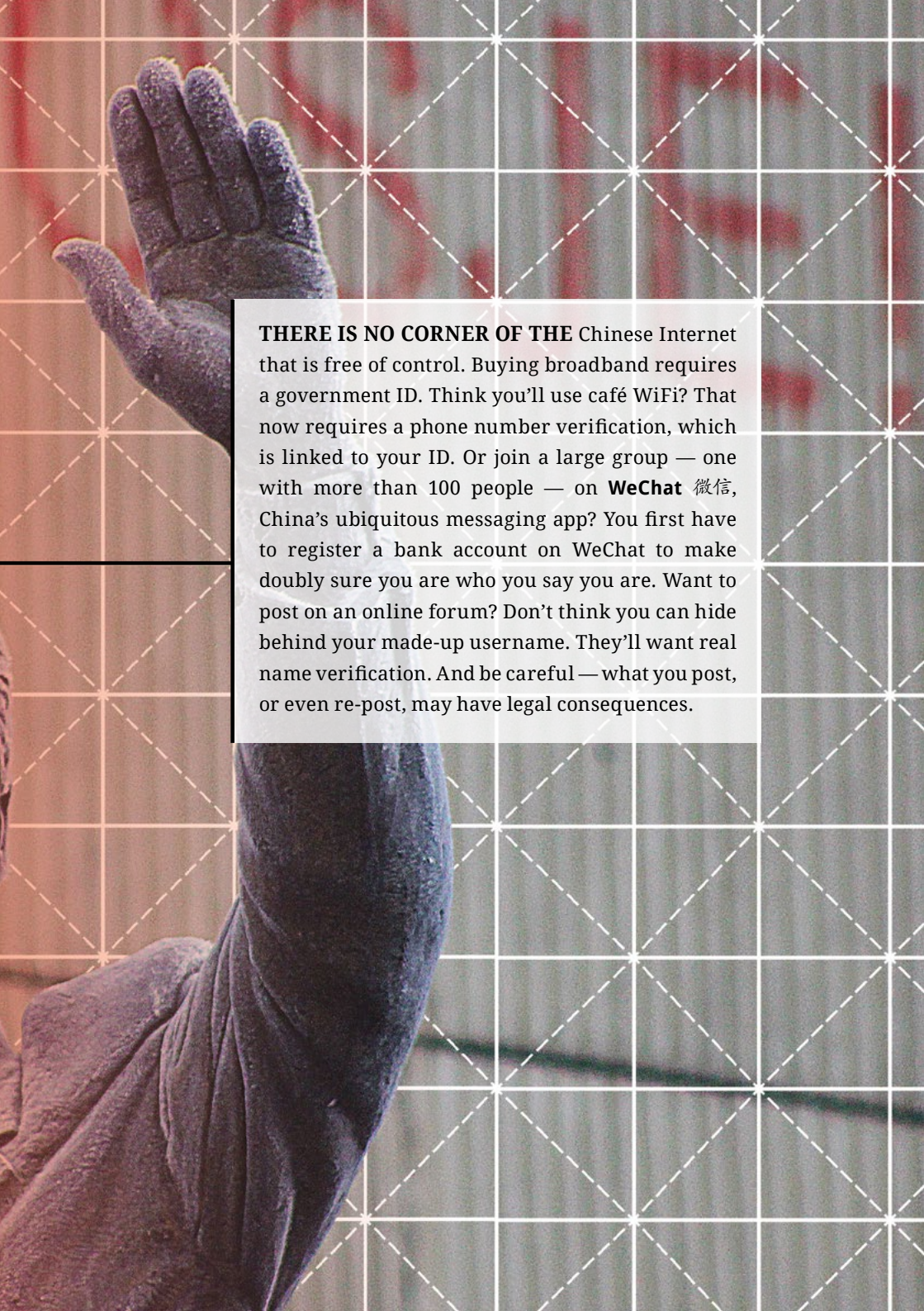
6月
7月
8月
9月
10月
11月
12月
2016年1月
2月
3月
4月
5月
6月
7月
8月
9月

6

‘NAILING JELLO TO A WALL‘

Lorand Laskai

Frozen statue of Bill Clinton in Pristina, Kosovo
Source: Agron Beqiri, Wikimedia Commons



THERE IS NO CORNER OF THE Chinese Internet that is free of control. Buying broadband requires a government ID. Think you'll use café WiFi? That now requires a phone number verification, which is linked to your ID. Or join a large group — one with more than 100 people — on **WeChat** 微信, China's ubiquitous messaging app? You first have to register a bank account on WeChat to make doubly sure you are who you say you are. Want to post on an online forum? Don't think you can hide behind your made-up username. They'll want real name verification. And be careful — what you post, or even re-post, may have legal consequences.

Lu Wei, the man who 'nailed Jello to a wall'
Photo: Wikimedia Commons

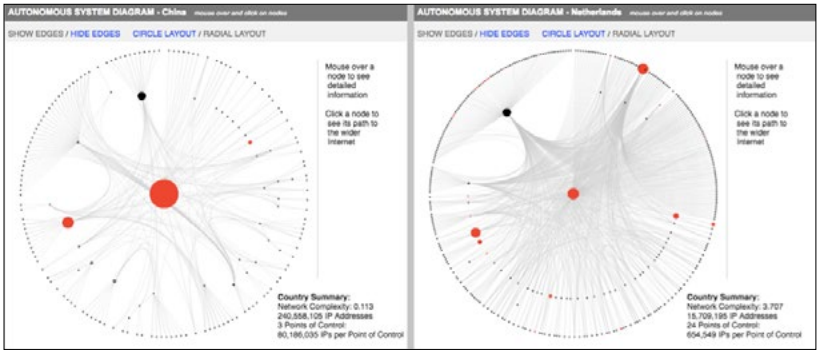
Back in 2014, Lu Wei 鲁炜, until recently the head of the Cyber Administration of China 国家互联网信息办公室 (CAC), said, 'The Internet is like a car. If it has no brakes … once it gets on the highway you can imagine what the end result will be. And so, no matter how advanced, all cars must have brakes.' As China's Internet gatekeeper, Lu was prone to metaphor about the need for order in cyberspace: in those same remarks, he described 'freedom and order' as 'twin sisters' that 'must live together'.[1] The Chinese Internet of 2016 has more than just brakes — it is subject to a regime of ever-stricter control and supervision. A Chinese individual in 2016 has a better chance of anonymity offline than online, away from the thousand prying eyes of China's army of censors.

In the early days of the Internet, many people globally assumed that cyberspace would elude the state's effort to control it. US President Bill Clinton famously quipped in 2000 that controlling the Internet would be like 'nailing jello to a wall'. 'Liberty will spread by cell phone and phone modem', he proclaimed. 'Imagine how much it could change China.'[2]

Chinese officials imagined just this — and then took steps to stop it. In the mid-1990s, China's Ministry of Public Security 公安部 (MPS) kicked off its 'Golden Shield Project' 金盾工程 — a far-ranging attempt to harness emerging information technologies for policing.[3] Officials envisioned the integration of citizens' official files into a nationwide registry and the inception of data-driven surveillance. Yet they were also aware that developments in informational technology could outpace the speed at which the Party could control it. As the number of Internet users skyrocketed (from 22 million in 2000 to 721 million by 2016), the MPS focused on the more immediate task of stemming the virtual flow of unfiltered information into the country. They set up a series of filters and blocks at Internet

'choke points' where fibre-optic cables entered the country. The Internet in the US and other places is designed specifically to be porous and lack 'choke points', but for China these access points served as digital borders that needed to be controlled. With the help of the American technology conglomerate Cisco, they installed mirroring routers — the same filtering technology used by companies or schools, just on a much larger scale — that reflect the pulsating light of incoming traffic into government servers, creating an effective digital veto by which the authorities could keep unwanted websites or keywords from entering the country.

Today, the 'Great Firewall' — a name given to China's multifaceted system of Internet censorship by Geremie R. Barmé and Sang Ye in an article they wrote for *Wired* magazine in 1997 — is a sophisticated, finely tuned machine. The Great Firewall not only involves blocking external information, but also finding and proscribing politically-sensitive content generated from within China. It is not only capable of censoring content across the Chinese Internet, but also promotes a culture of self-censorship and control. International observers supposed that such control would stifle the ingenuity that led to the rise of IT hubs like Silicon Valley elsewhere in the world. Instead, China's regime of online control has spurred its own form of domestic technological innovation and entrepreneurship, creating mini-Silicon Valleys across the country.



Mappings of comparative routes to the outside web shows the vast difference between China, where two IPs (Internet Protocol address) filter a majority of traffic, and the Netherlands, which has 24 points of control
Source: cyber.harvard.edu/netmaps/geo_map_home.php

Apple 'appears' to have made special accommodations in China by putting user data on government servers and installing a government-required WiFi protocol on phones, the US Justice Department have said
Photo: Baetho, Flickr

In April 2016, US trade officials formally accused China's Great Firewall of being what the executives at foreign Internet companies have been calling it for years: a 'trade barrier'.[4] Chinese Internet regulators demand that companies surrender a much higher degree of control over software and user data than foreign companies can reasonably provide. Not only are China's Internet regulations and censorship cumbersome and hard to navigate, but technology companies, including Apple, that have broken into the Chinese market risk endangering their position on user privacy globally. In February 2016, China made an unexpected appearance during a showdown between Apple and US law enforcement over the San Bernardino gunman's encrypted iPhone, which Apple refused to unlock for investigators. During the court hearings, prosecutors cited Apple's compliance with Chinese government requests to undercut Apple's pro-user privacy position.[5] Whether or not Apple secretly provided Chinese authorities with a backdoor to circumvent user encryption protection — as a Faustian bargain for access to the Chinese market — remains a lingering concern among privacy advocates.[6]

By changing the rules of the Internet, the Chinese government has been able to nurture a trio of domestic Internet giants, commonly known as BAT (**Baidu** 百度, **Alibaba** 阿里巴巴集团, and **Tencent** 腾讯), which is willing to subscribe to the Party's regime of control. Most censorship doesn't occur at the internet service provider (ISP) level, but on individual platforms, which Chinese companies must police vigilantly.[7] It's no surprise that Chinese super-apps such as WeChat are built to facilitate censorship, creating a

seductively convenient — and easily manageable and monitored — online space where the user can chat, bank, order taxis, send money to other users, pay bills, and even donate to charities. As Chinese apps and technology interweave with Chinese citizens' everyday existence, so does Beijing's control.

Freedom and Order: The Legacy of Lu Wei

On 29 June, without explanation or warning, the Chinese media reported that Lu Wei had stepped down from head of CAC, ending his three-year tenure as China's all-powerful Internet gatekeeper.[8] Although Lu's brash, flamboyant style had made him enemies, his sudden deposition, unaccompanied by any sign of a clear political future, caught many observers by surprise. The media hailed his successor, Xu Lin 徐麟, who is close to Xi Jinping and previously served as Shanghai's propaganda chief, as China's biggest 'political star'.[9]

Xu Lin
Photo: cpc.people.com.cn

Whatever the reason for Lu's dismissal — a half a year later, the cause of Lu's fall remains unclear — his legacy is beyond question. While Internet freedom advocates celebrated the expansion of the free web, Lu launched a successful bid to bring China's cyber environs under state control, proving that China could assert its 'cyber sovereignty' 网络主权. So far, Xu Lin has proven to be a reliable steward of Lu's legacy, mobilising the expanding bureaucracy he created to police the Chinese web while keeping a lower profile than the attention-hungry Lu.

Early on, Lu showed an appreciation of the Internet that eluded most cadres in the Party. Writing in 2010, Lu argued in an article in *Seeking Truth* 求是 — the Party's theory journal — that China would not have national security until it achieved 'information security' 信息安全. When Xi

Jinping took power in 2013, the Internet was posing an ever-more complex and vexing challenge to CCP rule. Activists in the Middle East and elsewhere were using the Internet to help wage revolutions and people's revolt. Meanwhile, China's own forums and message boards were filling up with a unique class of independent voices: 'self-media' 自媒体, or what might be called public opinion 'influencers' which could hijack the public discourse from the stodgy propagandists with a single **Weibo** post — a prospect that the Chinese government found increasingly inconvenient. When a high-speed train in Wenzhou derailed in 2011 and the government attempted to cover up both the details of the tragedy and its cause (construction compromised by corruption), netizens poked holes in the official story faster than censors could erase their comments. They mocked and criticised the government, whipping up public anger into a frenzy that led to a series of official apologies, including an emphatic, personal apology from the president of the Shanghai Metro, Yu Guangyao 俞光耀, in the form of a bow during a televised press conference. In an article at the time, *New Yorker* journalist Evan Osnos quoted a Weibo user saying that the bow was a 'sign of progress'.

Yu Guangyao
Photo: Baike

Evidently, government officials were eager to avoid bowing too frequently, and Lu Wei was ready to help their cause. He was tasked with imposing government control over China's raucous virtual public square, first as the chairman of the State Council Information Office 国务院新闻办公室 (SCIO), then as the head of the CAC. Lu showed that the same tools of fear and intimidation used by authoritarian states to police its citizens offline were equally effective online. As Xi Jinping said in a secret speech on propaganda and ideology work in 2013, which was later leaked to

China Digital Times 中国数字时代, authorities would need to 'unsheathe the sword' 亮剑 to win the public opinion struggle online.[10] Lu did just that, adding a little showmanship in the process.

Charles Xue
Photo: YouTube

After taking over the SCIO, Lu assembled the most influential online social icons (often known as the Big Vs for having verified accounts on Weibo) for dinner outings, where he warned them that speaking out against the Party would have repercussions. As if to prove his point, in August 2013, while Lu was hosting his star-studded soirées, Chinese authorities arrested Charles Xue 薛必群 — a Chinese American businessman and influential microblogger. While he was arrested for soliciting prostitution, no one doubted the real reason for his arrest. In a humiliating televised-forced confession, Xue stated that he had used his online influence irresponsibly to stroke his vanity, saying that fame online made him feel like an 'the emperor of the Internet'.[11] Other would-be Internet emperors took notice. A former employee of Weibo, who worked in the online platform's censorship department in Tianjin between 2011 and 2013, told the Committee to Protect Journalists:

> The effect was felt immediately. The amount of original posting dropped rapidly. Users not only withdrew from serious commentary, but became reluctant to post about what they heard or saw in their daily lives, because any information not confirmed by government authorities could potentially be deemed as creating or spreading rumours.[12]

In 2014, Xi Jinping convened the first meeting of the Central Leading Group for Internet Security and Informatisation 中央网络安全和信息化领

April 2016: Xi Jinping presides over a symposium on cyberspace security and informatisation in Beijing
Source: news.cn

导小组, and established the CAC with a broad mandate for cyber control with Lu Wei at the helm. Under Lu, online censorship spiked. The CAC began requiring real-name verification for online activity and pushed for the criminalisation of the act of spreading of online 'rumours'. (See the *China Story Yearbook 2014: Shared Destiny*, Chapter 3 'The Chinese Internet 'Unshared Destiny', pp.106–123).

Lu also dispelled any doubt that China's biggest Internet companies, which are privately owned, could be effective collaborators with the Party — even if following the Party's tune occasionally required a little nudge. The CAC normalised the practice of summoning leading tech executives to the CAC office for reprimand. In 2015, in a rare public censure, the CAC even threatened to close down **Sina** 新浪 — China's largest news portal — if the company did not tighten censorship of its online news service.[13]

For the most part, however, officials have used the carrot rather than the stick to get Internet companies to work with the Party-state to achieve its vision for the Internet. The state leads the drive to increase popular access to the Internet, bringing millions of new Chinese users online each year — from the companies' perspective, customers. It pays to be on the

Party-state's good side. (See Forum 'Crayfish, Rabies, Yoghurt, and the Little Refuting-Rumours Assistant, pp.225–227.)

During Lu's tenure, online content frequently disappeared without any apparent rhyme or reason. This is because the actual work of censorship in China is highly decentralised, managed between local CAC offices and individual platforms and sites (which are responsible for self-policing). Researchers at the University of Toronto's Citizen Lab compiled a list of keywords blocked on China's three major video streaming apps and found that they differed from platform to platform.[14] There was one notable exception: each platform blocked the name of its competitors.

In December 2015, Lu Wei suggested that, like most people, he too had been inconvenienced by censorship, but that 'online space and actual society are the same — we want freedom but also order'.[15] It's clear the CAC wants Chinese netizens to subscribe to the same logic and become active participants in the policing of their fellows. Websites and online platforms such as WeChat feature a prominent 'report' 报告 button. The website of the CAC itself seeks to educate and involve people in the censorship

The caption above the image reads: 'Today is so-called "April Fools' Day" in the West. 'April Fools' Day does not accord with Chinese traditional values or socialism's core value system. We hope everyone will not believe, start, or spread rumours ☺'
Image: Weibo

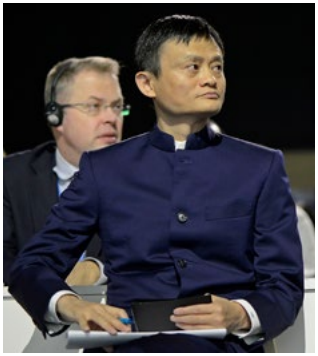
process by publishing rafts of statistics on censored content and sites that have been shut down. During one 'clean up' 净网 operation in 2016 alone, the CAC claimed to have shut down over one million accounts and closed more than 2,000 sites for disseminating 'pornography, false rumours, and violent or other illegal content'.[16] If you want to report content directly to the CAC yourself? The site provides an easy to remember phone number and URL (12377.cn). There's even an app.

The caption reads: 'Clients offered new "one-click reporting" service'
Source: cac.gov.cn

Spiritual Garden or Cultural Wasteland?

With its legions of censors and culture of self-censorship, the Chinese Internet has become, in Xi's words, 'clean and chipper' 晴朗 — at least as far as direct threats to Party rule are concerned. But the CCP aspires to a higher plane of control, in which China's Internet becomes nothing less than a 'spiritual garden' 精神家园 — an ennobling space where netizens complete their transformation into perfect citizens.[17] With over 700 million users, the Internet is increasingly the Party's most direct channel to its citizens, and it employs both online spectacle and its command over information to achieve this end.

In recent years, both Party publications and journals of theory have given expression to dreams of control and the potential of big data to enhance state control in the online sphere. The high-level policy document released in September outlining the government's plan for a 'Social Credit System' 人信用监督 brought such dreams one step closer to reality. (See Forum 'Cyber Loan Sharks, Social Credit, and New Frontiers of Digital Control', pp.213–222.) In a speech to an audience of 1.5 million political and



Jack Ma
Photo: UNclimatechange, Flickr

legal officials in October, Alibaba's Jack Ma 马云 teased officials with what big data could accomplish — and implicitly what Alibaba could offer the government — by describing a *Minority Report*–style future in which big data could predict who will commit a crime, providing 'a kind of predetermined sentencing'.[18]

For the time being, the CCP is focused on what officials like to refer to as a 'cleansing' 清理 of the Internet to eliminate harmful elements. At a conference on cyber security and propaganda in 2015, Lu Wei said that the government must 'consciously eliminate filth and mire such as online rumours, online violence, sex, and vulgarity', and 'foster online behavioural norms that venerate virtue and are inclined towards the good, use outstanding ideas, morals and culture to nourish the network and nourish society'.[19]

In 2016, authorities took solid aim at the 'filth and mire'. In April, The State Administration of Press, Publication, Radio, Film, and Television 国家广播电影电视总局 (SAPPRFT) censured Jiang Yilei 姜逸磊, a celebrated comedian and online blogger known as 'Papi Jiang' ('Papi' 酱), for using vulgar language. A number of freewheeling videos were removed from her Youku 优酷 channel, though after vowing to 'broadcast more positive energy', she was allowed to continue posting videos.[20] Other targets of the Party's drive for web purity were less lucky. In 2016, authorities cracked down on China's growing live-streaming sites, doling out strict new regulations and imposing harsh punishments on online users found violating the rules.

Papi Jiang
Photo: YouTube

Examples of 'vulgar' content that finds its way to the front pages of China's top news portals
Source: *Phoenix News, Red Net,* and *China News*

One twenty-one-year-old 'cam girl', Xue Liqiang 雪梨枪 was sentenced in November to four years in prison for posting obscene videos.[21]

SAPPRFT also imposed strict new guidelines and approval processes on the burgeoning online gaming scene. The leaked transcripts of one Chinese game company's exchanges with the regulators revealed a frustrating and expansive list of official concerns, from bare-chested male characters, to 'forbidden characters' (like death 死 or rob 抢), and the excessive use of English-language words.[22]

The Party's 'cleansing' of the Internet does not appear to have left it on the cusp of 'a golden age of Internet culture' 联网文化的黄金时代, as state-media has declared, but rather with less culture.[23] In the months after Papi Jiang's censure, and her voluntary adoption of 'positive energy', the comedian's star has faded. And despite the Party's best attempts and claims to the contrary, the Chinese Internet today is far from a clean, moral space. It is rife with financial and other scams, salacious content, and rumours.

As for regular media portals, the CAC regularly censures news sites for lewd content, 'clickbait' headlines, and rumour peddling. In July, it issued a strict ban on media outlets from quoting unverified information sourced on social media.[24] Yet without credible, independent media, rumours and disinformation spread like wildfire. The Party's solution: more control.

Avoiding the 'Digital Qing'

At the Cybersecurity and Informationalisation Work Conference 网络安全和信息化工作座谈 in April, President Xi began his most important speech of the year on Internet control with a journey through history.[25] 'There have been three major qualitative leaps in social development', Xi said, 'the agricultural revolution, the industrial revolution, and now the informational revolution. The China of the Qing dynasty was caught unprepared by the industrial revolution, resulting in one hundred years of national humiliation. China today must, by contrast, embrace the potential of the informational revolution to achieve the great rejuvenation of the Chinese nation.'

Chinese officials and the media often repeat that China is an 'Internet big country' 网络大国 on its way to becoming an 'Internet superpower' 网络强国. Most countries consider the Internet in terms of open borders and win-win cooperation. In contrast, China has applied the nation-state paradigm to the Internet, constructing digital borders and casting Internet development as a zero-sum arms race. On 7 November 2016, the National People's Congress 全国人民代表大会 (NPC) gave this view legislative force with the new Cybersecurity Law 网络安全法, ignoring intense opposition from international tech companies. The law's requirements for data localisation, strict real-name verification, and for companies to provide the government with 'technical assistance' (possibly digital backdoors) on request strongly disadvantages foreign tech companies — although Facebook is trialling censorship mechanisms that might allow it back in.[26] **Xinhua** 新

The Yarovaya Law refers to a pair of Russian federal bills passed in 2016 that tighten counter-terrorism and public safety measures in Russia. It is known to the public under the last name of one of its creators — Irina Yarovaya
Image: en.kremlin.ru

华 lauded the passage of the law and hailed Xi as an 'Internet Sage' 网络达人 who has mustered the troops to fight for China's Internet future.[27] Among those 'troops' are some of the world's biggest tech and Internet companies (including **Huawei** 华为 as well as Baidu, Tencent, and Alibaba, all of which are expanding their international clout. Gone are the days when Chinese authorities needed Cisco to help it build the Great Firewall.

At occasions such as meetings of the Internet Corporation for Assigned Names and Numbers and the Ten-Year Review of the World Summit on the Information Society (see Chapter 8 'Making the World Safe (for China)', pp.276–293), Beijing has defied the ideal of a unified, borderless web, asserting instead the concept of 'cyber sovereignty' — a concept that appeals to a number of authoritarian regimes around the world. In November, reports surfaced that Chinese officials and Huawei executives were in conversation with Russian officials about selling the data storage technologies needed to implement the Yarovaya Law, which requires companies to store data about Russian citizens within Russia and mirrors China's own data localisation drive.[28] Other governments, including Iran, Egypt, and Cambodia have expressed interest in similar Chinese

technology that would help them assert control over its own cyberspace. Chinese netizens joked about the Chinese government is bundling Internet control with other popular Chinese exports: 'buy a high-speed rail and we'll throw in a Great Firewall for free' 买高铁送防火墙.[29]

During last year's Paris terrorist attacks, the Chinese media contrasted the peaceful, calm space of the Chinese Internet to such foreign platforms as Twitter and Instagram, where radical jihadists may organise and recruit. The message had resonance beyond China. Even in the West, confidence in the idea of a 'free web' has given way to concerns over just how free might be too free. During the US election season, experts and policymakers fretted that online 'fake news' 虚假新闻, Internet trolls, and Russian bots were sowing chaos on the country's much-vaunted free web. Most American commentators would likely be surprised to hear that China has been combatting 'fake news' and 'clickbait' or 'sensationalist headline writers' 标题党 for years. Not to mention that the Party is always on guard against 'hostile foreign forces' 敌对外国势力, especially in cyberspace. Increasingly, China's model of Internet control looks like a bellwether of the Internet's future. Maybe jello can be nailed to a wall after all?

This text is taken from *China Story Yearbook 2016: Control*,
edited by Jane Golley, Linda Jaivin and Luigi Tomba, published 2017 by
ANU Press, The Australian National University, Canberra, Australia.