention between the 2 leaders included cooperation in AI, 5G, big data, cloud computing, and space collaboration. Pakistan is increasingly turning to the PRC to develop AI ethics and governance frameworks, as shown by its support for the PRC's Global AI Governance Initiative and collaboration on AI policy. The [joint statement](#) said: 'The Pakistani side welcomes the Global AI Governance Initiative announced by President Xi Jinping, and the PRC's endeavour to increase the right of developing countries in global AI governance.'

Pakistan's draft [National Artificial Intelligence Policy](#) provides more clarity on Pakistan's alignment with Chinese developments in AI and emerging tech. The policy highlights the Sino-Pakistan Center for Artificial Intelligence (SPCAI), which operates at the Pak–Austria Fachhochschule Institute of Applied Sciences and Technology in Haripur, Pakistan. SPCAI actively [maintains](#) strong academic and business relationships with the Guangdong University of Technology and the Shenzhen Institute of Advanced Technology, as outlined in Target 6 of the policy. The policy seeks to create regulatory frameworks to adopt global best practices for the development and spread of AI with a focus on bilateral and multilateral corporations through SPCAI (Target 11 of the policy). Pakistan also integrates its AI strategy with its national ambitions, taking inspiration from the PRC's aspirations to lead the world in AI. Pakistan appears to be adopting Chinese-style AI standards that promote a state-centred governance model, encouraging pro-censorship and surveillance algorithms instead of globally accepted standards developed by organisations such as the Institute of Electrical and Electronics Engineers, the International Organization for Standardization, the International Telecommunications Union, and the Organisation for Economic Co-operation and Development. This has the potential to equip the Pakistani state in the future to enable sophisticated and automated surveillance of its citizens.

Pakistan's 'Great Firewall'

The adoption of a Great Firewall narrative to cyber sovereignty, arguably the most quintessential digital infrastructure and cybersecurity governance model of the PRC, is becoming more popular throughout the region, which has also seen policy and technical adoption or reference in Cambodia, Nepal, and Thailand as previously [noted](#) by ARTICLE 19. This [includes](#) Pakistan.

The PTA [announced](#) plans to begin revamping the country's Web Management System (WMS), starting in January 2024. The upgrade [included](#) advanced deep packet inspection technology that will allow authorities to control network traffic at the internet gateway level, which raises concerns for censorship and surveillance at the infrastructure level. Although Pakistan had [reportedly](#) purchased its previous WMS from Canadian firm Sandvine in 2018, recent changes point to both a normative embrace of the PRC's infrastructure governance approach and the use of Chinese technology.

While there is a lack of public procurement records for the upgrade and limited information available, the WMS has notable [parallels](#) with the Great Firewall of China. The PTA published a tender for a Next-Generation Firewall in July 2024 but later [clarified](#) that the hardware would only serve their internal network. Despite its assurances to the contrary, Pakistan has [reportedly](#) deployed a firewall at its 2 main internet exchange points, which leaves concerns about the development of a China-style firewall unanswered without greater transparency from the PTA.

Vietnam

Mutual ideologies of one-party control

Nguyễn Khắc Giang, a Vietnamese political scientist, explained that the PRC and Vietnam tend to [learn](#) from one another due to their shared political ideologies. He stated that Vietnam's grand strategy [aligns](#) with the PRC's ambition to expand its influence, including in digital governance. Within the shared [market-Leninism](#) framework, the ruling party preserves its political monopoly over all aspects of life while embracing a market economy, bolstering legitimacy through economic liberalisation without political liberalisation. One area where this plays out is in tech development and governance.

[Vietnam considers the PRC as a comprehensive strategic partner](#), the highest level of diplomacy under Vietnam's foreign policies platform. The [joint statement](#) between Vietnam and the PRC during Xi Jinping's visit to Vietnam in December 2023 mentions cooperation in political security, government security, and regime security. In particular, the joint statement also says the countries agreed to strengthen cooperation in cybersecurity and 'intelligence exchange between the two sides and coordinate efforts to share experiences and collaborate on issues such as countering interference, combating separatism, and preventing "peaceful evolution" and "color revolutions" orchestrated by hostile and reactionary forces'.

Regular meetings between Vietnam and the PRC's security forces consistently highlight the importance of strengthening cooperation in cybersecurity. For example, in December 2023, a few days before Xi Jinping's visit, 2 deputy ministers of public security [reached an agreement](#) to organise more training programmes and provide equipment and tools to bolster their capabilities in combating high-tech crime. A similar meeting in January 2024 resulted in an [MoU](#) agreeing that both ministries would exchange experiences in preventing, combating, and addressing activities that misuse cyberspace to defame and slander the party and state, disrupt security and public order, and harm the friendly relations between Vietnam and the PRC. The foundation of digital authoritarianism in both countries is a shared belief in cyber sovereignty.

Cybersecurity as a matter of cyber sovereignty

Vietnam [established](#) a military department on 18 April 2012, less than 2 years after the PRC released its formative white paper on the concept, with the mandate of 'protecting the national information sovereignty in cyberspace', among other responsibilities.

The next milestone in normalising the concept in Vietnam's internet governance was [Decree](#)

[72/2013/NĐ-CP](#), issued on 15 July 2013. As of December 2024, it remains one of the most important legal documents regulating the internet in Vietnam. The decree stipulates that ‘Foreign organizations, businesses, and individuals providing public information across borders with users in Vietnam or access from Vietnam must comply with the relevant laws and regulations of Vietnam.’ It marked the government’s first effort to compel foreign companies to adhere to local laws, representing a major step towards asserting sovereignty over the internet, in line with the PRC’s.

Shortly afterwards, on 14 January 2014, Prime Minister Nguyễn Tấn Dũng issued a [decision](#) that explicitly mentioned the term ‘cyberspace sovereignty’ (*chủ quyền không gian mạng*, or *chủ quyền số quốc gia*).

The following year, Vietnam’s Minister of Public Security Trần Đại Quang, who later served as the President from 2016 to 2018, advocated for the concept of cyber sovereignty in his book [Cyberspace – Future and Actions](#). He referenced Xi Jinping’s [speech](#) at the 2018 Cybersecurity and Informatization Work Conference on the concept as a key source of inspiration for shaping Vietnam’s cybersecurity policies: ‘There is no national security without cybersecurity; the Internet and information security have become new challenges for the PRC as both are closely tied to national security and social stability.’

In 2016, the National Assembly elected Trần Đại Quang as President, one of the 4 highest roles in Vietnam’s political hierarchy. In that role, he continued to [instruct](#) Vietnam’s Ministry of Public Security in drafting the [Cybersecurity Law](#). In August 2017, he [emphasised](#) the importance of requiring foreign companies to store data locally and strengthening control over social networks. Quang was a key figure in influencing the government’s cybersecurity strategy to resemble the PRC’s digital authoritarianism model.

Since then, officials and think tanks within the Vietnamese Communist Party (VCP) have extensively discussed cyber sovereignty, which serves as the foundation for Vietnam’s internet governance. One especially formative event was the ‘[Protecting national sovereignty in cyberspace](#)’ conference in December 2021. Three Politburo members – those who hold the most powerful positions within the party – were in attendance.

More recently, in 2022, the then-Minister of Public Security Tô Lâm – one of the main architects of the 2018 Cybersecurity Law – published a book called [Cyberspace sovereignty – The Demands of the Era and National Obligations](#), which discusses cyberthreats as justifications for more repressive measures to control the internet. A series of conferences followed in [April 2022](#) and [February 2024](#) to discuss the book and cyber sovereignty model. In August 2024, Tô Lâm became the VCP General Secretary, elevating him to the most

powerful position in the country. These examples are emblematic of how Vietnam has integrated cyber sovereignty into high-level Party narratives, laws, and regulations, in line with the similar approach taken by the PRC.

Tracing the PRC's footprints in Vietnam's 2018 Cybersecurity Law

One of the earliest pieces of evidence of Vietnam learning from the PRC is a [2011 article](#) published in *Nhân Dân*, the VCP's official newspaper. It analysed the PRC's laws and regulations on content moderation, real-name registration requirements, punishing users' speech, and the use of firewalls.

The following year, the official website of the Vietnam People's Army featured an [article](#) with contributions from Nguyễn Thế Kỷ, then Deputy Head of the VCP's Propaganda Committee. The article highlighted lessons from the PRC, stating that the country 'establishes "firewalls" to block all foreign social media platforms deemed to pose significant risks and requires internet service providers to host their servers within China'. Nguyễn Thế Kỷ also referenced the PRC's internet laws as a model in a [2010 article](#) published in *Tuyên Giáo Magazine*, the official publication of the VCP's Propaganda Committee.

These articles suggest that long before Vietnam's 2018 [Cybersecurity Law](#), VCP officials were already discussing its key provisions, drawing inspiration from the PRC's norms-setting. As with the PRC, Vietnam's 2018 Cybersecurity Law is the cornerstone of its internet governance model. Arguably one of the most controversial pieces of legislation in the country's history, it demonstrates a high degree of similarity with the PRC's law in several key aspects.

First, both laws define cybersecurity in a manner that significantly diverges from the conventional understanding embraced by democratic governments. In most democratic contexts, people view cybersecurity as the effort to maintain a technically secure cyberspace, protecting against cyberattacks and the misuse of technology systems for criminal activities like hacking or unauthorised access to information. It should not include content controls.

In contrast, Vietnam's and the PRC's laws adopt a broader definition of cybersecurity, encompassing non-technical aspects such as content moderation, personal data protection and localisation, and restriction of expression critical of the ruling party. Both laws treat information and data in cyberspace as matters of national security, which in this context extends to protecting party and government officials as well as preserving the authoritarian regimes themselves.

After the passage of the 2018 Cybersecurity Law, the then-VCP General Secretary Nguyễn Phú Trọng [stated](#) that:

‘Around the world, many countries have this law. During the era of the Fourth Industrial Revolution, there are many benefits, but on the other hand, management becomes very challenging. From this, agitation, protests, disturbances, and attempts to overthrow the government can arise. Therefore, this law is necessary to protect the regime; people cannot be allowed to say whatever they want or insult whomever they please.’

He mostly summed up some critical parts of the law which clearly make ‘anti-state speech’ illegal in cyberspace. The VCP’s propaganda has widely echoed this narrative, especially in [2023](#) and [2024](#).

Second, the laws introduce 2 similar terms. The PRC’s law covers ‘critical information infrastructure’ while Vietnam’s law addresses ‘information system critical for national security’. The similar language used in both laws reflects how the laws define and manage these terms, especially when it comes to controlling content.

Third, both laws require heavy online censorship. Vietnam’s law clearly prohibits ‘information in cyberspace with contents being propaganda against the Socialist Republic of Vietnam; information contents which incite riots, disrupt security or cause public disorder; which cause embarrassment or are slanderous; or which violate economic management order’. The PRC’s law contains a similar provision. This is the legal ground for all other regulations on content moderation. Because the laws in both countries are vague and lack independent oversight, law enforcement often interprets and implements them arbitrarily to silence critics and suppress dissent.

Fourth, both laws mandate data localisation as a means of exerting control over tech companies, regardless of their country of origin. This requirement reflects the concept of cyber sovereignty, compelling tech companies to store data physically within the borders of the respective countries.

Fifth, both laws mandate that social media users register with their real identities and require platforms to verify these identities during the registration process. This requirement directly undermines the right to privacy and a principle of internet freedom: anonymity. Without anonymity, users have to expose their identities and online activities to authorities, which effectively places them under government surveillance. This not only leaves their privacy exposed and vulnerable to monitoring but also significantly raises the risk of suppressing their freedom of expression.

Finally, both laws compel internet users and tech companies to act as informants for the party. Users must identify and report 'harmful information' on the internet to the authorities. For tech companies, the obligations are even more stringent: they must proactively filter content on their platforms and grant authorities access to users' information upon request.

These parallel provisions in both cybersecurity laws suggest that Vietnam drew heavily from the preceding PRC law, enacted 2 years earlier.

Vietnam's law, in particular, seems designed to compel foreign tech companies to comply with local regulations. The flow of external information through foreign platforms like Facebook and Google had long posed a challenge to the Vietnamese Government, as they lacked both control and significant leverage over these companies. In addressing this issue, Vietnam used the PRC authoritarian model as guidance. Indeed, in a 2017 proposal sent to the National Assembly alongside the draft Cybersecurity Law, the Vietnam Ministry of Public Security openly acknowledged that they had looked to the PRC, among other countries, when drafting the law.

Subsequent legal documents have further developed the 2018 Cybersecurity Law's framework. [Decree 53/2022/NĐ-CP](#) introduces a compromise on data localisation. Foreign tech companies no longer have to store data locally if they comply with government demands for content moderation and access to user data. [Decree 13/2023/NĐ-CP](#) elaborates on personal data control measures under the law. It grants the government extensive access to citizens' online personal data without consent, citing national security and crime prevention. Notably, this decree empowers the Vietnam Ministry of Public Security to block entities from transferring personal data abroad under similarly vague justifications.

[Decree 147/2024/NĐ-CP](#), which took effect on 25 December 2024, enforces the real-identity verification requirement outlined in the 2018 Cybersecurity Law. It mandates social network users to register with real names and requires platforms to verify users' identities via local phone numbers or ID cards. The decree also authorises the government to suspend internet services for non-compliant users, block platforms that fail to adhere to these rules, and demand backdoor access to platform content for government searches.

The PRC's concept of cyber sovereignty has become a cornerstone of Vietnam's regulatory framework. The concept underpins key policies such as the 2018 Cybersecurity Law and its subsequent decrees, which closely mirror the PRC's normative approach. Through these regulations, Vietnam has taken bold and aggressive steps to extend its control over online discourse and personal data. The aim is to govern online speech as effectively as it does in physical spaces while enabling authorities to leverage users' personal data as a tool for enforcement and compliance.

Taiwan's cybersecurity strategies



Balancing
security and freedom

Key findings

Distinctive democratic cybersecurity model

Taiwan balances robust cybersecurity measures with the preservation of democratic values, focusing on multistakeholder engagement, transparency, and the protection of freedom of expression and privacy. This approach offers a contrast to the authoritarian norms promoted by the PRC.

Escalating threats from PRC cyber operations

Taiwan experiences up to 2.4 million daily cyberattacks, with CII such as undersea cables frequently targeted. High-profile incidents, including cyberattacks during Nancy Pelosi's 2022 visit, and operations by groups like NoName057, illustrate the persistent and sophisticated threats Taiwan faces.

Transparency and public engagement

Taiwan integrates public consultations into legislative processes, leveraging platforms like the Public Policy Network Participation Platform to balance security needs with civil liberties, ensuring accountability in cybersecurity governance.

Rights-based leadership

Taiwan resists adopting securitised digital development and emphasises transparency, collaboration, and democratic principles, positioning itself as a counter-model to the PRC's authoritarian digital governance. While challenges remain, Taiwan demonstrates that effective cybersecurity need not compromise fundamental freedoms.

Taiwan is facing an ever-escalating threat landscape characterised by an unprecedented volume of [cyberattacks](#). The PRC has intensified its use of [grey zone tactics](#), including cyber operations, combined with [United Front](#) information and influence campaigns pushing a unification narrative. The National Security Bureau documented that in 2024 the Taiwanese Government endured approximately [2.4 million cyberattacks daily](#) on average, which is twice the 2023 average of 1.2 million cyberattacks targeting government agencies, highlighting the severity of the challenge.

Initially concentrated on government agencies, these cybersecurity threats have expanded across industries, including targeting the physical layer of the internet infrastructure, such as [undersea cables](#). This expansion has amplified the potential for severe economic and operational disruptions. Attacking internet infrastructure can also have a dire impact on communications and network usage, thereby damaging freedom of expression and access to information.

Taiwan's role as a geopolitical flashpoint intersects with its vulnerability. Notably, the August 2022 [visit](#) of US Speaker Nancy Pelosi provoked a significant reaction from the Chinese Government, leading not only to military exercises but also to a [series of cyberattacks](#) that began before the visit and continued for 9 days. These attacks primarily consisted of Distributed Denial of Service (DDoS) attacks, website defacements, and highly convincing disinformation campaigns. On 10 September 2024, another [incident](#) occurred where the pro-Russian hacker group NoName057 claimed to have launched a series of DDoS attacks targeting websites of Taiwanese Government agencies and critical infrastructure, naming the operation 'OpsTaiwan'. During a press conference on 14 September, the Ministry of Digital Affairs (MODA) [reported](#) that they had recorded a total of 45 incidents. The attacks targeted local tax offices, regional civil aviation stations, the Directorate General of Budget, Accounting, and Statistics, financial institutions, and telecommunications operators. Foreign cyberthreats like these indicate that Taiwan has a strong need for coherent cybersecurity governance, but one that must balance transparency and human rights.

Even as cyber threats mount, Taiwan continues to forge a distinctive path in securing its digital space. Its approach puts openness first – bringing together voices from government, industry, and civil society while keeping citizens' rights at the heart of cyber defence policies. While facing complex security challenges, Taiwan shows that defending against digital attacks does not mean abandoning human rights. Our findings reveal Taiwan as a real-world example of how democracies can tackle cyber threats without compromising their values. This stands apart from the PRC's authoritarian model, which prioritises control over freedom.

Cybersecurity strategies

In light of these myriad threats, Taiwan's approach to cybersecurity governance navigates an increasingly complex digital threat landscape from the PRC. At the same time, Taiwan is trying to strike a careful balance between addressing legitimate cybersecurity risks and upholding fundamental democratic values, including the protection and promotion of freedom of expression and the right to privacy. This dual focus underscores Taiwan's efforts to foster a secure yet rights-respecting digital environment, with new the principle institutionalised in the 2016 [National Cybersecurity Develop Strategy](#) (國家資通訊安全發展方案). This strategy outlines 4 key objectives: strengthening infrastructure protection, combating cybercrime, fostering public-private collaboration, and building international partnerships. The National Communications Commission, the National Security Council's Cybersecurity Office, and the Executive Yuan's (Taiwan's executive branch of government) Department of Cyber Security are taking the lead in implementing these priorities. However, while these frameworks demonstrate a commitment to comprehensive governance, questions regarding coordination and resource allocation remain significant challenges.

The first phase of Taiwan's [Cybersecurity is National Security 1.0](#) initiative started in 2016 after former President Tsai Ing-wen took office. The initiative aimed to establish a foundational policy framework, including the [Cyber Security Management Act](#) (CSMA), the elevation of the Executive Yuan's Department of Cyber Security, and the creation of the Information and Electronic Warfare Command. Building on this foundation, the [Cybersecurity is National Security 2.0](#) strategy, launched in 2021, seeks to address gaps by focusing on organisational reforms, legal updates, talent cultivation, and industry integration.

The Cybersecurity is National Security 1.0 framework aimed to achieve a triad structure consisting of the National Security Council, the National Communications Commission, and the Executive Yuan's Department of Cyber Security during 2016–2020. The Cybersecurity is National Security 2.0 strategy further integrated military, intelligence, and law enforcement agencies into the national cybersecurity strategy, expanding it into a multi-pillar framework from 2021 to 2025.

This structure now includes the National Security Council, the Ministry of National Defense, MODA, the National Security Bureau, the Investigation Bureau, and the Criminal Investigation Bureau. Taiwan's strategy emphasises making structural improvements, like the [inauguration](#) of MODA in August 2022, and enhancing collaboration between agencies. Its success depends on resolving long-standing issues related to authority and accountability within Taiwan's decentralised governance model. In this sense, Taiwan's cybersecurity governance after 2016 is also highly institutionalised with the core concept of viewing cybersecurity as part of national security.

Cybersecurity legal framework

Progress of cybersecurity regulations

In 2018, Taiwan's [CSMA](#) underscored the government's efforts to bolster its cybersecurity governance framework. The CSMA provides a legal framework for assigning cybersecurity responsibilities to government agencies and critical infrastructure operators.

In 2023, MODA [promoted amendments](#) to the CSMA, with revisions aimed at strengthening the regulatory oversight of public and specific private entities enhancing audit mechanisms, and establishing accountability measures for [critical infrastructure](#) providers such as critical infrastructure operators and state-owned or state-controlled foundations. The proposed amendments also ensure that the authority- will actively consider how important and sensitive the business operations are for the critical infrastructure providers under its jurisdiction. This means that the authority- the Administration for Cyber Security (ACS) (資安署) will regularly audit the implementation of the providers' cybersecurity maintenance plans. The consideration will include the scale and nature of their information and communication systems, the frequency and severity of cybersecurity incidents, and other factors related to cybersecurity.

The ACS must create a draft annual audit plan and send it to the competent authority for review, which the Executive Yuan will then approve. Furthermore, the National Information and Communication Security Committee must also receive the annual audit plan for record-keeping. The composition of this committee reinforces accountability, as it includes non-government representatives (academics and experts) and local government representatives who serve as committee members, which further enhances transparency, preventing ACS from operating without external checks. Additionally, the amendments mandate stricter cybersecurity personnel requirements and grant the central regulatory authorities investigative powers over significant cybersecurity incidents in specific non-governmental but government-owned or controlled entities.

[Experts](#) highlighted that establishing clear legal obligations under the CSMA amendments represents a step forward in enhancing cybersecurity compliance. This clarity not only helps enterprises understand their responsibilities but also fosters greater accountability and heightens awareness of the need for proactive cybersecurity measures. For example, under the proposed amendments, enterprises may need to complete mandatory education and training programmes for personnel within a year or even a few months. By adopting a phased implementation approach, the amendments allow businesses to achieve compliance without straining their operational capacity, while simultaneously bolstering long-term cybersecurity resilience across industries.

In addition to the positive feedback, [one of the criticisms](#) of the [CSMA 2023 amendments](#) is its focus on audit mechanisms at the expense of fostering robust intelligence-sharing frameworks. While Article 9 of the amendments mandates the ACS to establish a cybersecurity intelligence-sharing mechanism, the legislative emphasis remains skewed towards compliance audits. This imbalance raises concerns about the CSMA's ability to address dynamic cybersecurity threats effectively. Experts argue that intelligence-sharing should form the core of the CSMA, aligning with international best practices to enhance the resilience of both public and private entities.

Another questionable issue is MODA's decision not to publicise the list of banned products deemed harmful to national cybersecurity. MODA's reluctance to disclose the list of critical infrastructure providers of these product has sparked controversy. MODA argues that publicising the list could expose vulnerabilities to hostile actors such as the PRC. Critics, however, contend that this approach may reflect a risk-averse bureaucratic mindset rather than a substantive strategy. Public agencies can query the ACS about these products under Article 11 of the original proposed amendments; however, critics have pointed out that the refusal to disclose the list publicly could limit accountability in the industry. MODA defends this stance, citing concerns over potential circumvention strategies, such as misrepresenting product origins. However, critics argue that transparency could enhance public oversight and incentivise compliance with security measures.

The Executive Yuan approved the draft CSMA amendments on 4 October 2024, and promptly submitted them to Taiwan's Legislative Yuan for legislative review. The Legislative Yuan is still discussing the proposed revisions. If the amendments successfully pass the second and third readings in the Legislative Yuan, they will officially come into effect. However, the prospects for their passage remain uncertain due to the ruling party's lack of a parliamentary majority, making bipartisan support a critical factor for advancing the proposed changes.

According to one senior digital and cybersecurity policy expert who requested anonymity in the ARTICLE 19 interview, the CSMA and the relatively newly formed MODA and ACS have extremely limited control or bargaining power to establish cybersecurity norms. Only the Presidential Office and the Executive Yuan have the authority to mobilise and coordinate different branches of government in this effort, which still requires extensive planning and greater political will from the political leadership. Despite Taiwan having enough technological expertise, the executive power is still in the beginning phase of establishing cybersecurity norms and is therefore relying on civil society to counter cyber threats.

Despite these efforts, the CSMA's limited scope, which primarily targets public agencies and specific private entities, has faced calls for broader applicability across industries. The rapid evolution of cyber threats necessitates a more inclusive regulatory framework

to address vulnerabilities in sectors not currently covered by the CSMA. Additionally, the lack of remedial mechanisms for entities subject to ACS audits, compared to administrative inspections, raises concerns about fairness and procedural integrity.

Strategies and practices of cybersecurity institutions

The role of MODA in cybersecurity governance has also expanded under the proposed amendments. By the end of 2021, the Ministry of Digital Affairs Organization Act passed its third reading in the legislature, paving the way for MODA's creation. MODA has taken on responsibilities from 5 government agencies: the National Communications Commission, the Ministry of Economic Affairs, the National Development Council, the Ministry of Transportation and Communications, and the Executive Yuan's Department of Cyber Security. Before this change, multiple government departments managed digital-related responsibilities, leading to high coordination costs when implementing digital policies. The establishment of MODA consolidates these dispersed functions under a single agency, ensuring a more streamlined and effective execution of Taiwan's digital policies and reducing bureaucratic inefficiencies.

The Executive Yuan has transferred its regulatory authority to MODA following the establishment of MODA and the ACS. This restructuring reflects the government's intent to centralise and streamline cybersecurity oversight, although the effectiveness of this transition will depend on MODA's ability to address long-standing coordination and capacity challenges within Taiwan's decentralised governance model.

Taiwan's experience offers an instructive contrast to the PRC authoritarian model because Taiwan has consistently prioritised the protection of freedom of expression while developing its cybersecurity governance framework, despite facing substantial cybersecurity threats and information manipulation campaigns from the PRC. Audrey Tang, the inaugural Minister of MODA, established many of the strategic directions. During her time as Digital Minister, Tang illustrated this approach through several key policy positions and initiatives.

She [stated](#) that when engaging with social media platforms, the government maintained principled discussions without direct intervention in content moderation practices. While acknowledging concerns about algorithmic transparency, particularly regarding Facebook's operations, Tang emphasised the importance of maintaining dialogue with platform operators. This approach sharply contrasts with the PRC authoritarian model premised on restricting expression as part of the information infrastructure securitisation process. In contrast, Taiwan prioritises fostering an open and democratic digital environment, emphasising dialogue over control. Unlike the PRC's tight grip on online discourse through

state censorship and algorithmic manipulation, Taiwan's strategy seeks to respect the principles of freedom of expression and transparency.

In international forums, such as the [Global Cooperation and Training Framework](#), which aims to strengthen partnerships among like-minded nations and expand Taiwan's international presence while addressing critical global challenges, Tang consistently [emphasised](#) that addressing controversial content must never compromise fundamental freedoms of expression. She explicitly rejected proposals to require disclosure of user internet protocol (IP) addresses in legislative reforms. Even when faced with significant public debate over the [Draft Digital Intermediary Service Act](#) in 2022, Tang, in her role as Minister of Digital Affairs, maintained clear institutional boundaries, emphasising that content regulation falls outside MODA's purview. Instead, she positioned the [ministry as an enabler of digital innovation and cross-sector development](#) rather than a regulatory body.

Tang's approach is perhaps best encapsulated in another [statement](#) during the interview with Liberty Times in 2023 August:

'We have invested considerable effort in demonstrating that defending against external information operations and protecting domestic freedoms of expression and assembly are mutually reinforcing, rather than competing, objectives. Strengthening our defences against external threats need not come at the cost of reducing domestic freedom of expression.'

While some [critics](#) have argued this approach may appear too passive in addressing foreign information manipulation and influence operations, in its early years MODA has established an important precedent for Taiwan.

Accordingly, Taiwan could lead a rights-based approach to cybersecurity governance, contrary to the PRC approach modelled on centralised control and cyber sovereignty. The PRC authoritarian model emphasises securitisation over multistakeholder engagement, implementing state control through mechanisms such as mandatory data localisation, content restrictions, and surveillance infrastructure. But Taiwan advocates another path – one that not only avoids infringing upon freedom of expression but actively maintains distance from any policies that might compromise this fundamental right, even in the face of significant information warfare challenges.

Given the rapid evolution of cyber threats, the adaptability of Taiwan's regulatory framework is a critical concern. Although Taiwan serves as a positive counterexample compared to the PRC authoritarian model of cybersecurity governance, it still faces its own set of problematic practices and challenges. For instance, in 2017, members of the Democratic Progressive

Party (DPP), typically known for their anti-CCP stance, [proposed](#) incorporating the concept of cyber sovereignty into Taiwan's [National Security Act](#). This proposal culminated in Article 4 which states: 'The maintenance of national security shall extend to cyberspace and its physical space within the territory of the Republic of China (Taiwan).'

Leading DPP legislator Yeh Yi-jin [advocated](#) for the inclusion of cyber sovereignty in the CSMA in 2017, asserting: 'National sovereignty now encompasses not only territorial and border issues but also the internet, as it can pose potential threats to national security. Only by including the internet within the scope of national sovereignty can cybersecurity issues be fundamentally resolved.' Thus far, attempts to embrace cyber sovereignty have failed but it remains a normative concern in Taiwan's evolving governance.

Transparency in cybersecurity regulation: The CSMA revision

Taiwan's CSMA demonstrates that it can develop cybersecurity regulations through transparent, participatory processes that protect both security interests and civil liberties. The CSMA's evolution particularly showcases the role of public consultation in preventing overreach and ensuring accountability in cybersecurity governance.

Central to this process is Taiwan's [Public Policy Network Participation Platform](#) (公共政策網路參與平臺), which serves as a vital channel for civic engagement in cybersecurity policymaking. The platform mandates public notice periods for draft legislation and enables citizens to actively shape policy development through structured dialogue. The Cybersecurity Law Subgroup (資通安全法小組) moderates these discussions, ensuring sustained engagement between citizens and policymakers.

This approach aligns with Taiwan's broader [Open Government National Action Plan](#), which has institutionalised mechanisms for public participation across governance sectors. Taiwan's open government and [open parliament](#) initiatives offer notable examples of progress, fostering transparency and inclusion through multistakeholder dialogues that reinforce legislative accountability. These efforts reflect Taiwan's broader commitment to ensuring that cybersecurity policymaking, alongside other critical governance matters, remains open, participatory, and grounded in democratic principles.

An illustrative case of the Public Policy Network Participation Platform concerns public discussions surrounding administrative inspections for non-governmental entities (e.g. private companies) as outlined in the initial draft of the CSMA. Key questions raised included:

- Should administrative inspections be triggered only by significant cybersecurity incidents or major deficiencies? Would such limitations risk missing early warning signs?
- Conversely, without such restrictions, could there be concerns regarding potential abuse of authority by central regulatory bodies?
- Are there alternative mechanisms or safeguards that can balance proactive oversight with accountability?

The public raised practical concerns about administrative capacity and whether regulatory authorities have sufficient resources and expertise to conduct effective inspections without professional help. They proposed involving judicial police, cybersecurity experts, or legal professionals during inspections, or exploring alternative measures if such accompaniment is not feasible.

The participatory process yielded concrete recommendations from the public, including:

- Specifying the industries subject to regulation.
- Using granular classifications or business registration criteria.
- Publicising details of inspection processes and outcomes, including pass/fail results, the names of supervising agencies and any accompanying professional bodies.
- Establishing clear procedural rules for inspections to ensure transparency and prevent overreach.

In response to these discussions, policymakers provided clarifications and adjustments to the platform. For example, they refined the scope of regulated entities to prioritise critical infrastructure providers and specific non-governmental organisations subject to a graded cybersecurity responsibility system. Central regulatory authorities deferred details regarding the frequency, content, and methodology of inspections to subsequent subordinate legislation.

Citizens can also further emphasise the importance of ensuring that inspection mechanisms do not disrupt business confidentiality or operations. Suggestions include verifying that cybersecurity mechanisms are functioning as intended, ensuring certificates remain valid, confirming that contracts with cybersecurity vendors adhere to standards, and monitoring the implementation of internal cybersecurity policies or standard operating procedures. This participatory approach shows that although there are incentives to adopt securitised digital

development in Taiwan due to the cyber threats it faces, Taiwan is still trying to develop transparency and include multi-stakeholderism while enhancing its cybersecurity norms.

Innovation through community engagement

In general, Taiwan has integrated cybersecurity into its broader economic and industrial policies, treating it as a pillar of strategic industry development. This approach, which ties security to innovation, aims to enhance competitiveness while mitigating risks, particularly in sectors such as smart manufacturing and 5G networks where vulnerabilities can have widespread implications. [Taiwan's multi-layered cyber defence system](#), supported by a national cybersecurity management platform, allocates responsibilities across agencies according to their roles and emphasises collaboration between the public and private sectors.

Taiwan's transparency in regulatory development is notable, with public consultations incorporated into legislative processes, aligning with democratic principles. However, balancing openness with the urgency required to counter immediate security threats remains a delicate challenge. While Taiwan has positioned itself as a regional leader in addressing cybersecurity challenges, its long-term resilience will depend on improving coordination with Taiwanese civil society, enhancing capacity, and ensuring the agility to adapt to emerging risks.

Grassroots initiatives like g0v.tw, the [Hacks in Taiwan Conference](#) (HITCON), and various hackathons are enriching Taiwan's cybersecurity ecosystem even further. HITCON (台灣駭客年會) has been a pivotal event since its inception in 2005, fostering cybersecurity awareness and advancing technical expertise. The event, organised by the Taiwan Hacker Association, includes conferences, workshops, and training programmes that address global cybersecurity challenges. Initiatives such as the [ZeroDay vulnerability reporting platform](#) and [Capture the Flag competitions](#) highlight HITCON's commitment to building cybersecurity capabilities and nurturing talent. The Taiwan Hacker Association also plays a critical role in bridging academia, industry, and government through events like the Internet of Things hackathons aimed at integrating innovation into the cybersecurity industry and attracting emerging talent.

Other initiatives such as [g0v.tw](#), rooted in the principles of open-source development, promote information transparency and civic participation. By combining online collaboration with offline events such as hackathons, g0v.tw enables citizens to engage in cybersecurity projects, learn technical skills, and collectively address cybersecurity challenges. The government adopted this participatory model, as shown by the [Presidential Hackathon](#) event in 2019. The platform facilitates public-private collaboration, leveraging open data

and technological innovation to optimise public services. Government ministries, including MODA and the Ministry of Health and Welfare, oversee the event, encouraging cross-agency and interdisciplinary cooperation.

Civil society actors such as [MyGoPen and Cofacts](#) have emerged as critical actors in countering information threats. Without relying on formal regulations, these organisations actively promote freedom of expression and empower citizens through fact-checking, media literacy, and public engagement. [MyGoPen](#) focuses on monitoring online content, particularly during sensitive periods like elections, to identify and counter disinformation campaigns. It verifies claims and disseminates accurate information to debunk false narratives that could influence public opinion. Similarly, [Cofacts](#) leverages an AI-powered platform where users can report questionable claims encountered online. Cofacts provides verified responses and educational resources, enabling individuals to distinguish between credible information and falsehoods and fostering a more informed public. Both organisations emphasise grassroots participation by involving citizens directly in the fight against information threats.

Civil society also plays a key role in addressing public concerns about rights to data privacy such as surrounding the [Electronic National Identification Card \(eID\) initiative](#). The Ministry of National Development Council announced plans for the eID in December 2018, with expectations for a full rollout in mid-2020. They designed the new eID to combine features of the existing national ID card and the Citizen Digital Certificate, incorporating an embedded chip for secure digital identity storage.

In September 2019, organisations such as the [Taiwan Association for Human Rights \(TAHR\)](#) and the [Judicial Reform Foundation](#) held press conferences to raise alarms about the potential privacy violations posed by the eID. They criticised the lack of transparency in the rollout process, particularly concerning data management practices and the scope of information stored on the cards.

By May 2020, TAHR launched a [petition](#) opposing mandatory eIDs and advocating for the continued availability of traditional identification cards. With support from over 200 experts, the petition demanded robust privacy legislation before introducing any new digital ID systems, emphasising the need for safeguards to protect personal data. CSOs also pushed for the establishment of an independent data protection agency to oversee eID implementation, stressing the risks associated with integrating databases spanning healthcare, education, and commerce without proper oversight.

Despite the initial plans, [concerns](#) from CSOs about privacy and legal frameworks led to significant delays and ultimately suspended the rollout in 2021. These CSO efforts exemplify

how civil society can counter cyber and information threats through inclusive, education-driven, and non-regulatory approaches. Their efforts strengthen freedom of expression while addressing complex challenges in Taiwan's democratic landscape.

Taiwan's cybersecurity governance shows how democracies can balance national security with civil liberties. Guided by transparency and measured platform engagement, Taiwan resisted policies that could threaten fundamental freedoms. Despite growing pressure towards securitisation, seen in recent legislative proposals incorporating cyber sovereignty concepts, Taiwan maintains its commitment to democratic values while addressing evolving threats. This experience demonstrates that protecting national security does not require authoritarian digital controls, offering valuable insights for democracies worldwide facing similar cybersecurity challenges.

Conclusion

The PRC's cybersecurity and broader digital governance norms rest on the notions of cyber sovereignty, multilateralism, and the securitisation of digital development. Through the Digital Silk Road and related cooperation agreements in the Indo-Pacific, and indeed around the world, the PRC has actively sought to position itself as a global norms-setter in digital governance.

ARTICLE 19's findings highlight how the spread of the PRC's digital governance model has led countries, particularly in the Indo-Pacific region, to adopt restrictive legislation, such as stringent cybersecurity and data localisation laws, often under the guise of national security or digital economy development.

The PRC's emphasis on cyber sovereignty shapes how Indonesia, Pakistan, and Vietnam develop their digital governance frameworks by prioritising state control over cyberspace and explicitly integrating it into national legislation. Indonesia has adopted the PRC's narrative on cyber sovereignty to turn away from a rights-based approach, seen as a Western encroachment, and embrace a PRC-led alternative to digital governance in the Indo-Pacific. Pakistan's legal frameworks include stringent data localisation mandates and censorship. Vietnam's Cybersecurity Law appears directly modelled on the PRC's in adopting similar provisions for data localisation that impose real risks on civil society in the country.

Another defining feature of the PRC's influence on cybersecurity norms noted by ARTICLE 19 in the Indo-Pacific region is the adoption of state-driven surveillance and censorship mechanisms. In Pakistan, the development of a China-style firewall and the integration of surveillance technologies from Chinese companies such as Huawei have significantly expanded the government's capacity to monitor and control online activities. Similarly, Indonesia has engaged in partnerships with Chinese firms to enhance digital surveillance capabilities, including training programmes for cybersecurity professionals. Vietnam has incorporated real-name registration and strict content moderation measures into its cybersecurity laws. ARTICLE 19's findings illustrate a growing alignment with PRC cybersecurity norms.

The PRC has effectively used bilateral institutional collaboration as a vehicle to export its governance model. MoUs with key agencies, such as Indonesia's BSSN, have facilitated direct knowledge transfer and alignment with PRC standards. Capacity-building programmes, often led by Chinese companies, have created dependencies that further entrench PRC norms and practices. These case studies highlight a pattern: by aligning legal frameworks and technological ecosystems with PRC norms, these states have institutionalised mechanisms

that centralise power at the expense of freedom of expression, the right to privacy, and other fundamental freedoms.

In contrast, alternative models, such as those demonstrated by Taiwan, emphasise transparency, multistakeholder engagement, and the protection of human rights within cybersecurity governance laws, policies, and institutions. Taiwan's emphasis on democratic principles and openness offers a path that reconciles national security with the preservation of rights and freedoms. Meanwhile, Taiwan still has room to further improve domestic norms and policies to better embrace a leading role in promoting a rights-based alternative to the PRC authoritarian model.

While Taiwan's internet governance presents an admirable counter-model to the PRC's authoritarian approach, it is not without its challenges. A primary concern lies in its vulnerability to persistent cyberattacks, particularly from the PRC. The growing scale and sophistication of these threats demand a more coherent and resilient cybersecurity strategy that must ensure human rights safeguards. Taiwan also grapples with coordination and capacity challenges within its decentralised governance model. Civil society-led efforts in countering cyber threats, while participatory, underscore the need for more effective multistakeholder coordination mechanisms to effectively address immediate security concerns. At the same time, greater engagement for Taiwan with the international community would benefit international norms-setting, strengthening solidarities to ensure greater pushback against norms diffusion from the PRC.

Priorities for dislodging China's grasp on cyber norms-setting

For the international community

1. Stand with Taiwan

Advocate for Taiwan's participation in global cybersecurity and digital governance discussions to strengthen the international coalition against digital authoritarianism.

2. Support multi-stakeholderism

Encourage governments to involve citizens, civil society, and industry stakeholders in policymaking, mandating public consultations for draft legislation and ensuring Taiwanese stakeholders can engage meaningfully in international forums by creating inclusive mechanisms that amplify democratic voices.

3. Empower rapid response

Mobilise regional networks to gather evidence concerning digital tools and policies, working closely with local civil society to spotlight these issues – while protecting against reprisal – and foster an alliance against rising digital authoritarianism with Taiwan at the centre.

For the Taiwanese Government

4. Prioritise digital human rights within cybersecurity

Taiwan should continue to promote transparency, data protection, and public accountability with laws explicitly safeguarding privacy, free expression, and access to information as the cornerstone of its cybersecurity norms-setting.

5. Lead in global advocacy for rights-based cybersecurity governance

The Taiwanese Government should leverage Taiwan's democratic credentials to promote human rights-centric digital governance internationally, combined with digital diplomacy outreach for capacity-building to support Indo-Pacific nations in developing robust cybersecurity policies aligned with democratic values.

For Taiwanese civil society and private sector

6. Facilitate international monitoring of the PRC's digital influence

Taiwan civil society can work collaboratively with regional partners to document and publicise the negative human rights impacts of PRC-driven initiatives under the Digital Silk Road, especially by leveraging its expertise of PRC threats and influence tactics to help identify new problematic technologies, policies, and practices.

7. Engage in international norms-setting

Taiwan's private sector, and broader civic-tech community, should take advantage of all opportunities to participate in international forums, especially those on internet governance and technical standards-setting.

Appendix: PRC cybersecurity regulations affecting human rights

2011 Internet Information Services Management Measures (互联网信息服务管理办法)*

Article 4	Requires a licensing system for commercial internet information services and a filing system for non-commercial internet information services.
Article 5	Targets internet information providers such as 'news, publishing, education' as requiring review and approval by the state, which leaves them vulnerable to arbitrary restrictions.
Article 14	Specifically singles out service providers of 'news, publishing, and electronic announcements' in compelling the recording of the information content and its release time, IP address, or domain name, while internet access providers must similarly record the user time and IP or domain name. Providers are to keep records for 60 days to be provided to authorities.
Article 15	Holds that internet information service providers shall not 'produce, reproduce, publish, or disseminate' information in violation of 9 categories, including spreading rumours or undermining social stability, which are outside the scope of permissible restrictions on the freedom of expression laid out under international law.

* While predating the 2017 Cybersecurity Law, the measures laid out some of the normative framework further elaborated in subsequent laws and policies and enforcement institutions. It has likewise been cited as among the enabling laws for other, more recent provisions.

Article 12	States that anyone using the internet must not engage in activities endangering national honour and interests, overturn the socialist system, advocate ethnic hatred and ethnic discrimination (which has been used more to prosecute ethnic and religious minorities engaged in rights advocacy), or create or disseminate false information, among others. As with other articles in the law, this is less about actual network security and more about controlling the type of information that is disseminated via networks, which should be outside the scope of any cybersecurity law for its risk of infringement on the right to freedom of expression.
Article 21	Requires network operators to adopt measures for monitoring and recording network traffic data and to store network logs for at least 6 months.
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. This requirement for real-name identification should be taken in tandem with the 2017 MIIT Notice on Cleaning Up and Regulating the Internet Access Service Market, which, among other things, criminalised all non-MIIT approved virtual private networks, critical not only as circumvention tools for evading censorship but also for preserving the right to privacy online.
Article 28	Continues that network operators must provide vaguely defined 'technical support' to public and state security organs, which could be read as a compulsion to comply with surveillance activities.
Article 37	Includes data localisation requirements which hold that CII operators must store 'important data' within mainland China. This requirement, among others, has been used to force companies like Apple to store user data inside the PRC, which has also entailed localising decryption keys.

Article 46	Prohibits individuals and organisations from establishing ‘websites or communication groups’ for ‘imparting criminal methods, the creation or sale of prohibited or controlled items’, or to ‘publish information related to ... other unlawful activities’. Taken together with Article 24 and MIIT provisions, this imposes further restrictions on communicating information about circumvention and anonymity tools, while also effectively prohibiting websites or messaging applications from sharing information about the PRC’s own human rights abuses, from stories about protest to the persecution of ethnic or religious minorities.
Article 48	Requires the broad categories of electronic information distribution and application service providers to censor vague categories of ‘information that laws and administrative regulations prohibit the publication or transmission of’. It compels providers to perform active security management, remove targeted information, store records, and report violators to the authorities. This provision is both a licence for government censorship and a requirement for private actors to pre-emptively screen and censor content prohibited by the authorities. Article 49 goes on to reiterate that such network operators shall cooperate with cybersecurity and information departments of relevant government bodies in implementing their obligations.
Article 50	Continues that the cybersecurity and information departments will conduct security supervision and management, and where they discover ‘prohibited’ information shall instruct network operators to stop its transmission, delete the content, and maintain a record. This obligation also applies to information from outside the PRC, whereby they are to notify relevant bodies to deploy technical measures to block the content. Taken together, Articles 49 and 50 are a blueprint for blanket censorship in the name of cybersecurity.
Article 58	Proffers a legal basis for targeted network interference ‘to protect national security and the social public order’, which may rise to the level of imposing internet shutdowns or broadband throttling, for example, the deliberate slowing down of internet speed as recorded in India, Indonesia, Myanmar, and Pakistan.

2017 National Intelligence Law (中华人民共和国国家情报法)

Article 7	States that 'all organizations and citizens shall support, assist, and cooperate with national intelligence efforts', an obligation equally incumbent upon tech companies abroad.
Article 11	Requires that those engaged in national intelligence work shall 'collect and handle intelligence related to foreign institutions, organisations or individuals' vaguely deemed a threat.
Article 12	Holds that national intelligence institutions 'may establish cooperative relationships' with individuals and organisations and 'retain them to carry out related work'.
Article 13	Holds that intelligence work institutions may compel 'relevant organs, organizations, and citizens' to provide support, assistance, and cooperation.
Article 15	States that intelligence work institutions may employ technical investigation measures.

2021 Data Security Law (中华人民共和国数据安全法)

Article 2	States that if data is handled outside of the PRC in a way that harms national security, public interest, or the 'lawful rights and interests of citizens or organizations of the PRC', then the PRC may pursue legal liability.
Article 26	Justifies reprisal should foreign regulators attempt to limit the PRC's global digital ambitions, noting, 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' that the PRC may take reciprocal measures.

2021 Personal Information Protection Law (中华人民共和国个人信息保护法)

Article 35	Does not require a notification duty for officials collecting personal information under certain vague and overbroad circumstances, such as where notification would impede official duties.
Article 36	Holds that personal identity recognition equipment, such as facial recognition cameras, may be used only for 'safeguarding public security' but this is left entirely to the security sector to define, which leaves open serious loopholes for exploitation such as in the forced collection of biometric data from Uyghurs and Tibetans and personal information collected by the state stored within the PRC.
Article 43	Introduces a right to retaliatory measures against any country or region that adopts vague 'discriminatory prohibitions, limitations or other similar measures' against the PRC relating to personal information. This could be read as a threat of retaliatory action should partners enact limitations on Chinese technology companies handling personal data.



ARTICLE19

article19.org