

Research
Paper

International Law
Programme


Asia-Pacific
Programme

March 2021

Restrictions on online freedom of expression in China

The domestic, regional and
international implications of
China's policies and practices

Harriet Moynihan and Champa Patel



北京市新型冠状病毒肺炎疫情
防控工作新闻发布会
第一百一十六场

北京市人民政府新闻
2020年6月14日

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Summary

- The Chinese government's highly restrictive approach to online freedom of expression has intensified under COVID-19. This has a detrimental effect on the ability of citizens to realize other rights, including the right of access to information, freedom of thought and opinion, and the right to health.
- While Chinese policies and technology have influenced the approach of some countries in the rest of Asia, the breadth, scale, detail and pervasiveness of the government's model of internet control, censorship and surveillance remain unique to China.
- In Asia more broadly, the reasons for tight controls on internet freedoms are complex and diverse – comprising historical, cultural and political factors, and drawing on influences from countries and companies in the West as well as China.
- China's influence on the technology governance of other countries, including in Asia, is on the increase through its 'Digital Silk Road' projects.
- China's restrictive approach to online freedom of expression is reflected on the international stage through advocacy of a broader concept of 'cyber sovereignty' at the UN and in other international forums. Debates over online freedom of expression are increasingly part of broader geopolitical conversations about whether technology governance should be open and global, or closed and state-based.
- At a time when illiberalism was already on the rise, the COVID-19 pandemic has made tighter state control of online freedom of expression even more attractive to many governments. It remains to be seen whether the increasing restrictions enacted under the guise of emergency measures will be repealed once the COVID-19 crisis ends, or whether – as seems more likely – the pandemic will have longer-term detrimental effects on a rights-based approach to technology governance.

Introduction

China has a high number of internet users, estimated at about 990 million,¹ and a host of popular social media applications, including Tencent WeChat, Sina Weibo and Baidu Tieba. This digital access is tempered, however, with extensive domestic laws and regulations that significantly restrict freedom of expression online. COVID-19 has provided the Chinese government with further opportunity to restrict online content and promote the state's own narrative about its handling of the pandemic.

This paper starts by mapping the Chinese government's restrictions on online freedom of expression, drawing on recent examples that have arisen in the COVID-19 context. The paper then analyses the degree to which the situation regarding online freedom of expression in China can be said to be unique, and the degree to which the government's approach shapes wider trends in Asia, both before and during COVID-19. The impact on the region of Western technologies and models is also examined.

Finally, the paper considers the trend of tightening restrictions on online freedom of expression in the broader context of China's growing influence on global technology governance in multilateral and bilateral settings. This includes China's increasing assertiveness in international debates about digital technology regulation, and the country's growing ambitions for its 'Digital Silk Road' initiative.

China's domestic restrictions on online freedom of expression

The Chinese government's restrictive online regime relies on a combination of legal regulations, technical control and proactive manipulation of online debates.² The online environment has tightened considerably under President Xi Jinping, with heavy investment in the 'Golden Shield Project'.³ Such initiatives are a key element in a government vision of 'cyber sovereignty' that allows it to strengthen state surveillance and control.

While Chinese citizens can sometimes access information and communication on the internet through workarounds such as virtual private networks (VPNs), the vast power imbalance between the state and individuals means that freedom of expression online is illusory. In China, there are practically no legal or practical barriers to surveillance online. The various techniques used by the government to restrict online freedom of expression are discussed below.

¹ Statista (2020), 'Number of internet users in China from December 2008 to December 2020', www.statista.com/statistics/265140/number-of-internet-users-in-china (accessed 2 Mar. 2021).

² OpenNet Initiative (2012), 'China', <http://access.opennet.net/wp-content/uploads/2011/12/accesscontested-china.pdf>.

³ Economy, E. (2018), 'The great firewall of China: Xi Jinping's internet shutdown', *Guardian*, 29 June 2018, www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.

Restrictions on content in China

China was already home to one of the world's most sophisticated and restrictive systems of internet control prior to Xi's leadership of the Communist Party of China (CPC). However, regulations and restrictions governing online content have proliferated under his tenure. Since 2015, the spread of false information that seriously disturbs public order constitutes a crime punishable by up to seven years in prison. In 2017, the government implemented a new Cybersecurity Law, which requires social media platforms to republish and link to news articles from state-approved news media.

In order to be permitted to operate, online platforms must abide by state-imposed constraints and cooperate on implementing heavy-handed restrictions on political, social and religious discourse. For example, in January 2018 Weibo suspended several of its accounts after authorities ordered it to 'clean up "wrong-oriented" and "vulgar" information'.⁴ Citizen Lab, at the University of Toronto, has documented how WeChat uses monitored content to train censorship algorithms.⁵

The growing connectivity of Chinese mobile applications means that the consequences of controls on online freedom of expression may play out in other walks of life.

In 2018, the Chinese authorities abolished the State Administration of Press, Publication, Radio, Film and Television – a ministry-level executive agency – and transferred its powers to the Propaganda Department, which is under the direct control of the CPC. Further online content regulations came into effect in March 2020. The Cyberspace Administration of China can suspend or shut down online platforms deemed to breach rules, such as the ban on content deemed 'exaggerated', 'improper' or containing 'sexual provocations', and content 'promoting indecency, vulgarity and kitsch'.⁶

The growing connectivity of Chinese mobile applications means that the consequences of controls on online freedom of expression may play out in other walks of life. Chinese 'super-apps' such as WeChat enable users not just to talk but also to pay for utilities, shop and send money. Such apps make a huge amount of personal data available for analysis by WeChat itself, third parties or the Chinese government.⁷ This data-harvesting capability is only set to increase as WeChat seeks to embed its platform into the Internet of Things (cars, domestic appliances, etc.).

⁴ Human Rights Watch (2019), *World Report 2019*, New York: Human Rights Watch, www.hrw.org/sites/default/files/world_report_download/hrw_world_report_2019.pdf.

⁵ Kenyon, M. (2020), 'WeChat Surveillance Explained', Citizen Lab, 7 May 2020, <https://citizenlab.ca/2020/05/wechat-surveillance-explained>.

⁶ Zhang, B. and Barata, J. (2020), 'Order of the Cyberspace Administration of China (No. 5)', World Intermediary Liability Map (WILMap), 1 March 2020, <https://wilmap.law.stanford.edu/entries/provisions-governance-online-information-content-ecosystem>.

⁷ Privacy International (2017), 'Case Study: Super Apps and the Exploitative Potential of Mobile Applications', 13 August 2017, <https://privacyinternational.org/case-studies/789/case-study-super-apps-and-exploitative-potential-mobile-applications>.

The Chinese government is also running local pilot projects of a 'social credit' system, under which Chinese citizens are scored based on the desirability of their online and offline activity. While the system has yet to be fully rolled out,⁸ there are concerns that criticizing the government on social media could decrease a person's score and trigger wide-ranging implications, including restrictions on free movement.⁹ This would constitute a further chilling effect on online freedom of expression. The cumulative impact of these differing measures is self-censorship online.

There is also an extraterritorial element to the Chinese government's restrictions on online expression. WeChat is not only subject to surveillance and censorship within China, but extends government controls to users around the world.¹⁰ There is evidence that surveillance and political interference are increasing on the international version of the app.¹¹

State-sponsored content and state pressure on content providers

State control over online platforms and content extends to propaganda and the manipulation of information. For example, during the 2019 Hong Kong protests on the proposed Extradition Bill, pro-Beijing news outlets in Hong Kong such as *Wen Wei Po* and *Ta Kung Pao* were mobilized in defence of the proposed measures.¹² Such measures speak to the CPC's broader agenda of trying to influence public debate, media and news reporting within mainland China. These actions also extend globally. Examples include pressure on cable television executives in the US to prevent broadcasts by a station founded by Chinese American Falun Gong practitioners; and a partly Chinese-owned South African newspaper's termination of a column because of the author's writing on Xinjiang.¹³

A related trend is the state's encouragement of, and support for, the amplification of nationalist voices that distort public debates. A prominent example is the online backlash against a Wuhan-based author, Fang Fang, over the English publication of her diaries of the city's coronavirus lockdown.¹⁴ As of 2017, China reportedly had between 500,000 and 2 million internet commentators employed to shape public opinion along the party line.¹⁵

⁸ Sun, Q. (2021), 'China's social credit system was due by 2020 but is far from ready', AlgorithmWatch, 12 January 2021, <https://algorithmwatch.org/en/story/chinas-social-credit-system-overdue>.

⁹ Vinayak, V. (2019), 'The Human Rights Implications of China's Social Credit System', Oxford Human Rights Hub, 6 September 2019, <https://ohrh.law.ox.ac.uk/the-human-rights-implications-of-chinas-social-credit-system>.

¹⁰ Wang, Y. (2020), 'WeChat Is a Trap for China's Diaspora', *Foreign Policy*, 14 August 2020, <https://foreignpolicy.com/2020/08/14/wechat-ban-trump-chinese-diaspora-china-surveillance>.

¹¹ Impiombato, D. (2020) "Page not found": what happens when diplomatic statements meet the WeChat censor', Australian Strategic Policy Institute, 23 September 2020, www.aspistrategist.org.au/page-not-found-what-happens-when-diplomatic-statements-meet-the-wechat-censor.

¹² Nip, J. (2019), 'Extremist mobs? How China's propaganda machine tried to control the message in the Hong Kong protests', *The Conversation*, 15 July 2019, <https://theconversation.com/extremist-mobs-how-chinas-propaganda-machine-tried-to-control-the-message-in-the-hong-kong-protests-119646>.

¹³ Cook, S. (2020), *Beijing's Global Megaphone*, Washington, DC: Freedom House, <https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone>.

¹⁴ Cook, S. (2020), '5 Predictions for Beijing's Assault on Internet Freedom in 2021', *The Diplomat*, 10 December 2020, <https://thediplomat.com/2020/12/5-predictions-for-beijings-assault-on-internet-freedom-in-2021>.

¹⁵ King, G., Pan, J. and Roberts, M. E. (2017), 'How the Chinese government fabricates social media posts for strategic distraction, not engaged argument', *American Political Science Review*, 111(3): pp. 484–501, doi:10.1017/S0003055417000144.

In contrast, the use of internet shutdowns and blackouts to curtail freedom of expression online – a rising trend in illiberal regimes around the world – is less prevalent in China. The government's more advanced and sophisticated system of internet control and censorship reduces the need for such a blunt tool. Nonetheless, there continue to be sporadic media blackouts in China, including in relation to protests in Hong Kong.¹⁶

The relationship between business and the state

In addition to the requirement to censor sensitive content, social media companies operating in China have obligations to the government in relation to the data that they hold on users of their platforms. In China, all social media platforms must be licensed, and users must register their identity information with service providers. This data must be made available to the state. The transfer of information between business and the Chinese authorities is 'comprehensive and systematic ... potentially conferring on the government swift and unfettered access to personal data of increasing intimacy and breadth'.¹⁷ Therefore, individuals' rights to privacy and control over their own data are significantly restricted.

Some technology companies in China have been hesitant to release such data. However, they can be legally compelled to do so.¹⁸ Technology companies that do not operate in China have shown more resistance to Chinese efforts to restrict and control the online sphere. For example, Facebook, Google and Twitter have refused to hand over data on Hong Kong protesters to the Hong Kong police.¹⁹

Internet service providers are also expected to cooperate with Chinese national security agencies when requested. For example, in 2017 Apple removed 60 VPN apps from its online store in China, on the basis that it was legally required to do so as the VPNs were not compliant with new regulations.²⁰ The 2020 Hong Kong National Security Law has further increased pressure on technology companies to hand over data to the authorities,²¹ negatively impacting freedom of expression online in the territory.

Impact of the COVID-19 pandemic on freedom of expression

The COVID-19 pandemic has exacerbated restrictions on online freedom of expression. A notable case was that of Dr Li Wenliang, who was arrested in January 2020 in connection with messages sent to a private social group on WeChat alerting his medical friends to signs of the virus. He was required to sign a statement that he would stop activity that 'severely disturbed social

¹⁶ Tan, D. W. (2019), 'Media blackout of Hong Kong protests in China', *Straits Times*, 2 July 2019, www.straitstimes.com/asia/east-asia/media-blackout-of-hong-kong-protests-in-china.

¹⁷ Khalil, L. (2020), 'Digital Authoritarianism, China and Covid', Lowy Institute Analyses, 2 November 2020, www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid%20.

¹⁸ Ibid.

¹⁹ BBC News (2020), 'Hong Kong: Facebook, Google and Twitter among firms "pausing" police help', 6 July 2020, www.bbc.co.uk/news/technology-53308582.

²⁰ BBC News (2017), 'Apple "pulls 60 VPNs from China App Store"', 31 July 2017, www.bbc.co.uk/news/technology-40772375.

²¹ Kirchgaessner, S. (2020), 'Big tech firms may be handing Hong Kong user data to China', *Guardian*, 30 September 2020, www.theguardian.com/world/2020/sep/30/big-tech-firms-may-be-handing-hong-kong-user-data-to-china.

order'.²² Dr Li later died of COVID-19. This sparked calls for greater freedom of expression in China, with thousands of posts across WeChat and Weibo mourning his death. However, this brief opening was followed by a severe crackdown on content critical of the Chinese authorities' actions. Citizen journalists have been arrested and jailed for videoing or blogging about the coronavirus lockdown in Wuhan.²³

Chinese Human Rights Defenders (CHRD), a network of Chinese and international NGOs, documented 897 cases involving Chinese internet users penalized for their online speech between 1 January and 26 March 2020.²⁴ According to CHRD, 'In the vast majority of these cases, or 93% of the total, police cited "spreading misinformation, disrupting public order" as the pretext for punishing online speech related to [the] COVID-19 outbreak in China.'²⁵

Chinese authorities have given online news outlets strict orders on the coverage of COVID-19 that effectively prevent deviation from the CPC's version of events.²⁶ Technology companies are expected not only to comply with laws restricting content²⁷ but also to promote news from pro-government outlets, including general health information about the virus. Chinese authorities have also restricted publication of academic research on the virus without prior state approval.²⁸ These restrictions have had significant international as well as domestic implications.

Chinese authorities have given online news outlets strict orders on the coverage of COVID-19 that effectively prevent deviation from the CPC's version of events.

For certain minority groups, such as the Uighurs, who have faced increased persecution and detention since 2014, the impact of online restrictions has been immense. Their use of information and communications technology (ICT) – including minority-language websites and social media – was already strictly controlled, but the pandemic has provided cover for further repression.

²² Nip, J. (2020), 'The politics of the coronavirus crisis', East Asia Forum, 15 February 2020, www.eastasiaforum.org/2020/02/15/the-politics-of-the-coronavirus-crisis.

²³ Davidson, H. (2020), 'Wuhan citizen journalist jailed for four years in China's Christmas crackdown', *Guardian*, 28 December 2020, www.theguardian.com/world/2020/dec/28/wuhan-citizen-journalist-jailed-for-four-years-in-chinas-christmas-crackdown.

²⁴ Chinese Human Rights Defenders (2020), 'COVID-19 and Human Rights in China', 3 June 2020, www.nchr.org/2020/06/covid-19-and-human-rights-in-china.

²⁵ Chinese Human Rights Defenders (2020), "A Healthy Society Should Not Have Just One Voice" – China Must End Crackdown on Online Speech in Response to COVID-19', 1 April 2020, www.nchr.org/2020/04/a-healthy-society-should-not-have-just-one-voice-china-must-end-crackdown-on-online-speech-in-response-to-covid-19.

²⁶ Freedom House (2020), *Freedom on the Net 2020: The Pandemic's Digital Shadow*, Washington, DC: Freedom House, https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf.

²⁷ Matsakis, L. (2020), 'How WeChat Censored the Coronavirus Pandemic', *Wired*, 27 August 2020, www.wired.com/story/wechat-chinese-internet-censorship-coronavirus.

²⁸ Gan, N., Hu, C. and Watson, I. (2020), 'Beijing tightens grip over coronavirus research, amid US-China row on virus origin', CNN, 16 April 2020, <https://edition.cnn.com/2020/04/12/asia/china-coronavirus-research-restrictions-intl-hnk/index.html>.

Information and media blackouts in China's Xinjiang region have undermined the Uighurs' ability to access relevant health information, as well as obscuring the extent to which the virus has affected Uighur communities.²⁹

The position under international human rights law

The UN Human Rights Council has held that '... the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice', in accordance with article 19 of the International Covenant on Civil and Political Rights (ICCPR).³⁰ The UN and other international organizations have emphasized that freedom from censorship, including freedom from blocking or filtering of the internet, is central for the exercise of freedom of expression.

The right of access to information is an important part of the right to freedom of expression, as it is needed in order to build opinions and express them. Blocking, filtering and censorship, plus the possibility of criminal prosecution, limit access to information and stifle online debate. State manipulation of the information that citizens are permitted to see (and not see) online also impedes the right of access to accurate information.³¹

Some 173 UN member states have recognized freedom of expression as a legally binding human right by ratifying the ICCPR. While China signed the ICCPR in 1998, it has not ratified the treaty and there is no prospect of it doing so in the short term. However, China is a party to other core UN human rights treaties containing provisions that protect the right to freedom of expression, including the Convention on the Rights of the Child³² and the Convention on the Rights of Persons with Disabilities.³³ In relation to the protection of minority groups, China is a party to treaties that enshrine the right to equal treatment and non-discrimination, including the International Covenant on Economic, Social and Cultural Rights,³⁴ the Convention on the Elimination of All Forms of Discrimination against Women³⁵ and the International Convention on the Elimination of All Forms of Racial Discrimination.³⁶

²⁹ Chaudry, V. (2020), 'The Impact of Covid-19 on Uighur Muslims: An Ignored Crisis', LSE Human Rights blog, 23 April 2020, <https://blogs.lse.ac.uk/humanrights/2020/04/23/the-impact-of-covid-19-on-uighur-muslims-an-ignored-crisis>.

³⁰ UN Human Rights Council (2012), 'Resolution on The Promotion, Protection and Enjoyment of Human Rights on the Internet', 29 June 2012, UN Doc A/HRC/20/L.13.

³¹ Milanovic, M. (2020), 'Viral Misinformation and the Freedom of Expression, Part II', EJIL Talk! Blogpost, 13 April 2020, www.ejiltalk.org/viral-misinformation-and-the-freedom-of-expression-part-ii.

³² Article 13 of the UN Convention on the Rights of the Child, adopted on 20 November 1989, entered into force on 2 September 1990, www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx.

³³ Article 21 of the Convention on the Rights of Persons with Disabilities, adopted on 13 December 2006, entered into force on 3 May 2008, [www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities-2.html](http://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities/convention-on-the-rights-of-persons-with-disabilities-2.html).

³⁴ See Articles 1 and 2 of the International Covenant on Economic, Social and Cultural Rights, adopted on 16 December 1966, entered into force on 3 January 1976, www.ohchr.org/Documents/ProfessionalInterest/cescr.pdf.

³⁵ See Article 3 of the Convention on the Elimination of All Forms of Discrimination against Women, adopted 18 December 1979, entered into force on 3 September 1981, www.ohchr.org/documents/professionalinterest/cedaw.pdf.

³⁶ See Article 5 of the International Convention on the Elimination of All Forms of Racial Discrimination, adopted on 21 December 1965, entered into force on 4 January 1969, www.ohchr.org/en/professionalinterest/pages/cerd.aspx.

Strict regulation of the internet, and government manipulation of the online narrative to enable citizens only to receive the state's version of events, implicates other rights beyond freedom of expression. These include not only civil and political rights such as freedom of association, freedom of assembly, freedom of thought and opinion, and privacy, but also economic and social rights such as the right to health.

The right to information is particularly important in the context of a pandemic, so that citizens can understand the risks to their health and how to protect themselves from the virus. The right to health – set out in the International Covenant on Economic, Social and Cultural Rights – includes the right to seek, receive and impart information and ideas regarding health issues, and the right to have personal health data treated with confidentiality.³⁷ China's restrictions on online discussions of the handling of the virus meant that some citizens were unable to access adequate information or medical care in the early days of the outbreak.³⁸ In some cases, such as that of Dr Li Wenliang, a lack of free expression also implicated the right to life.

The regional perspective: situating China's position on online freedom of expression within trends in Asia

Restrictions on online freedom of expression are not unique to China; indeed, they are increasing in many countries worldwide.³⁹ Among China's neighbours in Asia, countries with diverse political systems have enacted laws placing tight controls on free expression online and enabling surveillance. As with China, these restrictions have worsened as a result of emergency measures introduced under COVID-19.

The restriction of internet freedoms is notably stringent in Asia. For example, of the 213 internet shutdowns documented across the world in 2019, 143 took place in Asian countries.⁴⁰ Since 2019, two of the longest internet shutdowns have taken place in Asia: in India (in relation to Kashmir);⁴¹ and in Myanmar⁴² (in Rakhine and Chin states). In June 2020, the UN high commissioner for human rights, Michelle Bachelet, appealed to Asian countries to ensure their

³⁷ Office of the High Commissioner for Human Rights (2000), 'CESCR General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12)', Committee on Economic, Social and Cultural Rights, adopted 11 August 2000, www.refworld.org/pdfid/4538838d0.pdf.

³⁸ Human Rights Watch (2021), 'China: Seekers of Covid-19 Redress Harassed', 6 January 2021, www.hrw.org/news/2021/01/06/china-seekers-covid-19-redress-harassed.

³⁹ Shahbaz, A. and Funk, A. (2019), 'Freedom on the Net 2019: The Crisis of Social Media', Freedom House, <https://freedomhouse.org/report/freedom-net/2019/crisis-social-media>.

⁴⁰ Access Now (undated), Shutdown Tracker Optimization Project (STOP) Dataset, www.accessnow.org/keepiton (accessed 3 Mar. 2021).

⁴¹ Wallen, J. (2021), 'High speed internet restored in Kashmir after 'world's longest' blackout', *Telegraph*, 6 February 2021, www.telegraph.co.uk/news/2021/02/06/high-speed-internet-restored-kashmir-worlds-longest-blackout.

⁴² The Wire (2020), 'Human Rights Groups Criticise 'World's Longest Internet Shutdown' in Myanmar', *The Wire*, 28 June 2020, <https://thewire.in/south-asia/myanmar-worlds-longest-internet-shutdown>; and Hlaing, K. H. (2020), 'People in Parts of Myanmar Are Living Under the World's Longest Internet Shutdown. It's Putting Lives in Danger', *Time*, 16 November 2020, <https://time.com/5910040/myanmar-internet-ban-rakhine>.

efforts to combat false information about the pandemic adhered to the principles of legality, necessity and proportionality. This was in response to the use of 'fake news' laws being used to criminalize freedom of expression.⁴³

Unlike Africa, the Americas and Europe, which all have regional human rights treaties that enshrine the right to freedom of expression, as well as regional human rights courts to supervise the implementation of those rights by states parties,⁴⁴ Asia has no regional human rights instrument, and no human rights court.

Restrictions on online freedom of expression in Asia

As with China, even before the pandemic a number of South Asian and Southeast Asian governments had enacted laws to stifle online dissent. For example, in 2008 Indonesia enacted a law on information and electronic transactions. Passed to protect consumers in electronic transactions, it has also been used to criminalize political dissidents.⁴⁵ In 2018, Malaysia criminalized the sharing of misinformation, making it the first Southeast Asian country to do so.⁴⁶

In 2019, Singapore passed the Protection from Online Falsehoods and Manipulation Act, which gives government authorities the power to demand corrections, remove content and block webpages if content is deemed to be against the public interest or to undermine public interest in the government.⁴⁷ In November 2019, Thailand's government launched an 'Anti-Fake News Center' to combat unverified news on social media;⁴⁸ civil society organizations argue that it could be misused to suppress free speech and dissent.⁴⁹

Internet censorship and emergency laws during COVID-19

As in China, the prevalence of such laws, and of government actions based on them, has increased in Asia during the COVID-19 pandemic. Emergency measures restricting online freedom of expression can be observed in Bangladesh, India, Indonesia, Malaysia, Myanmar, Nepal, Pakistan, the Philippines, Sri Lanka, Thailand and Vietnam.

For example, since mid-March 2020 authorities in Bangladesh have arrested at least a dozen people under the Digital Security Act 2018 for comments about the coronavirus; those detained have included a doctor, opposition activists and

⁴³ UN News (2020), 'Asian countries urged to honour right to freedom of expression, over pandemic fear', UN News, 3 June 2020, <https://news.un.org/en/story/2020/06/1065532>.

⁴⁴ Article 9 of the African Charter on Human and Peoples' Rights, Article 13 of the American Convention on Human Rights, and Article 10 of the European Convention on Human Rights.

⁴⁵ Hamid, U. (2019), 'Indonesia's Information Law has threatened free speech for more than a decade. This must stop', *The Conversation*, 25 November 2019, <https://theconversation.com/indonesias-information-law-has-threatened-free-speech-for-more-than-a-decade-this-must-stop-127446>.

⁴⁶ Funke, D. and Flamini, D. (undated), 'A guide to anti-misinformation actions around the world', Poynter, www.poynter.org/ifcn/anti-misinformation-actions.

⁴⁷ Wong, T. (2019), 'Singapore Fake News law polices chats and online platforms', BBC News, 9 May 2019, www.bbc.com/news/world-asia-48196985.

⁴⁸ Tanakasempipat, P. (2019), 'Thailand unveils 'anti-fake news' center to police the internet', Reuters, 1 November 2019, www.reuters.com/article/us-thailand-fakenews-idUSKBN1XB480.

⁴⁹ Zsombor, P. (2019), 'Thailand's Anti-Fake News Center Fans Fears of Censorship', VOA News, 6 October 2019, www.voanews.com/east-asia-pacific/thailands-anti-fake-news-center-fans-fears-censorship.

students.⁵⁰ In the Philippines, the government passed Republic Act No. 11469, which criminalizes the making and spreading of false information on social media and other platforms.⁵¹ In less than a month after its implementation, the government arrested 47 people for alleged violations of the law.⁵²

In India, criminal law has been used against doctors from a private hospital in Aurangabad for allegedly spreading rumours on WhatsApp. On 25 February 2021, the Indian government announced new rules to regulate social media that will (among other things) require social media companies to take down misinformation or unlawful or violent content within 24 hours. The new rules have been criticized by rights groups for increasing the government's power over content on social media platforms.⁵³

Like China, several countries in the region have also been pressuring social media and other technology platforms to combat 'misinformation' on their sites. In Vietnam, for instance, state-owned telecom companies throttled traffic to Facebook, effectively restricting access to the platform, until Facebook agreed to take down content the Vietnamese government deemed anti-state.⁵⁴

Heightened surveillance during COVID-19 has raised concerns regarding the expansion, normalization and institutionalization of surveillance even after the pandemic ends.

Suppression of freedom of expression online is supported by growing state surveillance capacities, which are evident in several countries in Asia besides China. Indeed, Asia has been branded 'the world's surveillance hotspot', with new surveillance powers being assumed in 2020 by governments in Cambodia, India, Myanmar, Pakistan, the Philippines and Thailand.⁵⁵ Heightened surveillance during COVID-19 has raised concerns regarding the expansion, normalization and institutionalization of surveillance even after the pandemic ends.⁵⁶

Not every government in the region has increased restrictions on online freedom of expression during the pandemic. Taiwan has emerged as an exemplar of the democratic practice of providing open spaces for free expression online, leveraging

⁵⁰ Human Rights Watch (2020), 'Bangladesh: End Wave of COVID-19 'Rumor' Arrests', Human Rights Watch, 31 March 2020, www.hrw.org/news/2020/03/31/bangladesh-end-wave-covid-19-rumor-arrests.

⁵¹ Joaquin, J. J. B. and Biana, H. T. (2020), 'Philippine crimes of dissent: Free speech in the time of COVID-19', *Crime, Media, Culture*, pp. 1–5, doi: 10.1177/1741659020946181.

⁵² Ibid.

⁵³ See, for example, Access Now (2021), 'Indian authorities tighten control over online content', 25 February 2021, www.accessnow.org/indian-authorities-tighten-control-over-online-content.

⁵⁴ Nguyen, A. (2020), 'Vietnam's Government is Using COVID-19 to Crack Down on Freedom of Expression', *Slate*, 8 May 2020, <https://slate.com/technology/2020/05/vietnam-coronavirus-fake-news-law-social-media.html>.

⁵⁵ Nazalya, S. (2020), 'Asia emerges as world's surveillance hotspot', Human Rights Outlook 2020, Verisk Maplecroft, 30 September 2020, www.maplecroft.com/insights/analysis/hro-asia-emerges-as-worlds-surveillance-hotspot.

⁵⁶ Chok, L. (2020), 'The policy black box in Singapore's digital contact tracing strategy', LSE Southeast Asia Blog, 22 September 2020, <https://blogs.lse.ac.uk/seac/2020/09/22/the-policy-black-box-in-singapores-digital-contact-tracing-strategy>.

its existing digital infrastructure and strong state–civil society relations to create open channels of information regarding the pandemic. Rather than clamp down on free expression, the authorities have ensured the dissemination of factual information in an accessible form to the public. However, Taiwan remains the exception rather than the rule.

Diverse influences

The role of Chinese technologies and models

The scale and pervasiveness of China's model of internet control, censorship and surveillance are unique. The evidence suggests that, in controlling, censoring and monitoring internet users, governments in Asia are generally using their own tactics and adopting restrictions selectively, rather than copying China's stringent form of digital authoritarianism chapter-and-verse.

Nonetheless, some countries have sought to emulate the Chinese government's draconian approach to the online space. Vietnam's cybersecurity law draws directly from the Chinese model in stifling any form of political speech that the state deems undesirable rather than simply minimizing cybersecurity threats.⁵⁷ Myanmar's new draft cybersecurity bill, proposed by the military State Administration Council in the wake of the military coup of February 2021, reflects the same principles of the Chinese and Vietnamese laws in giving the junta extensive powers to access individuals' data, restrict or suspend access to the internet, and detain critics.⁵⁸ Calls for cyber sovereignty are by no means unique to authoritarian regimes in the region, having also been raised in India.⁵⁹

The Chinese government also actively seeks to influence other countries in Asia on internet governance through development projects. Under the aegis of the 'Digital Silk Road', part of the Chinese government's Belt and Road Initiative (BRI), Chinese companies have been entering into projects abroad to provide or improve ICT networks and capabilities, including through the laying of underground cables; the establishment of smart cities; and the installation of artificial intelligence (AI), cloud computing or surveillance technology capabilities. Chinese exports of surveillance technologies have found purchase among a wide range of countries in the region, including India, Malaysia and Thailand. Chinese-exported internet controls have been found to be most common in countries participating in the BRI, and spread more easily and often to countries with authoritarian or hybrid regimes.⁶⁰ Myanmar and Nepal are both recipients of Chinese infrastructure

⁵⁷ Sherman, J. (2019), 'Vietnam's Internet Control: Following in China's Footsteps?', *The Diplomat*, 11 December 2019, <https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps>.

⁵⁸ Human Rights Watch (2021), 'Myanmar: Scrap Sweeping Cybersecurity Bill', 12 February 2021, www.hrw.org/news/2021/02/12/myanmar-scrap-sweeping-cybersecurity-bill.

⁵⁹ Leigh, K., Kravchenko, S. and Rai, S. (2019), 'How 'Cybersovereignty' Splits the Once World Wide Web', Bloomberg, 2 May 2019, www.bloomberg.com/news/articles/2019-05-02/how-cybersovereignty-splits-the-once-world-wide-web-quicktake.

⁶⁰ Weber, V. (2019), *The Worldwide Web of Chinese and Russian Information Controls*, Washington, DC: Open Technology Fund, https://public.opentech.fund/documents/English_Weber_WWW_of_Information_Controls_Final.pdf.

projects to lay down fibre-optic links. In November 2020, President Xi Jinping pledged to further deepen cooperation with ASEAN countries through promotion of the Digital Silk Road.⁶¹

Media officials and journalists from the Philippines, Thailand and Vietnam have also received training in China on 'new media development'.⁶²

Notwithstanding this influence in its various forms, there is a certain wariness among Southeast Asian countries about the purchase of particular types of Chinese-made hardware, such as equipment for use in 5G telecoms networks. There is also general awareness, at least in Southeast Asia, of the risks involved in China's control over vast amounts of data.⁶³

China is not the only influence on approaches to online freedom of expression in the region. Culture and history also play a role. Many states in the region have had an uneasy relationship with international human rights law and standards.⁶⁴ The Bandung Principles, adopted in 1955, underline the central importance of mutual respect for sovereignty, the principle of non-interference in other states' internal affairs, non-aggression, political self-determination and equality among the 29 participant countries from Asia and Africa, most of which had recently become independent after colonial rule. In an 'Asian values' approach to human rights, community is prioritized over the individual, and socio-economic rights, including the right to development, prevail over civil and political rights.⁶⁵

Dignity, equality and fairness are a more dominant part of the discourse in Asia than, for example, the right to privacy, on which there has been so much focus in Western democracies during the pandemic. But the salience of the right to freedom of expression online is particularly resonant in the region when linked to socio-economic rights such as the right to health in the context of a pandemic.

The role of Western technologies and models

Western policies and technology have also influenced online freedom of expression in Asia. Amnesty International recently found that three companies, based in France, the Netherlands and Sweden respectively, have been exporting digital surveillance systems such as facial-recognition technology and network cameras to China's state security agencies.⁶⁶ Western companies have also exported surveillance technology to other countries in Asia, including India, the Philippines and Singapore.⁶⁷ Due to concerns about the role that some Western technology

⁶¹ Zhou, L. (2020), 'Let's build a digital silk road: Xi Jinping looks to cement China's ties with Asean', *South China Morning Post*, 27 November 2020, www.scmp.com/news/china/diplomacy/article/3111612/lets-build-digital-silk-road-president-xi-promises-ways-china.

⁶² Shahbaz, A. (2018), 'The Rise of Digital Authoritarianism', Freedom House, <https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism>.

⁶³ Center for Strategic & International Studies (2019), 'China's Digital Silk Road and Southeast Asia', Commentary, 15 February 2019, www.csis.org/analysis/chinas-digital-silk-road-and-southeast-asia.

⁶⁴ Saul, B. (2019), essay in *Security and Prosperity in Asia: The Role of International Law*, Chatham House Conference Paper, November 2019, www.chathamhouse.org/sites/default/files/CHHJ7378-International-Law-Research-Paper-INT-191031-WEB.pdf.

⁶⁵ Ibid; and Moynihan, H. (2018), 'Exploring Public International Law Issues with Chinese Scholars – Part 4', Chatham House Meeting Summary, 2–3 June 2018, www.chathamhouse.org/sites/default/files/publications/research/2018-06-02-Roundtable4-summary.pdf.

⁶⁶ Amnesty International (2020), *Out of Control: Failing EU Laws for Digital Surveillance Export*, www.amnesty.org/download/Documents/EUR0125562020ENGLISH.PDF.

⁶⁷ Carnegie Endowment for International Peace (2020), 'AI Global Surveillance (AIGS) Index', https://carnegieendowment.org/files/AI_Global_Surveillance_Index1.pdf.

exporters play in aiding human rights abuse overseas, the EU recently agreed to tighten rules on the sale and export of dual-use goods such as facial-recognition technology and spyware, where such technology could be used for human rights violations.⁶⁸

There is also some evidence that certain legislation from Europe has influenced models for curtailing online expression in Asia. Research by the Future of Speech Project indicates that at least 13 countries – including India, Malaysia, Pakistan and the Philippines – have adopted or proposed models similar to the German Network Enforcement Act (NetzDG). This law obliges social media platforms with 2 million or more users to remove illegal content – including hate speech and speech causing religious offence – within 24 hours, or risk fines of up to €50 million.⁶⁹ In practice, the laws in Asian countries allow far greater discretionary powers to governments than does the German law, but the latter has nevertheless become a reference point.⁷⁰ For example, Singapore's wide-ranging Protection from Online Falsehoods and Manipulation Act allows a minister to issue directions to internet intermediaries to correct or disable 'false statements of facts'.⁷¹ The vagueness of the language leaves it liable to abuse, including the targeting of political dissent. Prior to the adoption of the bill, a preliminary report referenced the German law.⁷²

Freedom House notes that powerful US-based technology companies with significant penetration in Asia – including Facebook (which owns WhatsApp and Instagram), Twitter and Google – have contributed to restrictions on online freedom of expression. The failure of US and other policymakers to regulate these platforms has enabled them to be exploited by anti-democratic forces, including in Asia.⁷³ For example, Facebook, which has more than 18 million users in Myanmar, has admitted that the platform was used to incite violence in Myanmar against the Rohingya people.⁷⁴ Such platforms have also served as conduits for disinformation and hate speech in the region.

But dominant US-based social media platforms are at least taking some measures to tackle these online harms. Facebook and Twitter have instituted a number of policies to address hate speech, civic integrity and influence operations in

⁶⁸ Euronews (2020), 'A win for global human rights' as EU agrees on tighter rules for surveillance tech exports', 9 November 2020, www.euronews.com/2020/11/09/a-win-for-global-human-rights-as-eu-agrees-on-tighter-rules-for-surveillance-tech-exports.

⁶⁹ Mchangama, J. and Fiss, J. (2019), *The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship*, Justitia Report, Copenhagen: Justitia, <http://justitia-int.org/en/the-digital-berlin-wall-how-germany-created-a-prototype-for-global-online-censorship>.

⁷⁰ The German NetzDG law does not create new categories of illegal content and is only an iteration of existing statutes in the German criminal code with regard to hate speech. In comparison, some of the laws in Asia are more restrictive and rely on broad and vague categories of content such as 'blasphemy' (Indonesia), 'embarrassing or slanderous information' (Vietnam), or 'false statements of facts' that the government considers to be harmful and untrue (Singapore).

⁷¹ Republic of Singapore (2019), 'Protection from Online Falsehoods and Manipulation Act 2019', Singapore Statutes Online, <https://sso.agc.gov.sg/Acts-Supp/18-2019>.

⁷² Mchangama and Fiss (2019), *The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship*.

⁷³ Shahbaz and Funk (2019), 'Freedom on the Net 2019: The Crisis of Social Media'.

⁷⁴ BBC (2018), 'Facebook admits it was used to 'incite offline violence' in Myanmar', BBC Asia, 6 November 2018, www.bbc.co.uk/news/world-asia-46105934.

the past year.⁷⁵ Indeed, Western online platforms are increasingly coming into conflict with governments in Asia over demands to censor or restrict online content. In Thailand, Facebook and the government have threatened each other with legal action over whether content critical of Thailand's royal family should remain online.⁷⁶ In India, where Facebook has nearly 300 million users, a Facebook page for agitating farmers was taken down by Facebook in February 2021 then restored following public outrage on social media.⁷⁷ In Myanmar, Facebook restricted the accounts of Myanmar's military for spreading 'misinformation' in the wake of the imposition by the military of an internet shutdown that blocked access to Facebook, Twitter and Instagram.⁷⁸

The EU and some Western democracies are striving to come up with regulation that tackles online harms of global platforms while preserving freedom of expression. The EU's draft Digital Services Act⁷⁹ and the UK's proposals for an Online Safety Bill,⁸⁰ both published in December 2020, are grounded in a proportionate, risk-based approach that seeks to regulate online systems as a whole, focusing on the policies and procedures of relevant technology companies rather than on specific online content. These proposals, which are still at an early stage, are the product of multi-stakeholder consultations, and aim to promote greater transparency for users and greater accountability of technology companies. Other countries, including Ireland and Australia, are seeking to adopt similar approaches in draft legislation on online harms.⁸¹

So while the reasons for tight controls on internet freedoms in Asia are complex and diverse (and draw on myriad influences), the gulf between the increasingly rights-centric approach favoured by some Western countries and companies, on the one hand, and the model pursued by the Chinese government, on the other, is widening.

⁷⁵ See for example, Clarke, C. (2020), 'Facebook announces new hate speech policies after Unilever joins advertising boycott', *The Drum*, 26 June 2020, www.thedrum.com/news/2020/06/26/facebook-announces-new-hate-speech-policies-after-unilever-joins-advertiser-boycott; Twitter (2020), 'Expanding our policies to further protect the civic conversation', 10 September 2020, https://blog.twitter.com/en_us/topics/company/2020/civic-integrity-policy-update.html; and Facebook (2021), 'February 2021 Coordinated Inauthentic Behaviour Report', 3 March 2021, <https://about.fb.com/news/2021/03/february-2021-coordinated-inauthentic-behavior-report>.

⁷⁶ Holmes, O. (2017), 'Thailand deadline for Facebook to remove illicit content passes', *Guardian*, 16 May 2017, www.theguardian.com/world/2017/may/16/thailand-deadline-for-facebook-to-remove-illicit-content-passes; and Lloyd Parry, R. (2020), 'Facebook forced to block page criticizing Thai royal family', *The Times*, 25 August 2020, www.thetimes.co.uk/article/facebook-forced-to-block-page-criticising-thai-royal-family-c6ldt7ddq.

⁷⁷ *National Herald* (2021), 'Facebook restores farmers' page but silent on why it was taken down', 21 December 2020, www.nationalheraldindia.com/india/facebook-restores-farmers-page-but-silent-on-why-it-was-taken-down.

⁷⁸ Disis, J. and Lockwood, P. (2021), 'Facebook restricts Myanmar military's accounts for spreading misinformation', *CNN Business*, 12 February 2021, <https://edition.cnn.com/2021/02/12/tech/facebook-myanmar-military-intl-hnk/index.html>.

⁷⁹ European Commission (2020), 'The Digital Services Act: ensuring a safe and accountable online environment', https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en.

⁸⁰ Department for Digital, Culture, Media & Sport; Home Office (2020), 'Online Harms White Paper: Full government response to the consultation', CPN 354, 15 December 2020, www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response.

⁸¹ Government of Ireland (2020), 'Online Safety and Media Regulation Bill', published on 10 January 2020, www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill; and Government of Australia (2020), 'Consultation on a Bill for a new Online Safety Act', www.communications.gov.au/have-your-say/consultation-bill-new-online-safety-act.

International implications of China's position on online freedom of expression

The Chinese government aims for China to become a technological superpower in the coming years. This aim includes leading in the development of AI, super-apps, 5G, smart cities and surveillance technology. But it also involves seeking to shape the global rules of technology governance. China is increasingly exporting its own approach to technology governance in the international context – through a vision of 'cyber sovereignty' that entails tight control of internet gateways, data localization and robust restriction of online freedoms.

China's ability to shape global technology governance has expanded significantly in the past 10 years. At the international level, this is a product of two factors: China's growing presence and influence at the UN; and its provision of digital infrastructure in a significant number of countries around the world as part of the 'Digital Silk Road' initiative. China's approach to online freedoms, including freedom of expression, is thus an important factor in global debates on the future of the internet.

Advancing the 'cyber sovereignty' model in international forums

Two bodies at the UN – the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace, and an Open-Ended Working Group working on a similar mandate⁸² – are currently debating the rules and norms that should apply to state behaviour in the digital realm. China is advocating for government control of the internet as the basis for international cooperation. This stance frames technology governance through a sovereignty and national security lens, without reference to individual freedoms. It promotes multilateral cooperation purely between states, as opposed to a multi-stakeholder model, favoured by many Western states, that also involves technology companies, civil society organizations, academics and other non-state actors.

China is increasingly exporting its own approach to technology governance in the international context – through a vision of 'cyber sovereignty' that entails tight control of internet gateways, data localization and robust restriction of online freedoms.

China has leveraged its networks in a series of minilateral forums, including the Shanghai Cooperation Organization (SCO) and the BRICS grouping, as well as in the BRI, to garner support for its approach to technology governance. The SCO submitted a Code of Conduct for Information Security, spearheaded

⁸² The full titles are the 'Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Field of Information Security' and the 'Open-Ended Working Group on Developments in the Field of Information Communication Technologies in the Context of International Security'.

by China and Russia, to the UN General Assembly in 2011, which proposed rules of behaviour in cyberspace. The draft code, which was revised and resubmitted in 2015,⁸³ has so far failed to attract widespread support because it is seen by some states as an attempt to entrench greater state control of the internet. But China and Russia continue to lobby strongly and consistently for 'cyber sovereignty' in the UN and other international forums.

Other actions by China on global technology governance also reflect manifestations of an overall vision of 'cyber sovereignty' based on state control of the internet at the expense of individual freedoms. China supported Russia's resolution, adopted by the UN General Assembly in 2019, to establish a committee of experts to consider a new cybercrime treaty. The draft resolution has been criticized by human rights groups for raising serious human rights concerns, including vague language that could facilitate the criminalization of legitimate expression online.⁸⁴

Additionally, in September 2020, China put forward an international Data Security Initiative, consisting of a framework with eight elements. The framework is premised on data localization, and the idea that states control the personal data of their citizens, as opposed to individual users having a contract with their service providers that is underwritten by human rights standards on freedom of expression, privacy and data protection.⁸⁵

China has rapidly increased its influence on standard-setting at the UN, and at other international standardization bodies for emerging technology such as AI, the Internet of Things and blockchain, including through securing leadership positions at the International Telecommunication Union (ITU) and putting forward a greater number of technical proposals to the ITU than any other country.⁸⁶ Chinese diplomats and technology companies have been advocating at the ITU for a decentralized internet infrastructure, which would lead to a more centralized, top-down version of the internet.⁸⁷ There are concerns that, as well as giving states more control over the internet, this 'New IP' could ultimately drive the fragmentation of the internet, which would increase cybersecurity threats while reducing legal certainty and predictability in cyberspace. Even based on existing Internet Protocol, several countries have followed China's lead in asserting greater government control over the internet, as with Russia's Sovereign Internet Law,⁸⁸ which entered into force in January 2021.

⁸³ NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (undated), 'An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?', <https://ccdcoc.org/incyber-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new>.

⁸⁴ 'Open Letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online' (undated), www.apc.org/sites/default/files/Open_letter_re_UNGA_cybercrime_resolution_0.pdf.

⁸⁵ Mueller, M. (2020), 'China's Data Security Initiative: Still Stuck in the Sovereignty Box', Internet Governance Project, 16 September 2020, www.internetgovernance.org/2020/09/16/chinas-data-security-initiative-still-stuck-in-the-sovereignty-box.

⁸⁶ Von Wijnen, A. (2020), 'The new power of technical standards', FreedomLab, 25 September 2020, <https://freedomlab.org/the-new-power-of-technical-standards>.

⁸⁷ Hoffmann, S., Lazanski, D. and Taylor, E. (2020), 'Standardizing the splinternet: how China's technical standards could fragment the internet', *Journal of Cyber Policy* 5(2), 29 August 2020, pp. 239–64.

⁸⁸ Human Rights Watch (2020), 'Russia: Growing Internet Isolation, Control, Censorship', 18 June 2020, www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.

China has also been creating new institutions on technology governance, including an International Research Centre for Big Data in support of the Sustainable Development Goals (SDGs).⁸⁹ The location of the centre in China represents a counterbalance, in an increasingly multipolar world, to the multiplicity of international institutions created by and based in the West. But it remains to be seen to what extent the centre will uphold the goal of SDG 16.10, 'to ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements'. In 2016, China was one of a number of countries that opposed a UN Human Rights Council resolution adopted on the promotion, protection and enjoyment of human rights on the internet. The opposing countries had suggested amendments that would have removed from the resolution key language from the ICCPR on the right to freedom of expression regardless of frontiers.⁹⁰

In the five years since that resolution, China has strengthened its influence in the UN Human Rights Council, evolving from a passive participant to an active rule-shaper.⁹¹ China's growing 'discourse power' in this area is reflected in the adoption by the council of two resolutions, proposed by China in 2018 and 2020, that reposition international human rights law as a matter of state-to-state relations without a meaningful role for civil society, rather than as an area of law centred on the individual.⁹²

This positioning on human rights in turn informs China's approach to online freedoms and technology governance. Many authoritarian and illiberal governments are attracted to a model that promotes the economic benefits of the internet while neutering the risk of citizens speaking up or protesting online. This is particularly the case during the current pandemic, when states are seeking to exert greater control over their citizenry, and over the narrative of their handling of the crisis.

Export of the 'cyber sovereignty' model through the Digital Silk Road

The 'Digital Silk Road', which provides a vehicle for the export of both China's technology and its approach to technology governance, is an increasingly important part of China's foreign policy. While China has a number of Digital Silk Road projects on its own doorstep, increasingly the initiative is focused further afield, particularly in Africa.⁹³ China provides more financing for ICT in Africa than all multilateral agencies and leading democracies do across the continent.⁹⁴

⁸⁹ Chinese Academy of Sciences (2020), 'CAS to Launch Int'l Research Center of Big Data for SDGs', 27 September 2020, http://english.cas.cn/newsroom/news/202009/t20200926_244297.shtml.

⁹⁰ Article 19 (2016), 'UNHRC: Significant resolution reaffirming human rights online adopted', 1 July 2016, www.article19.org/resources/unhrc-significant-resolution-reaffirming-human-rights-online-adopted.

⁹¹ Piccone, T. (2018), *China's Long Game on Human Rights at the United Nations*, Washington, DC: Brookings Institution, www.brookings.edu/wp-content/uploads/2018/09/FP_20181009_china_human_rights.pdf.

⁹² Richardson, S. (2020), *China's Influence on the Global Human Rights System*, Washington, DC: Brookings Institution, www.brookings.edu/wp-content/uploads/2020/09/FP_20200914_china_human_rights_richardson.pdf.

⁹³ Feldstein, S. (2020), 'Testimony before the U.S.-China Economic and Security Review Commission, Hearing on China's Strategic Aims in Africa', 8 May 2020, www.uscc.gov/sites/default/files/Feldstein_Testimony.pdf.

⁹⁴ Arcesati, R. (2020), 'The Digital Silk Road is a development issue', Mercator Institute for China Studies (MERICS), 28 April 2020, <https://merics.org/en/analysis/digital-silk-road-development-issue>.

China has also expanded its Digital Silk Road into the Middle East,⁹⁵ where many countries favour a sovereign and controlled internet and have enacted cybercrime laws incompatible with international human rights law, including freedom of expression.⁹⁶ At a joint investment forum in 2019, China and Saudi Arabia signed 35 economic cooperation agreements, including for the development of smart cities.⁹⁷

However, China's foreign policy ambitions in relation to the cyber sovereignty model are complicated by the fact that, in practice, multiple actors are involved – not just the CPC, but also technology companies and their users. China's approach to internet regulation, both within and outside the country, is therefore a constant process of negotiation between the government, 'big tech' and citizenry. Any idea of the Digital Silk Road as cohesive and powered purely from above is thus oversimplistic.⁹⁸ Investment does not always turn into influence,⁹⁹ and in practice there are tensions between what Chinese companies want (including profit and some transparency) and what the CPC and central government want.

China's approach to internet regulation, both within and outside the country, is a constant process of negotiation between the government, 'big tech' and citizenry.

We are nonetheless starting to see greater centralization and institutionalization of the BRI, as reflected in the evolution of the initiative between the first summit in May 2017 and the second in April 2019.¹⁰⁰ The degree of control that China exerts over Chinese technology companies is also reflected in the suspension of technology firm Ant Group's initial public offering in November 2020,¹⁰¹

⁹⁵ Zinser, S. (2020), 'China's Digital Silk Road Grows with 5G in the Middle East', *The Diplomat*, 16 December 2020, <https://thediplomat.com/2020/12/chinas-digital-silk-road-grows-with-5g-in-the-middle-east>.

⁹⁶ Hakmeh, J. (2018), *Cybercrime Legislation in the GCC countries: Fit for Purpose?*, Research Paper, London: Royal Institute of International Affairs, www.chathamhouse.org/2018/07/cybercrime-legislation-gcc-countries/freedom-expression-online-under-gcc-cybercrime-laws.

⁹⁷ Hoffman, Lazanski and Taylor (2020), 'Standardizing the splinternet: how China's technical standards could fragment the internet', p. 254.

⁹⁸ Triolo, P. and Greene, R. (2020), 'Will China control the global internet via its Digital Silk Road?', *SupChina*, 8 May 2020, <https://supchina.com/2020/05/08/will-china-control-the-global-internet-via-its-digital-silk-road>. See also Jones, L. and Hameiri, S. (2020), *Debunking the Myth of 'Debt-trap Diplomacy'*, Research Paper, London: Royal Institute of International Affairs, www.chathamhouse.org/2020/08/debunking-myth-debt-trap-diplomacy.

⁹⁹ Segal, A. (2017), *Chinese Cyber Diplomacy in a New Era of Uncertainty*, Aegis Paper Series 1703, Stanford, CA: Hoover Institution, Stanford University, 2 June 2017, p. 11, www.hoover.org/research/chinese-cyber-diplomacy-new-era-uncertainty.

¹⁰⁰ Tiezzi, S. (2019), 'Who Is (and Who Isn't) Attending China's 2nd Belt and Road Forum?', *The Diplomat*, 27 April 2019, <https://thediplomat.com/2019/04/who-is-and-who-isnt-attending-chinas-2nd-belt-and-road-forum>.

¹⁰¹ Sender, H. (2020), 'Jack Ma vs. the Party: Inside the collapse of the world's biggest IPO', *Nikkei Asia*, 18 November 2020, <https://asia.nikkei.com/Spotlight/The-Big-Story/Jack-Ma-vs.-the-Party-Inside-the-collapse-of-the-world-s-biggest-IPO>.

and the fact that the group's high-profile founder and former executive chairman, Jack Ma, a leader in UN norm development in digital cooperation,¹⁰² disappeared from public view for three months.¹⁰³

The idea of a straight dichotomy between the approach of the 'sovereign internet' group of states on the one hand, and states that support an open and global internet on the other, can also be overblown. The reality is more nuanced, with many states (including democracies) increasingly striving for some degree of 'data sovereignty' to protect their own companies and markets from US and Chinese technology giants,¹⁰⁴ and to create a secure data ecosystem governed by their own laws. The trend for data sovereignty has seen governments blocking apps by foreign providers (in 2020, India blocked 59 Chinese apps, including the popular TikTok and WeChat),¹⁰⁵ banning foreign telecoms providers (for example, the measures against China's Huawei by Australia, Japan, New Zealand, Taiwan, the UK and the US),¹⁰⁶ and restricting cross-border data flows. Where data sovereignty involves a government impinging on the privacy and personal data of individuals without adequate safeguards, it can be harmful to individual rights. But data sovereignty need not be incompatible with internet freedoms – for example, the GAIA-X initiative, the EU's plan for a unified cloud ecosystem, aims to preserve privacy and civil liberties.¹⁰⁷

Nevertheless, the increasing divide between the group of states, led by China and Russia, that advocate for greater state control of the internet and those advocating for an open and global internet has led to fears of a fragmented internet in the future.¹⁰⁸ Now that China is seeking to realize its technology ambitions on a global scale, the differences between China's 'cyber sovereignty' model on the one hand, and Western proposals for internet regulation rooted in international human rights standards on the other, are likely to come into sharper relief.

¹⁰² United Nations (2019), *The age of digital interdependence: Report of the UN Secretary-General's High-Level Panel on Digital Cooperation*, <https://digitalcooperation.org/report>.

¹⁰³ Bram, B. (2021), 'Jack Ma was China's most vocal billionaire. Then he vanished', *Wired*, 13 January 2021, www.wired.co.uk/article/jack-ma-disappear-ant-group-ipo.

¹⁰⁴ Scott, M. (2019), 'What's driving Europe's new aggressive stance on tech', *Politico*, 27 October 2019, www.politico.eu/article/europe-digital-technological-sovereignty-facebook-google-amazon-ursula-von-der-leyen.

¹⁰⁵ Griffin, A. (2020), 'TikTok banned in India along with 58 other mostly Chinese apps amid border tensions', *The Independent*, 29 June 2020, www.independent.co.uk/life-style/gadgets-and-tech/news/tiktok-ban-india-china-wechat-uc-browser-a9591941.html.

¹⁰⁶ Goodier, M. (2020), 'The definitive list of where every country stands on Huawei', *Tech Newstatesman*, 29 July 2020, <https://tech.newstatesman.com/security/where-every-country-stands-huawei>.

¹⁰⁷ Palantir (2020), 'Palantir and GAIA-X', Palantir Blog, Medium, 18 December 2020, <https://medium.com/palantir/palantir-and-gaia-x-85ab9845144d> (accessed 25 Jan. 2021).

¹⁰⁸ For discussion of the emerging camps, see Morgus, R., Woolbright, J. and Sherman, J. (2018), *The Digital Deciders: How a group of often overlooked countries could hold the keys to the future of the global internet*, Florida International University – New America Cybersecurity Capacity Building Partnership (C2B Partnership), www.newamerica.org/cybersecurity-initiative/reports/digital-deciders.

Conclusion

The post-Second World War order, including the UN Charter and the Universal Declaration of Human Rights, was constructed from principles and values that were agreed by a wide range of states, including representatives from the Republic of China.¹⁰⁹ But the intervening decades have witnessed seismic geopolitical power shifts, and a rapidly changing environment in which human rights are increasingly contested and politicized for strategic ends, with new and emerging powers seeking to redefine international norms.

One such contested space is online freedom of expression. Debates over online freedom of expression are increasingly part of broader geopolitical conversations about whether technology governance should be open and global, or closed and state-based. Technology has become increasingly pervasive in our lives, and the providers of that technology increasingly international. Moreover, the values informing that technology increasingly dictate how free, fair and inclusive the society using the technology can be, as well as the balance of power between the state and individual citizens. A fragmented and state-controlled internet not only carries troubling implications for individual rights online, such as freedom of expression; without an open, stable and secure internet, achievement of the SDGs and economic growth will also be more difficult.

At a time when illiberalism was already on the rise, COVID-19 has made tighter state control of online freedom of expression even more attractive to many governments. It remains to be seen whether the increasing restrictions enacted under the guise of pandemic-related emergency measures will be repealed once the COVID-19 crisis ends, or whether – as seems more likely – COVID-19 will have longer-term detrimental effects on an open and rights-based approach to technology governance.

¹⁰⁹ The Republic of China was recognized by the UN until 1971, when it was expelled and the UN General Assembly adopted a resolution recognizing the People's Republic of China as the only lawful representatives of China in the UN.

About the authors

Harriet Moynihan is a senior research fellow with the International Law Programme at Chatham House. Harriet leads on the programme's cyber and online work, including the relationship between international human rights law and internet governance. Harriet was formerly a legal adviser at the Foreign & Commonwealth Office, and in 2019 was a visiting fellow at the Bonavero Institute of Human Rights at the University of Oxford, where her research focused on internet governance.

Dr Champa Patel is the director of the Asia-Pacific Programme at Chatham House. Before joining Chatham House, she was the regional director and senior research adviser for the South Asia and Southeast Asia and Pacific offices of Amnesty International, responsible for managing the research, campaigns, media and advocacy for the region.

Acknowledgments

The authors would like to thank Urvashi Aneja, Renata Dwan, Sam Daws, Angelina Chamuah, Joyce Hakmeh and Tim Summers for their input into this paper.

The paper draws on insights from a roundtable held in November 2020 under the Chatham House Rule. The authors would like to thank the participants at that meeting, who gave generously of their time and provided valuable perspectives. The opinions expressed in this publication belong to the authors alone.

Sincere thanks are also due to the anonymous peer reviewers; Chanu Peiris and Jacqueline Rowe in the International Law Programme; Lucy Ridout and Chloe Sageman in the Asia-Pacific Programme; and Jake Statham for editing the paper, along with the wider Chatham House communications team.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical including photocopying, recording or any information storage or retrieval system, without the prior written permission of the copyright holder. Please direct all enquiries to the publishers.

Chatham House does not express opinions of its own. The opinions expressed in this publication are the responsibility of the author(s).

Copyright © The Royal Institute of International Affairs, 2021

Cover image: A press conference on the prevention and control work of the COVID-19 epidemic is held by the Information Office of Beijing Municipality on 14 June 2020 in Beijing, China.

Photo credit: Copyright © Han Haidan/China News Service/Getty Images

ISBN 978 1 78413 463 1

This publication is printed on FSC-certified paper.
designbysoapbox.com



Independent thinking since 1920



The Royal Institute of International Affairs
Chatham House

10 St James's Square, London SW1Y 4LE

T +44 (0)20 7957 5700

contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223