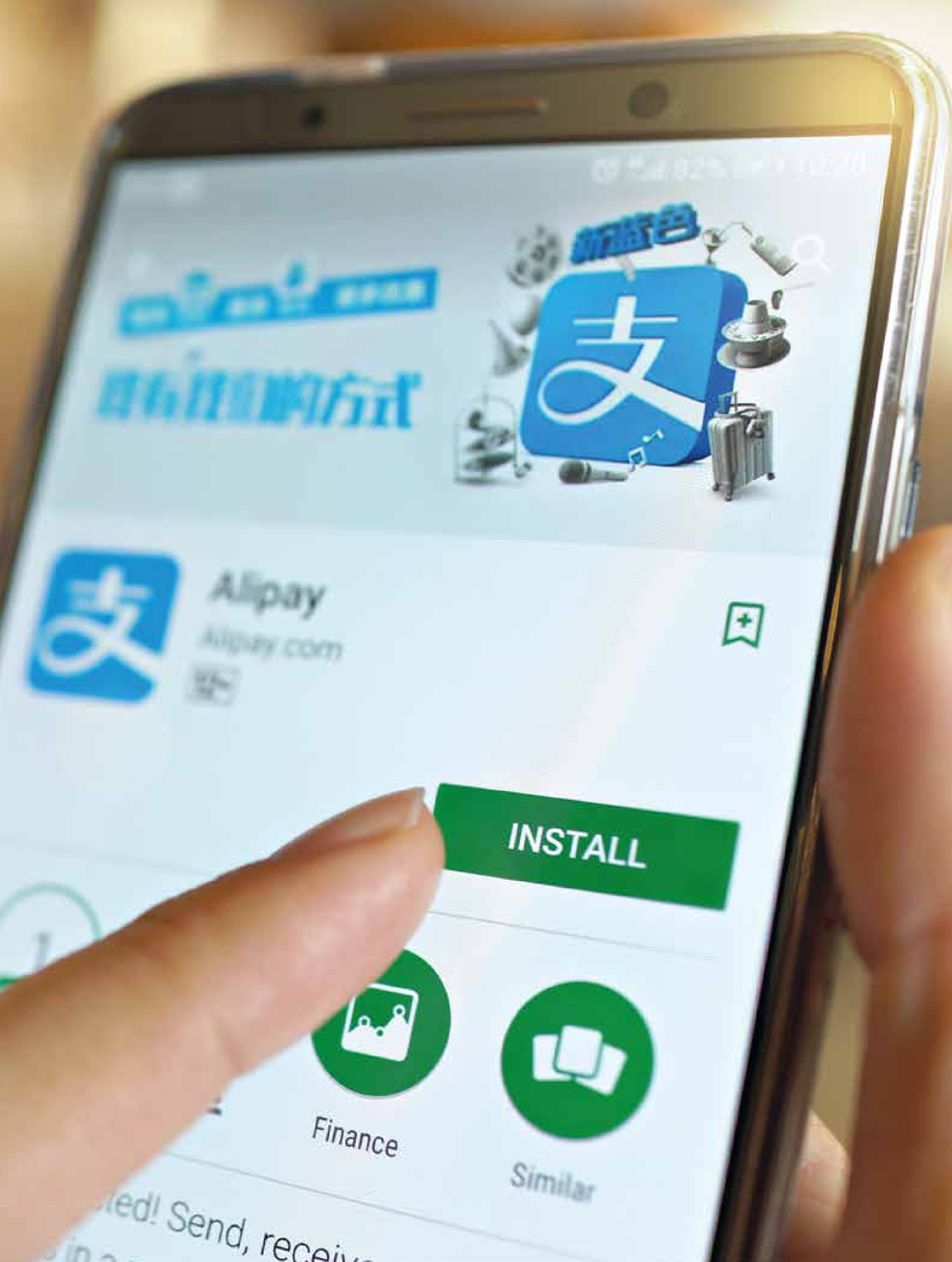
China and the Internet: a world wide web “with Chinese characteristics”

David Scott


Alipay
Alipay.com
INSTALL
Finance
Similar
ted! Send, receiv

Introduction

48 hours in Beijing. On December 25 (Christmas Day) 2017, the official Chinese state press agency Xinhua ran an article titled "China aims to become world-leading cyber power". The following day the Central Commission for Integrated Military and Civilian Development (CCIMCD) announced the setting up China's first Cybersecurity Innovation Center, the "security" involving domestic supervision and external military applications. This "strong cyber power strategy" (qiangda de wangluo zhanlue) is at the centre of China's drive for 'informatization' (xinxihua), which is seen as underpinning China's economic (and military) modernization, its push for an e-economy, and indeed its embrace of globalization.

Into this setting comes a ruling Chinese Communist Party (CCP) engaged in ongoing "regime survival". If China can control the Internet then it can establish "information dominance" (zhi xìnxi quan) in the battle for "discourse power" (huayu quan), and set much of the agenda for its international audience and domestic population.[i] The Internet has indeed become "the globalization of Chinese propaganda" outside China, in significant part through its widening online presence and activities.[ii] China's take on this global mechanism involves internal and external direction and control, an Internet "with Chinese characteristics" (juyou zhongguo tese). [iii]

The Internet has indeed become "the globalization of Chinese propaganda" outside China.

Inside China

Back in 2001, China joined the World Trade Organization (WTO) thereby signalling its embrace of globalization, and dare one say capitalism. Fifteen years later and China's internet restrictions were being raised in the 2016 Report to Congress on China's WTO Compliance submitted by the US Trade Representative, on the grounds that Western commercial operations in China were being hampered and that China was thereby failing to meet WTO rules on open and fair trade.

As with so many aspects of China's international rise, numbers are revealing. In 2001, Chinese internet users numbered around 34 million, a meagre 2.6% of the population. After sixteen years of globalization, China's internet users in 2017 numbered 772 million, some 55.8% of the population, with the rural areas posed to be the next growth area for China's e-economy. This leaves China not only as number one in the world, but also well ahead of the United States at around 287 million internet users.

In 2015, the total value of online sales was $581bn, making China the world's largest digital marketplace. Such a cyber-market space is an important side of China's two-fold economic positioning as it tries to (a) switch from an export-dominated economic model to one based on domestic consumption; and (b) move up the value chain to break free of a middle-income trap. A key enabler will be the "Internet Plus" (hulianwang+) strategy, introduced in 2015, that aims to integrate the real-world and digital economies of China. This was the focus of the Internet Plus and Digital Economy summit held in Hangzhou, on 20 April 2017. Hong Kong voices remain critical, arguing "we all know the key thing about the internet is freedom" and so "if Beijing misses the point and continues to censor access to information, Premier Li's new Internet Plus strategy will probably just get more Chinese to shop online rather than have any significant and long-term impact on the country's long-awaited economic transformation". iv

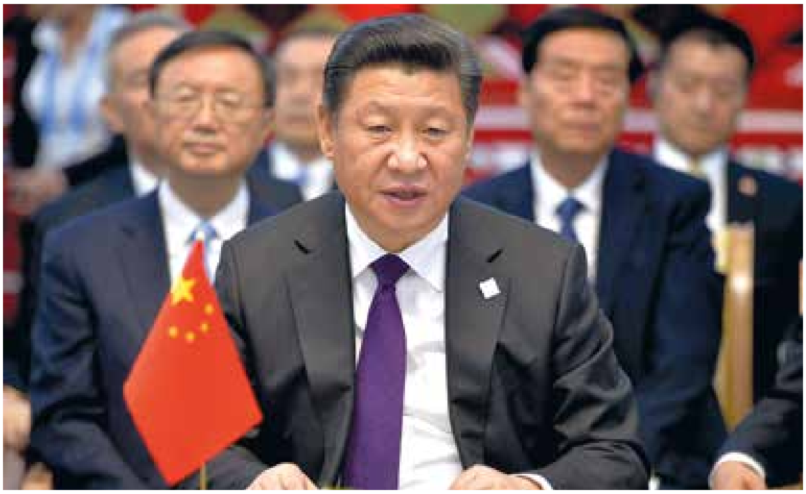
The actors

The internet actors in China involve a three-way relationship between the state, corporations and citizen (netizens).

The chief actors for the state include economic agencies like the Ministry of Industry and Information Technology (MIIT), and military departments like the People's Liberation Army (PLA). The state has sought to coordinate efforts through the propagandist State Internet Information Office (SIIO), which was set up in May 2011 within the State Council Information Office, which was then restructured into a ministry-level agency, the Cyberspace Administration of China (CAC) in April 2014, complete of course with its own online presence at www.cac.gov.cn. It has no English duplicate page for an international audience, but then its focus is the domestic Chinese population. CAC's fears were encapsulated in its Theoretical Studies Centre Group paper published in Qiushi on 15 September 2017, that "if our Party cannot traverse the hurdle represented by the Internet, it cannot traverse the hurdle of remaining in power for the long term". This was regime survival imperatives. Censorship guidelines are circulated weekly from the Communist Party's propaganda department and CAC to prominent editors and media providers throughout China.

If our Party cannot traverse the hurdle represented by the Internet, it cannot traverse the hurdle of remaining in power for the long term.

Political steerage of the Cyberspace Administration of China, and general internet strategy, is given by the Internet Security and Informatization Leading Small Group (ISILSG), set up in February 2014. ISILSG's key significance is that it is headed by Xi Jinping and brings together high-ranking officials from varying state units, including representatives from economic agencies, political and ideological units, and military departments. At its first meeting, Xi announced that "efforts should be made to build China into a 'cyberpower' (wangluo quanli)", and that "cyberpower" was part of the official "China Dream" goals. This came complete with Xi's assertion that "without cybersecurity (wangluo anquan) there is no national security (guojia anquan). The cyber security is security "with Chinese characteristics", protecting the security of the state rather than security of the citizen.



China’s Internet surge, against and by the state, has coincided with Xi Jinping’s own strengthening political position; dramatically demonstrated when the two-term Presidential clause was dropped from the constitution in February 2018, amid immediate heavy Internet censorship within China on the issue. Not surprisingly Xi has been heavily involved in steering China’s Internet policies. Xi Jinping’s speech to the Central Committee on Cyber Power Strategy, delivered on 9 October 2015 laid down various internal and external aims. Five areas pinpointed from his speech were:

- “Build a secure and controllable information technology system”
- “Deep integration of Internet and real economy, so as to promote digital economy and expand new space for economic development”
- “Enhance network management and cyber space security defense capability”
- “Use network information technology to promote social governance”
- “Stress internet governance, promote China’s views on cyber sovereignty and increase international discourse power”

As can be seen, these areas involved internal but also external control, internal and external discourse.

At the Work Conference for Cyber Security and Informatization, held on 19 April 2016, Xi “stressed the role of the Internet in directing and representing public opinion”. [vi] The key is of course not so much the Internet “representing” Chinese netizens but in terms of the state “directing” these netizens. He went on to argue that with regard to external matters, “internet core technology is the greatest ‘vital gate’, and the fact that core technology is controlled by others is our greatest hidden danger”. Great power rivalry was embedded in the Internet; “the cybersecurity game between large countries is not only a technological game, it is also a game of ideas and a game of discursive power” (huayu quan).

The relationship between state and corporate actors is further complicated by China’s increasing involvement in the globalization process.

Outside the state several different actors are prominent. These include Internet application and service providers such as Alibaba, telecommunications equipment manufacturers such as Huawei, search engine providers like Baidu, and network operators such as China Mobile. Moreover, the relationship between state and corporate actors is further complicated by China’s increasing involvement in the globalization process. Chinese capital is to some extent interacting with other corporate actors outside China, a transnational process that is a part of globalization. In 2014, four of the ten largest global Internet firms in market capitalization were based in China: Alibaba; Tencent; Baidu; and JD.com. Moreover, some of these Chinese capital giants are gaining positions in governing bodies regulating the World Wide Web. Huawei emerged as a significant player in Internet standardization while other companies, such as Alibaba and Baidu also quickly acquired international stature.

Outside the state and these domestic internet companies is the world of China's online public, its netizens. One of China's most prominent human rights activists Liu Xiaobo, dubbed "China's Nelson Mandela", saw the Internet as a crucial tool for his cyber-journalism. In a widely circulated online tract titled "Me and the Internet" (wo yu hulianwang) composed on 14 February 2006, he trumpeted the Internet as "the best tool for the Chinese people in their project to cast off slavery and strive for freedom":

> *In recent years, the Internet has vastly brought out the awakening of ideas about rights and the defence of civil rights among the Chinese people. The effect of the Internet in improving the state of free expression in China cannot be underestimated. Now through the Internet that connects the whole world, all I need is a computer and my personal information*

FOR MORE ARTICLES,
GO TO **HUAWEN.AC.UK**

> *space has expanded to previously unimaginable breadth. The Internet allows people to speak and communicate and it offers a platform for the spontaneous civilian organizations.*

Although awarded the Nobel Peace Prize in 2016, Liu died in July 2017 still serving an 11-year sentence imposed in December 2009 for "inciting subversion of state power". The same charges were levelled against another online activist Zhen Jianhua, when arrested in September 2017. Zhen was the executive director of the Human Rights Campaign in China (Quanli Yundong) at https://www.hrcchina.org; an online platform publishing information related to detentions of activists, police abuses, and other human rights violations. He was also the founder of ATGFW.org, a website at https://www.atgfw.org providing technical information and services to circumvent government controls, complete with the opening motto "Across the Great Firewall".

State policy

An ongoing struggle has ensued within China as the state constantly tries to shape and create what would in effect be a national-level Chinese intranet, filtered and controlled within China, rather than a international-level global internet of free access and circulation of ideas and information. The domestic rationale is explicit, promoting official regime values; "an ambitious agenda to place digital technologies at the heart of propaganda, public opinion and social control work". [vii] Reuters reported Xi Jinping on 21 April 2018 as warning that "we cannot let the Internet become a platform for disseminating harmful information and stirring up trouble with rumours".

China's first serious Internet legislation was in 1994, the Ordinance for Security Protection of Computer Information Systems, which gave the responsibility of Internet security protection to the Ministry of Public Security. In 1995 the first Internet service was set up in China. Very quickly the state stepped in, with "Temporary Measures for the Management of Computer Information Networks' International Connection" announced in February 1996. The irony is that such restrictive measures were not temporary. Instead they have been ever strengthened and made permanent. The Computer Information Network and Internet Security, Protection, and Management

Regulations approved by the State Council on 11 December 1997 included banning anyone "inciting to overthrow the government or the socialist system" or "injuring the reputation of state organizations". This has been no empty threat. The state systematically pursues leading cyber-critics as part of its deterrence policy of "killing the chicken to scare the monkeys", as already noted with regard to Liu Xiaobo and Zhen Jianhua.

China's 2010 White Paper, produced by the State Council Information Office (SCIO), entitled The Internet in China welcomed the Internet as "an engine promoting the economic development of China". It affirmed that "China takes Internet development as a significant opportunity to boost its reform and opening-up policies and modernization drive"; but "reform and opening up" (gaige kaifang) was economic reform and technology transfer within the "4 modernizations" programme. Its talk of "enhancing the capability of governance" and "building a 'harmonious society" (hexie shehui)" was another way of saying "regime survival". Its claim that "Chinese citizens fully enjoy freedom of speech on the Internet" was unconvincing, given that it went on to stress that the state Internet "regulations clearly prohibit the spread of information that contains contents subverting state power, undermining national unity, infringing upon national honour and interests". It also emphasized China's sovereignty; "within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected".

Xi's administration took big steps in reshaping China's internet control agencies by passing the Cybersecurity Law in November 2016, which came into force on June 2017. Domestic network operators in China provide network access, domain registration, fixed line and mobile services, and instant messaging. Under the Cybersecurity Law such network operators now have to require users to provide true identity information when signing service agreements with them. The fact that network operators are required to provide technical support and assistance to state security services, not only on matters of crime but also on matters of state security, makes this state tracking of individuals all the easier.

A particularly controversial aspect of the Cybersecurity Law is the requirement that data collected in China must be stored in China and should not generally be transferred and/or stored outside China. To transfer data out of China, a network operator is now obliged to seek the consent of the National Cyberspace Administration and State Council. This raises potentially difficult questions about trade secrets and intellectual property rights. Will a multinational company be comfortable disclosing details of its computer systems to the Chinese government? Multinationals were quick to argue that this would hamper their effective operations in China, increase their costs, and give Chinese companies an unfair advantage.

On the technical front, the PRC has become famous for setting up the notorious "Great Firewall"

Great Firewall

On the technical front, the PRC has become famous for setting up the notorious "Great Firewall" (fanghuo changcheng) of China.[viii] This has operated since 2003 within the Bureau of Public Information and Network Security Supervision, blocking access to foreign websites which the state deems harmful. Supervision is the key part of its remit. This is part of the wider monitoring of information carried out in the National Public Security Work Informational Project, better known as the "Golden Shield Project" (jindun gongcheng) operated by the Ministry of Public Security. The Golden Shield also involves over 30,000 human monitors of on-line social media sites. Local authorities employ further monitors; for example Beijing municipality has over 10,000 volunteers. Surveillance of social media goes hand in hand with its manipulation through the so called "five mao party" (wumaodang) operatives, on account of them supposedly being paid 5 mao, in effect 50 cents per posting.

Censorship is national, targeting particular groups, but is also regional. Xinjiang faced 10 months of external access blockage during 2009-2010, and later in 2015 the government shut down the mobile service of residents in Xinjiang who were using software that let them circumvent Internet filters. The Internet was also shut down in the Ganzi Tibetan Autonomous Province during March 2017.

Whereas the Golden Shield monitors domestic use of the internet within China, the Great Firewall blocks foreign websites from coming into China. As of September 2017 over 3000 websites were being blocked by China's Great Firewall system. Alongside a plethora of blocked pornography sites were a swathe of blocked technologies like Google, Youtube, Twitter, and Dropbox, and blocked information sites like Amnesty International, the New York Times, Reuters and the BBC. Websites that help users circumvent the firewall, like anonymizer.com and proxify.com are of course banned. Users who attempt to access blocked sites are met with two cartoon police mascots, called Jingjing and Chacha, who inform them they are being monitored.

Aside from blocking sites China also systematically restricts search engine providers. Human Rights, political democracy, Tibet, Xinjiang and Falun Gong are some of the particularly sensitive search terms that China has sought to shut down in China's cyberspace. Google felt impelled to pull out from China in 2010 due to increasing demands for self-censoring of its searches. Ironically on 14 December 2017 the Global Times ran an article headlined "Google's return indicates openness of Chinese market", which was true insofar as Google was returning to open up an artificial intelligence research centre, which was indicative of China's growing strength in science and technology. However, this did not mean that Google was returning as an independent search engine machine; it was not, on which the Global Times pointed in that above report on Google that "the country won't yield to pressure over how to best regulate cyberspace".

China's national companies have stepped into this vacuum, Robin Li's Baidu (with an 80% share of the Chinese market) in place of Google, and WeChat and Weibo in place of Twitter and Facebook. These of course comply with state regulations and ongoing surveillance. The state media may extol the "management inspiration" in these "regulations for WeChat and Weibo, which instills greater discipline"; but the underling logic is implicitly to do with political management; since "the development of Chinese social media is more stable, which has far less impact on China's politics than those in the US", meaning that "the Chinese government, in turn, can better build consensus" on the state terms.[ix]

Previously Chinese users have been able to use Virtual Private Network (VPN) technology to burrow through the Firewall, but in January 2015 the government successfully interfered with such gateways in China. The government subsequently ordered state-run telecommunications firms, which include China Mobile, China Unicom and China Telecom, to bar people from using VPN – with a deadline of February 2018.

A cat and mouse game operates in cyber-space between the Chinese state and its citizens.

A cat and mouse game operates in cyberspace between the Chinese state and its citizens. Chinese netizens continue to attempt to get around the Firewall, "scaling the wall" (fanqiang) amid a prevalent but porous censorship. The GreatFire.org at https://en.greatfire.org/ continues to run applications that circumvent the restrictions; namely FreeBrowser (free Android browser with built in circumvention that lets you access any blocked website), FreeWeibo for uncensored and anonymous Sina Weibo search, and FreeWechat for uncensored and anonymous WeChat search. As part of this ongoing online skirmishing, it is no surprise to find China's Great Cannon project redirecting Baidu browser traffic coming into the servers being used by GreatFire.Org so as to create significant Distributed Denial of Service (DDoS) attacks.

Cyber-nationalism

The state may of course be attempting to shape the internet within China, and of course human rights activists may continue to try and operate in this increasingly policed cyber space. However, in an era of globalization and glocalization, the two popular twists on

Online nationalism, i.e. cyber-nationalism, is a double edged weapon for Beijing.

the Internet in China are its role in increasing a “culture of consumerism” and “on-line nationalism”.

Globalization includes cross-cultural dissemination. Certainly Chinese broadband service providers provide Japanese hentai cartoons and the latest Hollywood blockbusters to feed Chinese consumer demand. Is Beijing worried? From a strict “regime survival” point of view, the answer is probably not since the state can thereby mollify and distract the population. Consumerism rather than religion can operate as the “opium of the masses”, and in post-Tiananmen Square times can avert the call for liberal democracy. Meanwhile, online mixing of traditional Chinese culture with propaganda state messages, ideology with entertainment (ideotainment as one analyst coined it), acts as a soft power cultural reinforcement in China for the state via the Internet.

Online nationalism, i.e. cyber-nationalism, is a double edged weapon for Beijing, riding the tiger as it were. [xi] This is exemplified with the online Qiangguo Luntan (“Strong Nation Forum”) run at the People’s Daily. To some extent online nationalism can be used to give a cover of legitimacy to Beijing’s control over Tibet, expansive policies in the Taiwan and the South China Sea, and foreign policy push backs against the US, India and most of all Japan. However, Chinese internet mobilization can slide into Han populist chauvinism, the online huanghan (“imperial Han”) netizens not only pushing Beijing further than it wishes internally and externally, but also ultimately undermining Beijing’s ability to meet patriotic expectations. So called “Red Hat hackers” (hongmaozi heike) populate the online hypernationalist patriotic group, ready to take down foreign websites through denial-of-service attack (DoS attack) on for example Taiwan, the Philippines, Vietnam, Japan and the US. The “Huaxia Hacker Alliance” headed by “Obedient Dog” at www.zhihu.com remains free to operate by the state, although fellow hackers at the 1937CN site www.1937cn.com were closed down by the state in February 2018, in the midst of its vehement attacks on South Korea.

Outside China

The White Paper International Strategy of Cooperation on Cyberspace released in 1 March

2017 forms a useful opening point for the PRC's view of the Internet outside China. It argued that in an "economically globalized and culturally diverse world and the profoundly changing global governance system, mankind has entered a new era of information revolution" and that "the rapid advancement of information and communication technologies (ICT) represented by the Internet has changed people's way of production and life and boosted market innovation, economic prosperity and social development". What of course the White Paper avoided was any talk of the Internet being a vehicle for democratization. Instead it stressed that cyberspace was "a new domain of state sovereignty" and that the West should respect China's "right to choose their own path of cyber development, model of cyber regulation and Internet public policies". As to cooperation, "the strategic goal of China's participation in international cyberspace cooperation is: resolutely safeguard the country's sovereignty, security and development interests in cyberspace; ensure secure and orderly flow of information on the Internet". The end sentence was crucial, the "strategic goal" in China's grappling with the Internet is ensuring the security of the ongoing political order in Beijing through control of information coming into China, circulating in China, and coming out from China.

The PRC's engagement with the internet outside China involves questions of techno-nationalism, cyber warfare, the country's weight in global internet governance, and its hosting of the World Internet Conference mechanism.

Techno-nationalism

An important undertone in China's Internet positioning is the techno-nationalism pinpointed by Jack Qui in 2003:

> *One thematic concern constantly accompanying the question of Internet, which underlies most discourse on technology and globalization in the PRC, is the memory of China being the most technologically advanced nation on the planet. As a result, restoring China's technical supremacy and thereby reviving the Middle Kingdom has been a constant goal for Chinese leaders.*[xii]

Super power computing has been a battleground between the superpowers. The US Titan mainframe with a speed of 18 quadrillion (petaFLOPS) floating point operations per second took the pole position in November 2012, only to be eclipsed in June 2013 by China's Tianhe-2 which ran at a speed of 34 petaFLOPS. China's leader position lengthened further in June 2016 with the arrival of the Sunway TaihuLight which runs at 93 petaflops. The accelerating nature of internet speed and superpower competition is indicated by the next US supercomputer, Summit, which is aimed at introduction in 2018, and will run at around 200 petaFLOPS. China though is aiming under its 2015 5-year Plan to introduce an exascale (1000 petaFLOPS) supercomputer by 2020. China's push for quantum computing technology has also been underpinned by the state, and has seen Alibaba take on Google. This development of indigenous "Chinese" technology is a source of pride to the state, techno-nationalism and glocalization, rather than techno-globalism and globalization.[xiii]

Suspicions remain that the Chinese government seeks to leverage its role as a major player in the global IT supply chain to propagate compromised hardware and software abroad. Amid rising distrust, US regulators have blocked Chinese takeovers of sensitive semiconductor chips companies like Aixtron (December 2016), Lattice Semiconductor (September 2017) and Xcerra (February 2018) – on national security grounds. Similarly, Huawei's dominance in emerging 5G Network technology was pinpointed in a US National Security Council draft in January 2018 as a direct threat to US security.

Cyber-warfare

"Cyber warfare" (wangluo zhanzheng) has become a recognised feature of Chinese military strategy. This was first announced in 1999 with the influential publication by two PLA colonels Liang Qiao and Xiangsui Wang titled Unrestricted Warfare. They argued that "computer virus infection can be included in the ranks of new-concept weapons" and concluded that "war is no longer war, but rather coming to grips on the Internet". [xiv]

Cyber applications were emphasized in May 2015, when the State Council Information Office released a White Paper entitled China's Military Strategy:

> *Cyberspace has become a new pillar of economic and social development, and a new domain of national security. As cyberspace weighs more in military security, China will expedite the development of a cyber force, and enhance its capabilities of cyberspace situation awareness, cyber defense, so as to maintain national security and social stability*

Like China's internal Internet practices and external military capabilities, China's moves towards cyber warfare capability remain extremely opaque.

The US, and also Japan, have their military communications and control systems underpinned by information technology; which makes them potentially vulnerable to the disruption posed by China's strategy of Network Electronic Warfare (wangdian yiti zhan). This is encapsulated in the Chinese military media:

> *The Internet has become the main battlefield. Having the power to control the network in the 21st century is just as decisive as grasping sea control in the 19th century and mastering the airpower in the 20th century. This is an online war, removing the real-world strategic opponents by overthrowing the network platform of the target countries.* [xv]

Further cyber-warfare positioning by China can be seen in disinformation, intelligence hacking, economic espionage and destabilising financial markets.

"Cyber warfare" ... has become a recognised feature of Chinese military strategy.

Just as the Chinese state has built up its army of internal cyber-monitors, so it is building up its external cyber-warriors. At a Symposium on Cyber Security and Informatization held in April 2016, Xi Jinping pledged greater state commitment, both financially and policy-wise, to developing "first class cyberspace security colleges" that could draw in the talented young "geeks and wizards" (guai cai qicai). The first batch of state-sponsored pilot programs was approved in mid-September 2017, including the Strategic Support Force Information Engineering University. Set up in 2015, the Strategic Support Force handles cyber, electronic and space warfare efforts by the state, and its deployment of these "cyber-warriors".

International governance

China's view on international governance of cyber space is part of its wider attempts to restructure the international system, with its call for a "new order in the cyber world":

> In essence, international relations in cyberspace are an extended version of that in the real world. The changing structure of world forces will have an obvious influence on cyberspace. The structure of the world is undergoing a transformation. Cyberspace should be conducted in a fair manner without any interference in the sovereignty of other countries. [xvi]

China's stance has been consistent on this sovereignty issue. The Position Paper at the World Summit on the Information Society (WSIS), released on 12 August 2015 set out China's position for "improving Internet governance":

> *We should establish a multilateral, democratic, and transparent international Internet governance system. The roles and responsibilities of national governments in regard to regulation and security of the network should be upheld. It is necessary to ensure that United Nations plays a facilitating role in setting up international public policies pertaining to the Internet. We should work on the internationalization of Internet Corporation for signed Names and Numbers (ICANN).*

The reference to the UN is precisely because of China's key veto rights in the Security Council, which is why China has been a supporter of the UN Internet Governance Forum. In the UN functional bodies, the election of Houlin Zhao as Secretary-general of the International Telecommunications Union in October 2014 represented a further avenue for Chinese influence in the international governance of the Internet.

ICANN's importance is that has previously overseen the world's DNS, IP address allocation and networking protocols – the glue that fits the Internet together. The problem for China is that ICANN had previously worked up until October 2016 under contract for US government departments, initially the US Defense Department and then the US Department of Commerce. Indeed, China boycotted ICANN meetings from 2001-2009 on account of this defence link up. This impending withdrawal of US government control became an issue in the US election, but by the time Trump was elected in November 2016 the privatization had already taken place.

World Internet Conference

The World Internet Conference (WIC) was set up by China in November 2014. The first WIC conference, entitled An Interconnected World Shared and Governed by All, was an explicit attempt by China to make its weight felt, and of course was addressed by Xi Jinping. In his Welcome Address Xi noted that "the development of the Internet has posed new challenges to national sovereignty". His calls for "an international Internet governance system of multilateralism, democracy and transparency" was highly ironic given the lack of democracy (its so called "democracy with Chinese characteristics", and "human rights with Chinese characteristics") within China and the lack of transparency in Internet use within China. The state media quoted Li Yuxiao, director of the Institute of Internet Governance and Law at Beijing University, as saying at the 2014 WIC that "China is transforming from a participant of the Internet into having a leading and dominant role in it". [xvii]

In early December 2017 China hosted the fourth World Internet Conference (WIC), titled Developing Digital Economy for Openness and Shared Benefits. Wang Huning, a member of the all-powerful Politburo standing committee announced that "China stands ready to develop new rules and systems of internet governance to serve all parties and counteract current imbalances" that he considered advantaged the West and disadvantaged China. Chinese commentary was glowing "during the conference, China contributed Chinese wisdom and plans for global Internet governance, laying a solid foundation for international cooperation in cyberspace". "Management" was a continuing Chinese theme at the 2017 WIC. Yang Shuzhen, president of the Chinese Academy of Cyberspace Studies (CACS) argued that "the Chinese government has been focusing on strengthening cyber space management while encouraging openness and innovation". [xix] However, "management" by the Chinese government is used in the sense of political control rather than technical management, and management in order to achieve required outcomes, which in the case of Beijing is regime survival.

A significant development in 2017 was that for the first time Western technology leaders — including Apple CEO Tim Cook, Google CEO Sundar Pichai, and Facebook executives, whose platforms have faced ongoing restrictions and sometimes outright banning in China — attended the WIC conference. Controversy was caused by Cook's keynote speech:

> *The theme of this conference — developing a digital economy for openness and shared benefits — is a vision we at Apple share. We are proud to have worked alongside many of our partners in China to help build a community that will join a common future in cyberspace.*

This was welcomed by the PRC state media as evidence of consensus, but this focus on an open digital economy totally ignored the increasing restrictions and curbs being placed on the Internet within China.

A further spin off in 2017 from the 4th WIC was China's announcement of a Digital Silk Road initiative, to serve as the digital counterpart of the overland and maritime Silk Road initiatives ('Belt and Road') across Eurasia and across the Indo-Pacific – aimed at encouraging e-commerce cooperation. Xi Jinping had already signalled this drive for Chinese-funded "cyberspace-connectivity" at his keynote Speech opening the Belt and Road Forum held in Beijing in May 2017, which highlighted China's expertise in the "digital economy, artificial intelligence, nanotechnology and quantum computing, and advance the development of big data, cloud computing".

If these restrictions are maintained, the economic success of China might slow down, which could in turn create pressure for political democratization and regime change.

Future trajectories

In December 2000, US President Clinton famously compared cracking down on the Internet in China with "trying to nail Jello to the wall"! However, these earlier expectations that the Internet would by itself be unstoppable in China and would provide an effective political counterbalance to the state, have not been realised. Nevertheless, while the state is managing in the immediate-term to pretty effectively throttle an open Internet, this very success may be creating longer-term economic problems. Globalization has brought economic success for China, but this complicates its Internet dynamics in two ways.

Firstly, Chinese internet companies are themselves becoming global actors. At the moment companies like Baidu have served as channels for state-run Great Cannon operations, which disrupted anti-censorship websites such as those operated by GreatFire.org.[xx] For the moment the domestic Chinese Internet giants have operated in line with government policy, but their increasingly international focus may lead to a divergence of interests between them and the Chinese state. Their interests may eventually lie in opening up the Internet inside China in line with globalization operations rather than acting as agents for Beijing. Secondly, restricting internet access is now starting to hamper external multinational operators in China. This was clear in the furore surrounding the impact of the new cyber laws in June 2017. If these restrictions are maintained, the economic success of China might slow down, which could in turn create pressure for political democratization and regime change. If these internet restrictions are eased, so as to allow globalization's economic advancement, then space for political democratization and regime change will open up. Either way, regime survival is threatened. ■

References

[i]China eyes cyber influence’, Global Times, 16 December 2015

[ii] Roger Creemers, ‘Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century’, Journal of Contemporary China, Vol. 26, No. 103 (2017), pp. 85–100; K. Edney, The Globalization of Chinese Propaganda: International Power and Domestic Political Cohesion (New York: Palgrave Macmillan, 2014).

[iii]Amy Chang, ‘How the “Internet with Chinese characteristics” is rupturing the Web’, Commentary (CNAS), 15 December 2014. Also Guobin Yang, ‘A Chinese Internet? History, practice, and globalization’, Chinese Journal of Communication, Vol. 5, No. 1 (2012), pp. 49–54.

[iv] George Chen, ‘Can Li Keqiang’s Internet Plus strategy really save China?’, South China Morning Post, 8 March 2015. Cf. Hu Yue, ‘Internet Plus sets the trend’, China Today, 11 May 2016.

[v]‘Xi vows to build China into a cyber power’, Xinhua, 27 February 2014. Also ‘Xi leads China in building cyberspace strength’, Xinhua, 18 April 2018.

[vi]‘China’s Xi calls for better development of Internet’, Xinhua, 19 April 2016. Also Rongbin Han, Contesting Cyberspace in China: Online Expression and Authoritarian Resilience (New York: Columbia University Press, 2018).

[vii]Guobin Yang, ‘The return of ideology and the future of Chinese internet policy’, Critical Studies in Media Communication, Vol. 31, No. 2 (2014), pp. 109–113. Also ‘China to promote core socialist values online’, Xinhua, 18 December 2017.

[viii]Margaret Roberts, Censored: Distraction and Diversion Inside China’s Great Firewall (Princeton: Princeton University Press, 2018); vs. ‘Why does the Western media hate the GFW so much?, Global Times, 11 April 2016.

[ix] Ai Jun, ‘Troubled by Internet trolling? China may offer management inspiration’, Global Times, 31 October 2017. Also Jason Ng, Blocked on Weibo: What Gets Suppressed on China’s Version of Twitter (and Why) (New York: The New Press, 2013).

[x]Johan Lagerkvist, ‘Internet ideotainment in the PRC: National responses to cultural globalization’, Journal of Contemporary China, Vol. 17, No. 54 (2008), pp. 121–140.

[xi]Christopher Hughes, ‘Nationalism in Chinese cyberspace’, Cambridge Review of Internaional Affairs, 13(2), 2000, pp. 195–209; Xu Wu, Chinese Cyber Nationalism: Evolution, Characteristics and Implications (Lanham: Lexington Books, 2007).

[xii]Jack Qiu, ‘The Internet in China: data and issues’, Working Paper (Annenberg Research Seminar on International Communication), 1 October 2003.

[xiii]Richard Suttmeier and Xiangkui Yao, China’s post-WTO technology policy: Standards, Software, and the Changing Nature of Techno-nationalism (Washington, DC: National Bureau of Asian Research, 2004); Jack Qiu, ‘Chinese techno-nationalism and global wi-fi policy’, in Michael Curtin and Hemant Shah (eds.), Reorienting Global Communication (Urbana: University of Illinois Press, 2010), pp. 289–303.

[xiv]Liang Qiao and Xiangsui Wang,

Unrestricted Warfare (Panama City: Pan Pamerican Publishing Company, 2002), pp. 16, 119. Also Jason Fritz, China's Cyber Warfare: The Evolution of Strategic Doctrine (Lanham: Lexington Books, 2017).

[xv] Sang Feng, 'Network sovereignty shows national sovereignty', PLA Daily, 20 May 2015.

[xvi] Ding Gang, 'Don't turn Internet into victim of hegemony', Global Times, 3 July 2013.

[xvii] Zhao Yinian and Cao Yin, 'China wants its voice heard in cyberspace', China Daily 21 November 2014; also Shannon Tiezzi, 'The Internet with Chinese Characteristics', The Diplomat, 20 November 2014.

[xviii] Zhang Shengli, 'China paves way for Internet governance', Global Times, 11 December 2017.

[xix] Chen Qingqing 'China's Internet remains open despite management', Global Times, 4 December, 2017. Cf. Xiao Qiang, 'The rise of China as a digital totalitarian state', Washington Post, 21 February 2018.

[xx] Harlan Whatley, 'Chinese Internet companies and their quest for globalization', SSRN Electronic Journal, March 2013; Adam Segal, 'The Great Cannon and the globalization of Chinese Internet companies', Council on Foreign Relations, 14 April 2015.