China Perspectives

2015/2 | 2015
Re-imagining the Chinese Worker

Becoming a Cyber Power

China's cybersecurity upgrade and its consequences

Samson Yuen

OpenEdition Journals

Electronic version
URL: http://journals.openedition.org/chinaperspectives/6731
DOI: 10.4000/chinaperspectives.6731
ISSN: 1996-4617

Publisher
Centre d'étude français sur la Chine contemporaine

Printed version
Date of publication: 1 June 2015
Number of pages: 53-58
ISSN: 2070-3449

Electronic reference
Samson Yuen, « Becoming a Cyber Power », *China Perspectives* [Online], 2015/2 | 2015, Online since 01 January 2017, connection on 15 September 2020. URL : http://journals.openedition.org/chinaperspectives/6731

cefc News Analysis

Becoming a Cyber Power

China's cybersecurity upgrade and its consequences

SAMSON YUEN

On 21 January 2015, Internet users in China who were trying to access blocked websites and smartphone apps encountered difficulties connecting to virtual private networks (VPNs), a popular circumvention tool for bypassing censorship in a country where government control of online space has been notorious. Astrill, StrongVPN and Golden Frog, three major providers of commercial VPN services that reported service disruptions, all blamed the interference on the Chinese cyberspace authorities. The attack, they claimed, was carried out with a level of sophistication unseen before. (1)

Having the world's largest online population with more than 600 million Internet users, China has also been known for its highly restrictive Internet control, which forms an integral part of the government's extensive oversight of information flow, ranging from media to culture. A recent Freedom House report detailed the government's sophisticated techniques to impose information control, including strategic control over key information nodes, censorship outsourcing, stronger Party leadership, ideological re-emphasis, and a crackdown on social media. (2) But so far, the Chinese authorities have kept their hands off the use of VPNs, which leaves a small window for China's Internet users – from ordinary surfers to privileged elites – to enjoy an unfettered Internet for entertainment and professional uses. The clampdown on VPNs hence suggests the government's new thinking with respect to circumvention around the censors, or what is known as the Great Firewall (*fanghuoqiang* 防火墙). What explains the change? And why such timing?

State media later said that the VPN block was due to an upgrade of the Great Firewall, (3) and senior state officials, for the first time, even acknowledged responsibility. According to Wen Ku, director of telecom development at the Ministry of Industry and Information Technology (MIIT), the VPN block was intended to ensure the healthy and lawful development of the Internet. (4) Although VPN providers managed to recover their services by reconfiguring their settings to outwit the Great Firewall, it appeared that Chinese cyberspace authorities are serious and open about clamping down on circumvention tools, and that they are refining their technology to shut off China's Internet and turn it into an Intranet if necessary. The block also appeared as the latest episode in a series of cyber-policing measures over the past few months, including the blocking of Google and Gmail and deliberate attacks on foreign sites such as Microsoft, Yahoo, and Apple. While these measures reflect the continuation of China's long-standing policy to increase oversight on the Internet, they further suggest that the authorities are taking steps to control segments in cyberspace that cannot be readily monitored – channels that were once allowed to leave an open door for Internet users to access information from foreign sources.

This article begins by discussing possible reasons behind the VPN block and linking it to the institutional expansion of the cyberspace authorities, which has resulted in a series of measures to tighten up cybersecurity. It argues that these measures reflect two main strategies: content control and technological self-sufficiency. These two strategies are key building blocks in China's conception of cybersecurity, a notion defined by Chinese officials as technologies and processes designed to protect against Internet-based threats to a wide range of domains, including political and ideological integrity, data, technology, applications, businesses, and communication channels. (5) These strategies are not only aimed at maintaining regime survival and protecting national security, but are also intended to nurture the domestic economy – particularly the technology industry. The increasingly restrictive Internet policies suggest that China is keen to pursue cybersecurity as a national priority, and is doing so regardless of the serious consequences it might entail.

The VPN block: Why now?

The timing of the VPN block was puzzling, given the fact that the Chinese authorities had long tolerated VPN use despite their onerous control over the Internet. In an online discussion initiated by *ChinaFile*, George Chen, a Hong Kong-based journalist, raised the question and considered the VPN ban as part of China's ongoing ideological crusade against Western values, directed by President Xi Jinping, from universities to cyberspace. (6) The ideology war began with the circulation of Document No. 9 around April 2013, which warned against seven perils including "Western constitutional democracy" and "universal values," (7) followed by a recent but unpublished direc-

1. "China blocks virtual private network use," *BBC*, 26 January 2015, available at www.bbc.com/news/technology-30982198 (accessed on 27 February 2015).
2. "The Politburo's Predicament: Confronting the Limitations of Chinese Communist Party Repression," *Freedom House*, January 2015.
3. Cao Siqi, "Foreign VPN service unavailable in China," *Global Times*, 23 January 2015, available at www.globaltimes.cn/content/903542.shtml (accessed on 27 February 2015).
4. Gao Yuan, "Blocking VPN is for Internet safety: Official," *China Daily*, 27 January 2015, available at http://usa.chinadaily.com.cn/business/2015-01/27/content_19420002.htm (accessed on 27 February 2015).
5. "Meiyou wangluo anquan jiu meiyou guojia anquan" (Without cybersecurity, there is no national security), *People's Daily*, 18 May 2014, available at http://politics.people.com.cn/n/2014/0518/c1001-25030371.html (accessed on 8 March 2015).
6. "Is China's Internet Becoming an Intranet? A ChinaFile Conversation," *ChinaFile*, 29 January 2015, available at www.chinafile.com/conversation/chinas-internet-becoming-intranet (accessed on 2 March 2015).
7. Chris Buckley, "China Takes Aim at Western Ideas," *The New York Times*, 19 August 2013, available at www.nytimes.com/2013/08/20/world/asia/chinas-new-leadership-takes-hard-line-in-secret-memo.html?_r=0 (accessed on 26 March 2015).

tive, Document No. 30, which allegedly "demands cleansing Western-inspired liberal ideas from universities and other cultural institutions." [8] The message of the latter text was echoed in a new directive published by the central government in January 2015, which called for the strengthening of propaganda and ideological work in higher education. [9] After its circulation, education minister Yuan Guiren urged universities to shun textbooks that promote Western values, a move widely seen as a step up to imposing stricter political discipline and control in China's education system.

In the same discussion, Charlie Smith, a co-founder of GreatFire.org and FreeWeibo.com, points to something more. He contended that the ban was not just a reflection of the Party's growing repugnance toward foreign values, but also a logical step in the recent ramp-up of cybersecurity and a further move to establish the concept of "cyber-sovereignty" (*wangluo zhuquan* 网络主权), a principle stipulating that national governments have the right to supervise, regulate, and censor online information within their own borders. [10] The concept has become China's foundational policy in promoting the need of national information borders on the diplomatic front, especially in the wake of Edward Snowden's revelations about U.S. cyber-espionage on foreign countries, including China. [11] According to government rhetoric, "cyber-sovereignty" and "cybersecurity" are closely-related concepts in China's Internet policy: while "cyber-sovereignty" serves as a diplomatic principle on the global arena, "cybersecurity" concerns the safety of domestic cyberspace. [12] Despite their different orientations, both concepts share the same goal: the need for a state-centric approach to monitoring cyberspace. This article will focus on "cybersecurity" and its domestic implications.

The rising power of cyberspace authorities

The increasingly restrictive cybersecurity measures ought to be first explained from an institutional perspective. Over the past few years, China's cyberspace authorities have undergone rapid expansion and have significantly increased their powers. In December 2013, the Politburo established the Central Leading Group for Cyberspace Affairs (*zhongyang wangluo anquan he xinxihua lingdao xiaozu* 中央网络安全和信息化领导小组), led directly by President Xi Jinping and tasked with the drafting of "national strategies, development plans, and major policies." The group established an office to implement its tasks, named as the Office of the Central Leading Group for Cyberspace Affairs, more commonly known as Cyberspace Administration of China (CAC) (*wangxinban* 网信办). The office became a new cyberspace authority replacing the State Internet Information Office (SIIO), an entity established by the State Council in May 2011 to operate under the State Council Information Office (SCIO) as an Internet regulatory body.

The replacement of the SIIO by the CAC resulted in an *independent* and *consolidated* cyberspace authority with significantly expanded powers, since it separated the Internet regulatory body from the State Council and led to the merging of entities with different organisational pedigrees. As a State Council agency, the SIIO was a government body mainly responsible for promulgating policies to lower-ranking ministries. [13] The newly established leading group, on the other hand, is a more powerful authority that reports directly to the Politburo, with an importance on par with other leading groups such as the one on deepening reform and national security, also led by President Xi himself. Given its ties to the central leadership, the CAC is able to involve itself in high-level policy-making and coordinate implementation across China's political bureaucracy, "[bringing] control over a broad policy area to a single conference table." [14] According to Wang Yukai, a member of the Advisory Committee for State Information, this organisational arrangement carries strategic importance. As cyberspace affairs involve matters that fall under the scope and interests of different government departments, the Internet regulatory body requires more power to strike down barriers between different power-holders in the Communist Party, government, and military to enable effective policy implementation. With the founding of the CAC, the previously fragmented Internet governance landscape can now be consolidated under one regulatory agency. Subsequently, the consolidation of power was followed by its institutional expansion at the local level. As of July 2014, ten provinces had established provincial leading groups on cyberspace affairs. Mega cities such as Beijing have also established their own cybersecurity committees. [15]

With their expansion both at the central and local level, the cyberspace authorities have become an increasingly influential stakeholder in China's political scene. Since the establishment of the CAC, Minister Lu Wei has gained wide exposure in the media. Dubbed "China's web doorkeeper," [16] Lu has met with numerous foreign diplomats, government ministers, and corporate leaders, [17] has toured around the continents, paid visits to foreign tech giants such as Facebook, Apple, and Amazon, [18] and has addressed audiences from decision-makers to university students, with a mission to promote the concept of "cyber-sovereignty" and China's involvement in global Internet governance. On the other hand, the CAC supported two locally-held Internet conferences in 2014: first was the China-ASEAN Cyberspace forum in Nanning, Guangxi, in September, and then came the World Internet Conference in Wuzhen, a town in Zhejiang, in November – both were the first of their kind. [19] The second World Internet Conference is scheduled to

8. Chris Buckley and Andrew Jacobs, "Maoists in China, Given New Life, Attack Dissent," *The New York Times*, 4 January 2015, available at www.nytimes.com/2015/01/05/world/chinas-maoists-are-revived-as-thought-police.html (accessed on 26 March 2015).
9. The full document, entitled "Opinions Concerning Further Strengthening and Improving Propaganda and Ideology Work in Higher Education under New Circumstances," was not published. The Xinhua summary, which is available at http://news.xinhuanet.com/2015-01/19/c_1114051345.htm, is translated by China Copyright and Media at https://chinacopyrightandmedia.wordpress.com/2015/01/19/opinions-concerning-further-strengthening-and-improving-propaganda-and-ideology-work-in-higher-education-under-new-circumstances/.
10. "Is China's Internet Becoming an Intranet? A ChinaFile Conversation," *ChinaFile*, *op. cit.*
11. Scott Livingston, "Beijing Touts 'Cyber-Sovereignty' in Internet Governance," *China Law Blog*, 19 February 2015, available at www.chinalawblog.com/2015/02/beijing-touts-cyber-sovereignty-in-internet-governance-global-technology-firms-could-mine-silver-lining.html (accessed on 8 March 2015).
12. "Xi Jinping: zunzhong wangluo zhuquan weihu wangluo anquan" (Xi Jinping: respect cyber-sovereignty, safeguard cybersecurity), *Wenweipo*, 19 November 2014, available at http://news.wenweipo.com/2014/11/19/IN1411190036.htm (accessed on 8 March 2015).
13. "China sets up office for Internet information management," *Xinhua*, 4 May 2011, available at http://news.xinhuanet.com/english2010/china/2011-05/04/c_13857911.htm (accessed on 8 March 2015).
14. Cary Huang, "How leading small groups help Xi Jinping and other party leaders exert power," *South China Morning Post*, 20 January 2014, available at www.scmp.com/news/china/article/1409118/how-leading-small-groups-help-xi-jinping-and-other-party-leaders-exert (accessed on 26 March 2015).
15. Li Jing, "Beijing sets up leading small group to guide internet policy," *South China Morning Post*, 9 May 2014, available at www.scmp.com/news/china/article/1507791/beijing-sets-leading-small-group-guide-internet-policy (accessed on 8 March 2015).
16. Paul Mozur and Jane Perlez, "Gregarious and Direct: China's Web Doorkeeper," *The New York Times*, 1 December 2014, available at www.nytimes.com/2014/12/02/world/asia/gregarious-and-direct-chinas-web-doorkeeper.html?_r=0 (accessed on 17 March 2015).
17. See list of ministerial activities on CAC's website: www.cac.gov.cn/ldhd.htm.
18. Edmond Lococo and Lulu Yilun Chen, "Zuckerberg, Cook Meet China's Internet Minister in U.S.," *Bloomberg Business*, 9 December 2014, available at www.bloomberg.com/news/articles/2014-12-08/china-s-internet-minister-visits-apple-facebook-offices (accessed on 2 March 2015).
19. "1st China-ASEAN Cyberspace forum opens," *Xinhua*, 18 September 2014, available at http://news.xinhuanet.com/english/china/2014-09/18/c_133653564.htm (accessed on 2 March 2015).

be held again in Wuzhen in October 2015. In December 2014, the CAC launched its official website to release news and regulations about cyberspace affairs, an apparent move to acquire its own voice. [20]

Tightening content control under the CAC

But more importantly, the Internet watchdog has significantly enlarged the scope of Internet oversight. It has initiated a number of "strike-hard campaigns" on China's cyberspace, including a crackdown on Big V microbloggers, or influential accounts in the Chinese social media, [21] and a nationwide campaign to clean up online porn and rumours. [22] Under the latter campaign, the watchdog has shut down 1.8 million accounts in social networking platforms and instant messaging services [23] as well as hundreds of websites for violations ranging from pornography to "publishing political news without a permit." [24] It has even threatened to close down Internet news service Sina Corp., the owner of China's biggest microblogging site, Sina Weibo, "if it fails to improve censorship of illegal content". [25] In February 2015, the watchdog announced new guidelines to enforce real-name registration (*shimingzhi* 实名制), which requires Internet users to register public accounts with their real names while banning accounts that impersonate people or organisations. [26] According to the CAC, the use of real online identities helps "ensure a safer online environment" and prevents "the spreading of rumours and information relating to terrorism, pornography and violence on the Internet," and will be extended from instant messaging tools (such as WeChat and QQ) to forums and micro-blogging platforms. [27]

Previously, China has made repeated attempts to enforce real-name registration, such as on the micro-blogging platform Weibo, which achieved some success by driving users away from the platform (while diverting them to instant messaging tools such as WeChat). While the latest regulation only applies to the public accounts on instant messaging tools, it appears to be a serious attempt to extend real-name registration more comprehensively across China's Internet outlets. Experts warned that this could discourage outspoken individuals from setting up public accounts, effectively eradicating space for critical, sarcastic, or literary online content. [28] As Bill Bishop, editor of the influential China newsletter *Sinocism*, remarked, "The real real-name registration [is] clearly coming." [29] Yet others have questioned the effectiveness of Internet real-name registration, pointing to the fact that China's social media market is too fragmented to enforce the restrictions and that netizens are mobile enough to migrate to alternative platforms. [30] However, if real-name registration is enforced systematically on all platforms, netizens might ultimately run out of alternates to migrate to. The cyberspace authorities saw this as a way to eradicate online rumours and critics that might pose threats to Party survival. But an airtight control on information might after all create a bigger market for unofficial opinions and rumours, which could well emerge in alternative forms.

While these Internet campaigns articulated China's intent to ramp up content control, Internet watchers suspected that the authorities launched numerous attacks on foreign websites for similar purposes. For example, *GreatFire.org*, a group that monitors online censorship in China, has accused the cyberspace authorities of staging man-in-the-middle (MITM) attacks on Google, Yahoo, Microsoft Outlook, Apple's iCloud, and even HSBC's corporate banking website. A man-in-the-middle (MITM) attack is a malicious Internet assault that "hijacks an online connection to monitor and sometimes control communications made through that channel." [31] In August 2014, Internet users in China trying to access Google via CERNET, China's education network, which still allowed access to the website after the authorities completely blocked it on commercial networks since 4 June 2014, were unable to do so anymore due to a suspected MITM attack. [32] A similar attack was launched in October on Apple's iCloud, coinciding with the launch of the new iPhone 6 in China, in which hackers attempted to gain access to usernames and passwords on the cloud service, where Apple users store their messages, contacts, and photos. [33] In November, Chinese Internet users reported problems connecting to HSBC's corporate banking portal, which appeared to have been blocked by the cyberspace authorities because it uses an Akamai domain that provides encrypted login for clients. *GreatFire.org* believed the authorities wanted to block access to mirror websites that the censorship watchdog hosts with Akamai. "The authorities have decided that they are better served by plugging a small leak than allowing commerce to thrive," *GreatFire.org* wrote in a post. In December, the cyberspace authorities appeared to have completely blocked Gmail, which users had previously still been able to access via third-party email services such as Apple Mail or Microsoft Outlook despite an earlier block on Gmail's website. This resulted in a dramatic plunge in Google traffic in China ever since. [34] After Google, the

20. "Cyberspace Administration of China launches official website," *Xinhua*, 31 December 2014, available at http://english.gov.cn/news/top_news/2014/12/31/content_281475032291728.htm (accessed on 2 March 2015).
21. Chris Buckley, "Crackdown on Bloggers Is Mounted by China," *The New York Times*, 10 September 2013, available at www.nytimes.com/2013/09/11/world/asia/china-cracks-down-on-online-opinion-makers.html?_r=0 (accessed on 2 March 2015).
22. "China inspects online videos in porn, rumor crackdown," *Xinhua*, 6 November 2014, available at http://news.xinhuanet.com/english/china/2014-11/06/c_133771062.htm (accessed on 2 March 2015).
23. "China shuts almost 1.8 mln accounts in pornography crackdown – Xinhua," *Reuters*, 20 September 2014, available at www.reuters.com/article/2014/09/20/china-internet-idUSL3N0RL02820140920 (accessed on 9 April 2015).
24. "Authorities cleaning up China's Internet," *Shanghai Daily*, 14 January 2015, available at www.china.org.cn/china/2015-01/14/content_34553452.htm (accessed on 2 March 2015); "China shuts dating websites over fraud, obscenity," *Xinhua*, 19 February 2015, available at www.chinadaily.com.cn/china/2015-02/19/content_19623280.htm (accessed on 2 March 2015).
25. "Sina faces suspension over lack of censorship," *Xinhua*, 11 April 2015, available at http://news.xinhuanet.com/english/2015-04/11/c_134142437.htm (accessed on 14 April 2015).
26. "China to ban online impersonation accounts, enforce real-name registration," *Reuters*, 4 February 2015, available at http://uk.reuters.com/article/2015/02/04/uk-china-internet-censorship-idUKKBN0L810020150204 (accessed on 2 March 2015); The regulations are translated in full by China Copyright and Media, https://chinacopyrightandmedia.wordpress.com/2014/08/07/provisional-regulations-for-the-development-and-management-of-instant-messaging-tools-and-public-information-services/.
27. Cao Yin, "Push for real IDs to expand," *China Daily*, 14 January 2015, available at http://usa.chinadaily.com.cn/china/2015-01/14/content_19312751.htm (accessed on 2 March 2015).
28. Paul Carsten, "China imposes new restrictions on instant messaging tools," *Reuters*, 7 August 2014, available at www.trust.org/item/20140807084511-rn98y/?source=fiTheWire (accessed on 2 March 2015); Amy Qin, "China to Force Authors to Provide Real Names When Publishing Online," *The New York Times Sinosphere Blog*, 26 January 2015, available at http://sinosphere.blogs.nytimes.com/2015/01/26/china-to-force-authors-to-provide-real-names-when-publishing-online/ (accessed on 2 March 2015).
29. Bill Bishop's Twitter account, https://twitter.com/niubi/status/559908681530101762.
30. David Caragliano, "Why China's 'Real Name' Internet Policy Doesn't Work," *The Atlantic*, 26 March 2013, available at www.theatlantic.com/china/archive/2013/03/why-chinas-real-name-internet-policy-doesnt-work/274373/ (accessed on 2 March 2015).
31. "After Gmail blocked in China, Microsoft's Outlook hacked, says GreatFire," *Reuters*, 19 January 2015, available at www.reuters.com/article/2015/01/19/us-microsoft-china-idUSKBN0KS12520150119 (accessed on 2 March 2015).
32. "Authorities launch man-in-the-middle attack on Google," *GreatFire.org*, 4 September 2014, available at https://en.greatfire.org/blog/2014/sep/authorities-launch-man-middle-attack-google (accessed on 2 Mach 2015).
33. "China collecting Apple iCloud data; attack coincides with launch of new iPhone," *GreatFire.org*, 20 October 2014, available at https://en.greatfire.org/blog/2014/oct/china-collecting-apple-icloud-data-attack-coincides-launch-new-iphone (accessed on 2 March 2015).
34. Paul Carsten, "Google's Gmail blocked in China," *Reuters*, 29 December 2015, available at www.reuters.com/article/2014/12/29/us-google-china-idUSKBN0K70BD20141229 (accessed on 2 March 2015).

latest victim was Microsoft's Outlook, whose users are now unable to send and receive messages using SMTP and IMAP email protocols. [35] All the attacks appeared to be connected to the CAC, *GreatFire.org* claimed, and they "[signal] that the Chinese authorities are intent on further cracking down on communication methods that they cannot readily monitor." [36]

In light of these intensifying efforts on content control, it is not surprising that cyberspace authorities have taken a further step to disrupt VPN services. The rising power and expanding reach of the cyberspace authorities appear to be the key reason accounting for the latest efforts to squeeze out the remaining freedom on the Chinese Internet. Meanwhile, Xiao Qiang, a U.S.-based China media observer, supplemented the view with a technological dimension, situating the issue against the long-standing competition between China's Great Firewall and the circumvention tools. Quoting a *Global Times* interview with Fang Binxing, who is widely regarded as the "father of the Great Firewall," Xiao described the competition between the GFW and VPNs as a "ceaseless war," with the GFW long lagging behind VPNs. He suggested that the VPN block means that the GFW is gaining the upper hand in this ceaseless war. [37] It must be noted, however, that not all VPNs were blocked – only the commercial ones were targeted. In fact, many institutional VPNs and the less popular ones are still working. [38] China's official policy is not to ban VPNs altogether, but to require domestic or foreign companies running a VPN business in China to register with the Ministry of Industry and Information Technology. [39] The firewall upgrade to block some of the VPNs was justified by state media as a move to enforce Chinese laws. [40] This means that China may still intend to maintain a window allowing circumvention around the censors, but that such a window must be monitored by the authorities. As Xiao pointed out, VPNs still play a crucial role in shaping the unofficial media environment inside China. They allow sensitive information leaked by "information brokers" to be brought back inside the Great Firewall, an instrument likely used by power-holders to spread rumours about their political enemies and to drive political bickering. In light of its potential value, it does not seem likely that China will completely ban the use of circumvention tools.

More recent reports suggested that the Great Firewall could further be turned into an offensive weapon by diverting Internet traffic that flows through it to overload targeted websites. In March 2015, Github, an American website that acts as a library of code for programmers and hosts pages that enable users to view sites blocked in China, suffered from a distributed denial of service (DDoS) attack by diverting traffic from China's own Internet giant Baidu, intending to remove two pages on Github, one with code from *GreatFire.org* and another that hosts links to mirror sites of the Chinese version of *The New York Times*, whose website was banned in China since 2012. [41] The attack followed a March 16 report on *The Wall Street Journal* that described the ways anti-censorship groups use cloud servers, run by companies such as Amazon.com, Microsoft Corp. and Akamai Technologies to get around China's Great Firewall. A report published by the University of Toronto's Citizen Lab called this "new weapon" the Great Cannon, which was not just an extension of the Great Firewall, but "a distinct attack tool that hijacks traffic to (or presumably from) individual IP addresses, and can arbitrarily replace unencrypted content as a man-in-the-middle". Accordingly, the Great Cannon possesses the ability to "exploit by IP address", which allows it to launch cyberattacks on "targeted individuals who communicates with any Chinese server not employing cryptographic protections". [42] The latest attack suggests that China's Internet authorities not only have the ability to block content from outside, but also the capability to take the offensive on both websites and individuals. In addition, the involvement of Baidu in the attack further suggests that Chinese authorities are willing to pursue cybersecurity at the expense of fostering development of the tech and business sector.

Technological self-sufficiency

China's cybersecurity concerns are not limited to just the flow of information, but further extend to the technological landscape, where the government has become increasingly cautious against foreign technology, ranging from software to computer chips. The concern became particularly heightened in light of the Snowden revelations. A recent report published by Kaspersky Lab, a Russian cybersecurity firm, served as a fresh reminder of the importance of technological safety in cyberspace. It said that the United States has found a way to permanently embed surveillance and sabotage tools in computers and networks located in countries such as Iran, Russia, Pakistan, Afghanistan, and China. According to the report, the spyware is linked to *Stuxnet*, a computer worm that disabled about 1,000 centrifuges in Iran's nuclear enrichment program, under a project run jointly by Israel and the United States. [43]

In light of the cybersecurity concerns in the technological realm, the Chinese government is rushing to introduce security requirements in the commercial sector. One example was a new restriction for technology vendors of China's banking sector. The restriction, set out in a 22-page document approved in December 2014, requires companies that sell computer equipment to Chinese banks to "turn over secret source code, submit to invasive audits and build so-called back doors into hardware and software." [44] The use of backdoors has been identified by China as one of the key sources of cyber-attacks by the United States. According to the SIIO, a Chinese security team found that 2,016 IP addresses in the U.S. had implanted backdoors in 1,754 Chinese websites, involving 57,000 backdoor attacks. [45] Hence, protection against backdoors is deemed sorely necessary in strategic sectors such as banking, which holds sensitive financial information of the state. The same reason had been used by the United States to prevent Huawei, a major Chinese maker of computer servers and cell phones, from entering the U.S. market.

35. "After Gmail blocked in China, Microsoft's Outlook hacked, says GreatFire," *Reuters*, *op. cit.*
36. "After Gmail blocked in China, Microsoft's Outlook hacked, says GreatFire," *Reuters*, *op. cit.*
37. "Is China's Internet Becoming an Intranet? A ChinaFile Conversation," *ChinaFile*, *op. cit.*
38. Wei Sisi, "What's Really Happening with China's Great Firewall," *ProPublica*, 2 February 2015, available at www.propublica.org/article/whats-really-happening-with-chinas-great-firewall (accessed on 2 March 2015).
39. Zhang Zihan, "Foreign-run VPNs illegal in China: govt," *Global Times*, 14 December 2012, available at www.globaltimes.cn/content/750158.shtml (accessed on 2 March 2015).
40. Cao Siqi, "Foreign VPN service unavailable in China," *Global Times*, 23 January 2015, available at www.globaltimes.cn/content/903542.shtml (accessed on 27 February 2015).
41. Paul Mozur, "China Appears to Attack GitHub by Diverting Web Traffic", *The New York Times*, 30 March 2015, available at www.nytimes.com/2015/03/31/technology/china-appears-to-attack-github-by-diverting-web-traffic.html (accessed on 14 April 2015).
42. Bill Marczak et al., "China's Great Cannon", *CitizenLab*, 10 April 2015, available at https://citizenlab.org/2015/04/chinas-great-cannon/ (accessed on 14 April 2015).
43. Nicole Perlroth and David E. Sanger, "U.S. Embedded Spyware Overseas, Report Claims," *The New York Times*, 16 February 2015, available at www.nytimes.com/2015/02/17/technology/spyware-embedded-by-us-in-foreign-networks-security-firm-says.html (accessed on 2 March 2015).
44. Paul Mozur, "New Rules in China Upset Western Tech Companies," *The New York Times*, 28 January 2015, available at www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html?_r=0 (accessed on 2 March 2015).
45. "China publishes latest data of U.S. cyber attack," *Xinhua*, 20 May 2014, available at http://news.xinhuanet.com/english/china/2014-05/20/c_126520552.htm (accessed on 2 March 2015).

A draft counterterrorism law, which is expected to be approved within months, goes a step further by extending the requirement to more firms. It requires all technology companies to hand over encryption keys and source codes and also to install security "backdoors," which would mean that the Chinese government will know how their products work, making them vulnerable to hacking. (46) While some foreign tech companies, such as Apple Inc., have reportedly agreed to the requirement of security inspections, (47) others have objected to the new policies and complained that they amounted to protectionism in a letter sent to the cybersecurity leading group led by President Xi. (48) The rules were further criticised by Human Rights Watch as "enforcing a system of complete, permanent digital surveillance." (49) So far, China has showed no intention of watering down the rules. If they are eventually passed by the legislature without significant revision, it will be a stark indication that Beijing will not compromise cybersecurity for foreign technology.

Meanwhile, the growing caution against foreign technology is shaping a new wave of technological development in China. In the component industry, for example, cybersecurity concerns have become an impetus for the Chinese government to reduce reliance on foreign chips and encourage the development of domestic chips, owing to their importance in controlling key functions of smartphones, televisions, computers, and networking equipment, and their perceived vulnerabilities to eavesdropping if they are manufactured by foreign firms. (50) As Wu Hequan, an expert at the Chinese Academy of Engineering, argued in his research report posted on *People's Daily*, cybersecurity must be safeguarded through developing solid home-grown technology, primarily computer chips. (51) State Council expert Wang Yukai put it in similar perspective: "[s]ecurity is actually a technological competition in which China, lacking core technology, has lagged behind due to excessive dependence on overseas equipment and information systems." (52) In light of the increasing strategic importance given to electronic components, semiconductors, for example, have been named as a key strategic sector for China since September 2013. (53)

The tendency to promote domestic tech players is further demonstrated by a recently approved state procurement list, which has dropped a number of leading foreign technology brands such as Apple Inc., along with U.S. network equipment maker Cisco Systems Inc., security software firm McAfee, and network and server software firm Citrix Systems. The number of foreign tech brands fell by a third on the list, and less than half of those with security-related products remained. Meanwhile, the almost two-fold increase in procurement products came mostly from local makers. (54) The procurement list followed the exclusion of Apple products, Microsoft's Windows 8 operating system, and Symantec and Kaspersky antivirus products last year from the state purchase directory. (55) The implications are consistent and clear: local products offer more security guarantees; and by awarding contracts to local makers, China in effect subsidises the domestic tech industry and nurtures home-grown giants to become as competitive as their overseas rivals. Although this raised suspicion of protectionism that might violate World Trade Organisation (WTO) rules, Bien Perez, an *SCMP* technology reporter, said that the complex regulations will make it difficult for the U.S. government and technology firms to take legal action against Beijing, as it did not sign a plurilateral treaty on government procurements, despite a commitment to do so. "As a result, China is able to remove any foreign brands that the government doesn't like from its state procurement lists with little potential WTO blowback," Perez argued. (56)

The dovetailing of security concerns with commercial interests has formed a strong justification for censorship and cyber-protectionism. Most notably, a *Global Times* op-ed attempted to praise Internet censorship by arguing that China's Great Firewall has given rise to the three domestic tech giants: Baidu, Alibaba, and Tencent (known as the BAT), and that it has not affected its opening-up policy. The firewall only blocks certain overseas websites in a targeted fashion, rather than isolating China's Internet from the overseas one, the column argued. (57) Without the Great Firewall, "China would become the realm of Google China, Yahoo China, and Facebook China." (58) In a similar but less triumphant tone, MIIT official Wen Ku said that China's Internet companies should owe their successes to the "good policy environment" created by the Chinese government, (59) or the top-down policy support often regarded by Chinese businessmen and entrepreneurs as the prerequisite for doing business in China. Both *Global Times* and Mr. Wen's words revealed that China's Internet censorship is not a pure political or national security concern; it has an equally significant economic dimension. In addition, these two dimensions, political and economic, will become mutually reinforcing. As these domestic giants rise up, they will develop their own set of interests and become key stakeholders in China's political process. This has been demonstrated, for example, by Alibaba's recent slam on a Chinese state regulator against its criticism of the excess of counterfeit goods on its e-commerce platform. (60) Although their ascent might help

46. Heather Timmons, "Apple is reportedly giving the Chinese government access to its devices for 'security checks'," *Quartz*, 23 January 2015, available at http://qz.com/332059/apple-is-reportedly-giving-the-chinese-government-access-to-its-devices-for-a-security-assessment/ (accessed on 2 March 2015).
47. Rob Price, "Apple Agrees to Let the Chinese Government Inspect iPhones Over Security Fears," *Business Insider*, available at www.businessinsider.com/apple-china-security-audits-nsa-2015-1#ixzz3TEyaotwC (accessed on 2 March 2015).
48. Paul Mozur, "New Rules in China Upset Western Tech Companies," *The New York Times*, 28 January 2015, available at www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html?_r=0 (accessed on 2 March 2015).
49. "China: Draft Counterterrorism Law a Recipe for Abuses," *Human Rights Watch*, 20 January 2015, available at www.hrw.org/news/2015/01/20/china-draft-counterterrorism-law-recipe-abuses (accessed on 2 March 2015).
50. Eva Dou and Don Clark, "China Looks to Prop Up Domestic Chip Makers," *The Wall Street Journal*, 27 January 2015, available at www.wsj.com/articles/china-looks-to-prop-up-domestic-chip-makers-1422387551 (accessed on 2 March 2015).
51. "Weihu wangluo anquan bixu you guoying jishu" (Safeguarding cybersecurity requires excessively hard technology), *People's Daily*, 18 May 2014, available at http://paper.people.com.cn/rmrb//html/2014-05/18/nw.D110000renmrb_20140518_3-05.htm (accessed on 2 March 2015).
52. "China eyes Internet power," *Xinhua*, 8 March 2014, available at http://news.xinhuanet.com/english/special/2014-03/08/c_133171308.htm (accessed on 1 March 2015).
53. Eva Dou and Don Clark, "China Looks to Prop Up Domestic Chip Makers," *op. cit.*
54. "China drops Apple, Cisco & Intel for state purchases," *Fortune*, 25 February 2015, available at http://fortune.com/2015/02/25/china-drops-apple-cisco-intel-for-state-purchases/ (accessed on 2 March 2015).
55. "China Said to Exclude Apple from Procurement List," *Bloomberg*, 9 August 2014, available at www.bloomberg.com/news/articles/2014-08-06/china-said-to-exclude-apple-from-procurement-list (accessed on 2 March 2015).
56. Bien Perez, "WTO rules make it difficult for Cisco and Apple to challenge Chinese government 'black list'," *South China Morning Post*, 27 February 2015, available at www.scmp.com/business/companies/article/1724817/difficult-cisco-and-apple-challenge-chinas-government-procurement (accessed on 17 March 2015).
57. "China Owns 'Great Firewall,' Credits Censorship With Tech Success," *The Wall Street Journal*, 28 January 2015, available at http://blogs.wsj.com/chinarealtime/2015/01/28/china-owns-great-firewall-credits-censorship-with-tech-success/ (accessed on 2 March 2015).
58. "Fanghuoqiang daigei Zhongguo hulianwang shenme yingxiang?" (What impact does the Great Firewall bring to China's Internet?), *Global Times*, 28 January 2015, available at http://opinion.huanqiu.com/editorial/2015-01/5526579.html (accessed on 2 March 2015).
59. "China Owns 'Great Firewall,' Credits Censorship With Tech Success," *The Wall Street Journal*, *op. cit.*; Emily Parker, "The Chinese Government Is Investing Heavily in the Maker Movement," *Slate*, 14 May 2014, available at www.slate.com/blogs/future_tense/2014/05/14/the_chinese_government_is_investing_heavily_in_the_maker_movement.html (accessed on 8 April 2015).
60. Charles Clover, "Alibaba slams regulator over critical report," *Financial Times*, 29 January 2015, available at www.ft.com/intl/cms/s/0/f04493b0-a7b2-11e4-be63-00144feab7de.html#axzz3TFdji5D0 (accessed on 3 March 2015).

build up China's domestic technology industry and its technological capability, it could create perverse incentives for increasing Internet censorship. As beneficiaries of the Great Firewall, domestic giants will have the interest to build up, rather than lower, the Great Firewall in order to fend off competition. It creates the economic foundation that turns the Firewall into a permanent structure, as opposed to a makeshift one that the *Global Times* op-ed so anticipated.

Conclusion

While it is typical (although not necessarily justifiable) for governments to impose some form of censorships to safeguard national security and also to impose some form of protectionist measures to nurture domestic industries, China, as its recent policies have suggested, appears to be taking a militant approach on both aspects, emphasising a state-centric and comprehensive control on online information on the one hand, and a nationalist industrial policy on the technology sector on the other. Although relatively successful, both approaches are not without substantial costs. An increasingly sophisticated system of information control not only further tramples upon the human rights enshrined in China's own Constitution, but also drains the Party's public support and dampens the country's creativity and innovation, the necessary ingredients for a more advanced economic development. A *New York Times* report, for example, warned that the VPN ban had "provoked a torrent of outrage among video artists, entrepreneurs and professors." [61] According to the report, these elites might not have the slightest intention of overthrowing the Communist Party, but barring them from connecting to banned foreign websites and apps such as Facebook, Twitter, Instagram, Flickr, Google, or Gmail might irritate them, in turn eroding popular support for the Party. In addition, the newspaper argued that the block on VPNs might carry a huge economic cost as it might stifle "the innovation and productivity needed to revive the Chinese economy at a time of slowing growth." [62]

In his *SCMP* column, George Chen compared China's "closed-Internet" policy to the "closed-door" policy of the Qing Dynasty, suggesting that the impact could be extensive. "Many mainland scholars are now limited to do their research as they can rely mostly on domestic search engines and online research tools where English-language information is limited. Students also find it difficult to stay in touch with foreign universities or employers after the blocking of Google's email service," Chen wrote. [63] A China news portal reported that the disruption (and later, the complete ban) of Gmail is now affecting tens of thousands of Chinese students who rely on the email provider to stay connected to their U.S. universities or apply to them. [64] Another *SCMP* report suggested that the VPN block is preventing foreigners and millions of Chinese from using Google-based business tools while hurting small-and-medium-sized foreign companies that depended on VPNs, as larger companies could afford direct links to overseas servers. [65]

On the other hand, cyber-protectionism in the tech landscape not only drives out foreign tech enterprises, but also their technology, experience, and know-how, which Chinese firms could learn from under collaboration. Without competitive pressure from foreign technology, the extent of success in building up its home-grown technological capabilities will now be questionable. Worse still, the policy promotes a chauvinistic culture that anything foreign would be harmful for China's national security, which will further erode the spirit of learning, innovation, and creativity. For now, the golden days of reform and opening might be over. A closed-door policy with an increasingly restrictive Internet now moves to the centre stage to become part of the popular political catchword – the "new normal" (*xinchangtai* 新常态).

Samson Yuen is a PhD candidate in politics at the University of Oxford and is a research assistant at the CEFC (samson.yuen@sant.ox.ac.uk).

CEFC News Analysis is compiled from the CEFC's fortnightly selection of Press Highlights, available at www.cefc.com.hk.

61. Andrew Jacobs, "China Further Tightens Grip on the Internet," *The New York Times*, 29 January 2015, available at www.nytimes.com/2015/01/30/world/asia/china-clamps-down-still-harder-on-internet-access.html?_r=0 (accessed on 2 March 2015).
62. *Ibid.*
63. George Chen, "China to pay price for 'closed-internet' policy," *South China Morning Post*, 26 January 2015.
64. "Gmail youxiang zhongduan huo yanzhong yingxiang shuwan Zhongguo xuesheng shenqing Meiguo daxue" (Stoppage of Gmail might seriously affect tens of thousands of students applying to U.S. universities), *China Daily*, 30 December 2014, available at http://news.china.com/domestic/945/20141230/19160346.html (accessed on 26 March 2015).
65. "China blocks VPN services that let internet users get around censorship," *South China Morning Post*, 23 January 2015.