Behind the Great Firewall: How China's Government, Businesses, and Populace Compete to Shape the Chinese Internet

An STS Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

James Houghton

May 5, 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Signed: _____

Approved: _____ Date _____

Peter Norton, Department of Engineering and Society

Behind the Great Firewall: How China's Government, Businesses, and Populace Compete to Shape the Chinese Internet

Introduction

Chinese citizens are subject to some of the strictest censorship in the world. The Chinese government blocks nearly all of Google's services, Facebook, Twitter, and even some academic journals. Even today, political expression is limited, and whistleblowers are silenced (Griffiths, 2020). Although many in China remain complacent due to highly integrated applications like WeChat, a small minority is vocal about combating censorship. The relationship between Chinese authorities and web users is complex and requires investigation.

The Communist Party of China (CPC) has built what is now called the Great Firewall of China (GFW), a web traffic monitoring and censorship system. The CPC routinely uses it to scan for and block content it deems sensitive or inappropriate (Zheng, 2017). Although some people working in academia and business may have methods, by exemption or otherwise, of bypassing some of the GFW restrictions, the CPC has plugged many of its holes in recent years, impeding research and business opportunities. However, nearly all Chinese web users including students do not seek to access the uncensored web, and many businesses thrive with the lack of much foreign intervention. With over 800 million Internet users in China (McCarthy, 2018), any censorship decision by the CPC may have global effects. For an example, one need look no further than the recent coronavirus outbreak (Griffiths, 2020).

Review of Research

The CPC's censorship techniques are the most advanced in the world (Yuan, 2019), and their success has sparked research interest. Researchers have measured Chinese online political engagement despite the CPC's efforts (Chen, 2016; Lu and Zhao, 2018), finding that even perception of censorship can inhibit political expression and protest. Guo and Feng (2012) have applied the Theory of Reasoned Action to explain the Chinese government's success in building public support for censorship. Adding to this, Chen and Yang (2019) found that, even when given free access to foreign information, very few Chinese university students took advantage of it. Brehm's theory of reactance, introduced in 1966, is highly relevant in this case, as Chinese web users face more web usage restrictions.

Chin (2018) studied the origins and development of media censorship in China since the 1950s. Wong and Kwong (2019) analyzed differences between censored and uncensored academic works, finding that censorship of this variety is usually based on keywords, but sometimes a blacklist is used. They also found that these censorship requests in China sometimes affect researchers globally. Similar techniques are applied to internet censorship, notably in censoring Wikipedia articles and foreign publications. Yang (2017) argues that the CPC has a clear motive: to control information to prevent challenges to official narratives and eliminate "unauthorized collective actions". That assessment is not challenged here.

This work gives an overview of the techniques the CPC uses to control the internet in China, how web users react, and some of the key results of the competition between them. Web users discussed here include: foreign and domestic web users, university students, researchers, and technology business employees.

With Private Help, the CPC Maintains Control of New Media

The CPC launched the Cyberspace Administration of China (CAC) in 2014 to implement new censorship policies (Creemers, 2015). It had previously been quiet about its censorship activities, often denying censorship allegations, but with the creation of the CAC it accepted its status as the world's most powerful internet censor (Chin, 2015). CAC declares as its sole purpose to "protect the lawful rights and interests of citizens, legal persons, and other organizations" and to "preserve national security and public well-being" (CAC, 2017). President Xi Jinping himself asserts that China's heavily censored internet model protects its citizens and should serve as a global standard (Mai, 2017).

Under this heavily censored internet model, many Western news and information organizations have either been censored or have ceased operation in China. As a part of the CPC's first censorship wave in 2001, *Voice of America* and *The New York Times* were both blocked in China, though *The New York Times* was promptly unblocked. In 2008, YouTube, a Google product, was blocked. In 2010 following many hacking attempts, Google ceased all operations in mainland China after revealing that it believed that the Chinese government was attempting to "limit the freedom of speech on the web". In 2012, *Bloomberg* and *The New York Times* were both blocked after reporting on various Chinese officials' family assets. *The Economist* and *Times Magazine* were both blocked in 2016 for criticizing Xi Jinping (Yang, 2017). These news organizations, as well as the BBC, *The Guardian, Business Insider, NBC, Reuters, The Wall Street Journal, The Washington Post,* and others, remain blocked as of March 2020 (GreatFire, 2020). Although keyword blocking for webpages has been a common tactic, the uptake of secure HTTPS transmission for webpages makes this kind of blocking impossible, leaving countries a choice to either fully block or allow those webpages. Wikipedia, once only

partially censored in China via keyword blocking, has now been fully blocked since migrating to HTTPS in 2015 (Clark et al., 2017).

The CPC also maintains control of domestic online news sources. In June 2017, a new cybersecurity law came into effect that required all online news services to be managed by party-sanctioned editorial staff (Shepherd, 2017). The CAC claimed that these regulations would "strengthen management of information" and "promote the healthy and orderly development of internet news, in accordance to law" (BBC, 2017).

Although the CPC claims to promote public safety, dissidents have been threatened or detained for acts like posting to Twitter (Shih, 2019). To comply with Chinese law, tech companies delete politically charged posts en masse (Bamman et al., 2012). Large Chinese technology companies have had to tread a fine line between censorship and user engagement. In 2017, following the introduction of a new cybersecurity law, Tencent, Weibo, and WeChat were all fined the maximum legal amount for allowing certain kinds of information on their platforms that the CPC deemed damaging (Cadell & Li, 2017). In response, the business of internet censorship among private companies has been growing quickly.

Many censors believe they are doing a public service by hiding the vast amounts of "evil and pollution" that can be spread on the Internet. Inke is a publicly traded livestreaming service based in Hong Kong that has over 25 million active users, the most popular of its kind in China. In order to operate in mainland China, Inke must comply with censorship regulations set by the CAC. Zhi Heng, the head of the Content Security Department of Hunan Inke, had an interview with the *South China Morning Post* in which he disclosed several kinds of "irregular behaviors," acts that are disallowed by the government, including depicting smoking and showing tattoos

(Li, 2019). Inke censorship workers also assist the government in quelling protest, as Heng recalls:

> The most memorable incident so far was a case involving local government plans to build a refuse incineration plant near a city in China. [The local citizens] gathered to protest. We located the scene and used it as a center point to draw a circle with a radius ten kilometers on a GPS map. All users in that circle were not allowed to live stream. In the end, we prevented the incident from getting worse. (Li, 2019)

Heng and his approximately 1,200 coworkers are not government employees. Although Inke has its own policies on allowable content, most of the Content Security Department's work is in compliance with the CPC's censorship requirements.

Most Chinese Web Users Remain Complacent

Chinese web users have relied on unlicensed VPNs[1] and internet anonymity systems like Tor to side-step censorship. Despite China's efforts, Tor and several VPN services remain fully operational in China; however, only an estimated 1% of Chinese citizens use them. Most of the approximately 800 million Chinese Internet users are apparently content with convenient, highly integrated online services such as WeChat that the government can easily monitor and control (MacKinnon, 2012; McCarthy, 2018). The few who strive to access the uncensored Internet must cope with the performance penalties that come with circumvention services and the language barriers of non-Chinese websites. The performance penalties can impair productivity for some Chinese technology companies, increase costs, and stifle innovation (Bao, 2013). More importantly, such disadvantages can deter efforts to evade internet censorship.

[1] The CPC has a process for licensing VPN services. Officially licensed VPNs are administered by state-owned enterprises and are monitored at all times. Corporate VPNs that bypass the GFW must keep VPN usage records (Koty, 2018). For these reasons, in this paper *VPN* refers to unlicensed and non-corporate VPNs.

Such heavy censorship has found to not only make it difficult to access sensitive information, it also fosters an environment in which people do not seek such information in the first place. Multiple studies have confirmed these findings, including one performed by researchers at Stanford and Peking University where 1,000 students at two different Beijing universities were given free tools to bypass the GFW. Half of them did not use the services at all, and almost none used them to browse foreign news (Yuan, 2018; Chen, 2019).

Many Chinese Internet users do not attempt to bypass the GFW to avoid persecution by the CPC. In June 2017, after enacting the same cybersecurity law that led to fines for Tencent, Weibo, and WeChat, multiple individuals selling unlicensed VPNs were arrested and sentenced to up to five and a half years in prison. In December 2018, a Shaoguan resident Zhu Yunfeng was fined RMB 1000 (roughly $163) for using a VPN, Lantern Pro, to access the Internet. The Chinese government intentionally made this fine public, perhaps to scare others from bypassing the GFW (Lam, 2019). Following incidents like these, Western VPN providers have acknowledged that their Chinese users may be prosecuted by the Chinese government (Markuson, 2019). Additionally, the Chinese government has created and deployed a technology that disables targeted devices like mobile phones that attempt to use unauthorized VPNs or download foreign messaging applications like Whatsapp (Yang, 2017). Activists in China who use the Internet to broadcast their messages quickly often face severe consequences. Huang Qi, a human rights activist who ran the popular website 64 Tianwang, for which he received the Cyber-Freedom Prize from Reporters Without Borders, was imprisoned for a third time in 2019 and is now serving a twelve-year sentence (BBC, 2019).

The CPC's Internet Censorship Leads to Collateral Damage

GitHub is a code-sharing website used by amateur and professional software engineers that is used globally, including China. Many businesses, especially software companies, rely on it to innovate and stay profitable. GitHub provides a good example of an internet service that is required inside China but also provides forms of censorship circumvention.

GitHub is used by organizations such as the Tor Project to distribute the Tor Browser and other information for circumventing Chinese censorship, and GreatFire, an anti-censorship organization. It is also used by activists in China such as the 996.ICU group to communicate with each other and foreign media companies (Feng, 2019). For these reasons, the CPC decided to block GitHub starting in early 2013. The pattern of blockages and techniques used by the CPC provide insight into what effects censorship can have beyond the CPC's main objective.

Innocent Services Are Blocked Unintentionally

The first two GitHub blocks occurred on January 21 and January 26, 2013, which lasted for two and five days respectively. The CPC blocked direct access to GitHub using two methods: a DNS hijacking attack, which made it difficult to load the webpage at all, and a man-in-the-middle attack, which loaded a version of the page from the Chinese government's servers, not a genuine version from GitHub. Although some organizations could bypass these attacks using VPNs or other proxies, many relied on mirror sites, effectively copies of the original sites. GreatFire runs mirror sites on the U.S.-based content delivery network Akamai, so to follow through with the GitHub block, the CPC instituted a block on all traffic from Akamai's servers. Although this did block the GitHub mirror sites, it also brought down thousands of other services including HSBC's Chinese banking services (Silbert, 2014; Carroll, 2014).

GitHub is not the only service to be blocked in such a coarse way. In fact, any website that uses Google's content delivery networks (CDNs) or integrate with a blocked service like Facebook or Twitter, will either have their functions limited or blocked entirely (Jiang, 2014). The CPC never intended to block these services, but that was the result of the censorship methods that have in place.

Some Censorship Techniques Have Global Effects

The CPC orchestrated a distributed denial of service (DDoS) attack on GitHub starting on March 26, 2015. Although the CPC was intending to block access to only two pages (a *New York Times* mirror and a repository of links to proxies that bypass the GFW), the attack crippled the entire website for nearly five days. Globally, GitHub faced outages that affected not only its free users, but also businesses that pay for their services (Rabkin, 2015). The attack was so notable that the software used to perform it became known as the Great Cannon (Marczak et al., 2015). The Great Cannon has been deployed several times: once in 2017 that targeted the New York-based Chinese-language news website Mingjing News, and most recently in August 2019, when it was used to temporarily take down the LIHKG forum where Hong Kong residents were organizing anti-Beijing protests, despite Hong Kong being outside the jurisdiction of the CPC's censorship (Cimpanu, 2019). The continued use and maintenance of a weapon like the Great Cannon shows that the Chinese government not only wishes to censor its domestic internet, but also wishes to censor the Internet more expansively, even globally.

Censorship Complicates Business Development

The censorship of GitHub provides an example of how censorship may negatively affect small business development. Following the first attack, founder of Beijing-based technology

incubator Innovation Works and former head of Chinese operations at Google Kai-Fu Lee criticized the block, stating that “Blocking GitHub is unjustifiable, and will only derail the nation’s programmers from the world, while bringing about a loss of competitiveness and insight” (Kan, 2013). Because GitHub was only blocked for a few days at a time, there were only very minor economic consequences. Although GitHub is accessible in China today, the lack of specific criteria determining when such a site will be blocked means that GitHub and other sites could be blocked again at any time, leaving small companies that depend on these sites scrambling to stay afloat (Koty, 2017). Large Chinese companies such as Alibaba, Tencent, and Baidu are not affected as heavily, as the CPC has waived many of the GFW’s restrictions for them (Yang, 2017). This uneven application of censorship is discussed in more depth later.

Alibaba is not, however, exempt from self-censoring in compliance with CPC policies. Alibaba must constantly monitor items being sold on its marketplaces, videos uploaded to its Youku service, and various other kinds of user-generated content. Self-censoring is not an easy task, and according to a report to investors in 2019, poses a serious business risk (Li, 2019).

On the other hand, blocking foreign services can act like cyber-tariffs, reducing international competition and promoting Chinese businesses. Kai-Fu Lee has stated that services such as Renren, a Chinese alternative to Facebook, without the GFW, would hold much less market share or not exist at all (Bao, 2013). The same can be said for the very large social media companies like Weibo (a Twitter alternative) and Baidu (a Google Search alternative) (Chander, 2013). Although the success of these companies and products in China is undeniable, most of these companies do not seem to compete globally due to the GFW. Because the population of China is so large and the GFW has prevented effective foreign competition, Chinese technology companies have developed economies of scale without the need to compete overseas. Most

companies, even some of the largest such as Baidu only provide Chinese-language interfaces, demonstrating that they do not currently seek a more global user base (Chander, 2013).

The CPC Knows That Some Censorship Decisions Affect Business and Education

The CPC allows some large private corporations and some universities, especially those associated with Western universities, to bypass the GFW (Koty, 2017). This is likely because the CPC is aware that these institutions benefit greatly from fewer restrictions. Yang (2017) argues that it also provides some legitimacy to the CPC's regime, quelling some potential political unrest.

Universities and Researchers in China Face Unequal Internet Restrictions

Some large universities in China have non-state-owned internet service providers, so they are able to bypass the GFW (Yang, 2017; Sharma, 2017). Although the CPC have the opportunity to crackdown on this, they do not. However, other researchers not affiliated with these institutions are hampered by the severe restrictions to global information. "Internet accessibility is a major obstacle for our research. It makes international collaboration difficult and damages the reputation and competitiveness of Chinese science institutes," said an astronomer in Beijing, who only spoke to the media anonymously out of fear of retaliation from the CPC (Normile, 2017). Luo Fuhe, Vice-Chairman of the Chinese People's Political Consultative Conference (CPPCC), recommended that the CPC lift restrictions on foreign sites that are frequently visited by experts, but his recommendations were not reported in official media and were quickly deleted from social media (Sharma, 2017).

U.S joint venture campuses in China are treated slightly differently, as the CPC must comply with the proposed terms for those institutions. The United States Government

Accountability Office (GAO) studied twelve institutions in China in 2015, and found in all cases that academic freedom was not restricted, as their respective agreements stipulated that academic freedom would not be infringed. Faculty could teach anything they chose, even if it was politically sensitive. Administrators of these universities maintained that academic freedom was nonnegotiable. However, internet censorship specifically was a challenge for seven out of the twelve campuses. At these campuses, restricted access to information, including online databases, significantly impacted productivity (GAO, 2017).

Some Chinese Corporations Do Not Face Heavy Internet Censorship

The Chinese government understands that many local companies greatly benefit from being able to bypass the GFW. Corporate site-to-site VPNs pose few legal issues, as they only route traffic between campuses, not out of China.[2] However, corporate VPNs that bypass the GFW exist in a legal gray area: they are neither explicitly allowed nor explicitly prohibited. Corporate VPN usage is not often targeted by the Chinese government, but they are sometimes affected by other crackdowns (Koty, 2018). Yang (2017) interviewed employees of various Chinese technology companies including Alibaba, Tencent, and Baidu and found that many of them had access to a VPN that bypassed the GFW.

Conclusion

There are many misconceptions about the extent of Chinese internet censorship and its purpose. As we have seen, internet censorship permeates nearly all areas of society, affecting university education and business operations. The CPC, in its efforts to stay in power, has

[2] Domestic site-to-site VPNs allow users in areas of China with slightly more restricted internet access to bypass those restrictions, but this does not concern the CPC.

successfully taken control of new and old media, having convinced individuals and private companies that their joint censorship efforts are righteous and justified. Company self-censorship is rampant. Although research can still be done and businesses can still be successful, being disconnected from global innovation and developments in every field is detrimental to both the Chinese people and the rest of the world. The CPC treads a fine line between political stability and economic success, often making rash decisions that harm its citizens. A new generation of children and students are growing up in China with limited curiosity for uncensored news and documents. Although internet regulation is not inherently harmful, the CPC's highly political censorship is. The steps it would take to reintroduce unrestricted political discourse to China are unclear. In fact, it is unclear if such steps should even be taken. In my view, freedom of information is essential for a thriving global society, and the Western world should continue to provide censorship circumvention tools for anyone who wishes to use them.

References

Bamman, D., O'Connor B., Smith, N. A. (2012, March 5) Censorship and deletion practices in Chinese social media. *First Monday.* journals.uic.edu/ojs/index.php/fm/article/view/3943/3169.

Bao, B. (2013, April 22). How Internet Censorship Is Curbing Innovation in China. *The Atlantic.* www.theatlantic.com/china/archive/2013/04/how-internet-censorship-is-curbing-innovation-in-china/275188.

BBC (2017, May 3). China announces tighter regulations for online news. *BBC News*. www.bbc.com/news/technology-39791781.

BBC (2019, July 29). China jails award-wining cyber-dissident Huang Qi. *BBC News*. www.bbc.com/news/technology-49150906.

CAC (2017, May 2). Cyberspace Administration of China. 互联网信息内容管理行政执法程序规定 [Provisions on Administrative Law Enforcement Procedures for Internet Information Content Management]. www.cac.gov.cn/2017-05/02/c_1120902931.htm.

Cadell, C., Li, P. (2017, Sep. 29). Tea and Tiananmen: Inside China's new censorship machine. *Reuters.* www.reuters.com/article/china-congress-censorship/tea-and-tiananmen-inside-chinas-new-censorship-machine-idUSL4N1LW25C.

Carroll, R. (2014, Nov. 18). China steps up web censorship and blocks HSBC. *The Guardian*. www.theguardian.com/world/2014/nov/18/china-blocks-hsbc-web-crackdown-censorship.

Chander, A. (2013, Aug. 12). How Censorship Hurts Chinese Internet Companies. *The Atlantic*. www.theatlantic.com/china/archive/2013/08/how-censorship-hurts-chinese-internet-companies/278587.

Chen, Q. (2019). When Chinese students were given the uncensored internet. *Inkstone*. www.inkstonenews.com/society/what-happened-when-researchers-gave-chinese-students-uncensored-internet/article/3015387.

Chen, Y. (2016). WeChat use among Chinese college students: Exploring gratifications and political engagement in China. *Journal of International and Intercultural Communication*. 1-19. 10.1080/17513057.2016.1235222.

Chen, Y., Yang, D. Y. (2019, June). The Impact of Media Censorship: 1984 or Brave New World? *American Economic Association*, 109(6), 2294-2332. doi.org/10.1257/aer.20171765.

Chin, J. (2015, April 28). China Internet Regulators Announce More Explicit Rules on Web Censorship. *The Wall Street Journal*. www.wsj.com/articles/chinas-internet-regulators-put-explicit-new-censorship-rules-in-place-1430233546.

Chin, S.J. (2018). Institutional Origins of the Media Censorship in China: The Making of the Socialist Media Censorship System in 1950s Shanghai. *Journal of Contemporary China*, 27(114), 956–972. doi.org/10.1080/10670564.2018.1488108.

Cimpanu, C. (2019, Dec. 4). China resurrects Great Cannon for DDoS attack on Hong Kong forum. *Zero Day*. www.zdnet.com/article/china-resurrects-great-cannon-for-ddos-attacks-on-hong-kong-forum.

Clark, Justin; Robert Faris; Rebekah Heacock Jones (2017). Analyzing Accessibility of Wikipedia Projects Around the World. *Berkman Klein Center for Internet & Society Research Publication.* nrs.harvard.edu/urn-3:HUL.InstRepos:32741922.

Creemers, R. (2015, Dec. 1). The Pivot of Chinese Cybergovernance: Integrating Internal Control in Xi Jinping's China. *China Perspectives.* journals.openedition.org/china perspectives/pdf/6835.

Feng, E. (2019, April 10). GitHub Has Become A Haven For China's Censored Internet Users. *NPR.* www.npr.org/2019/04/10/709490855/github-has-become-a-haven-for-chinas-censored-internet-users.

GAO (2016, Aug.). U.S. Universities in China Emphasize Academic Freedom but Face Internet Censorship and Other Challenges. *United States Government Accountability Office*. www.gao.gov/assets/680/679322.pdf.

GreatFire (2020, March 23). Censorship of Alexa Top 1000 Domains in China. Webpage. en.greatfire.org/search/alexa-top-1000-domains. Retrieved March 23.

Griffiths, J. (2020, Feb. 7). China's censors tried to control the narrative on a hero doctor's death. It backfired terribly. CNN. www.cnn.com/2020/02/07/asia/china-doctor-death-censorship-intl-hnk/index.html.

Guo, S., & Feng, G. (2012). Understanding Support for Internet Censorship in China: An Elaboration of the Theory of Reasoned Action. *Journal of Chinese Political Science*, 17(1), 33–52. doi.org/10.1007/s11366-011-9177-8.

Jiang, E. (2014). How Google's CDN prevents your site from loading in China. *Medium*. edjiang.com/how-googles-cdn-prevents-your-site-from-loading-in-china-67504845cd04.

Kan, M. (2013, Jan. 23). GitHub unblocked in China after former Google head slams its censorship. *Computerworld*. www.computerworld.com/article/2493478/github-unblocked-in-china-after-former-google-head-slams-its-censorship.html.

Koty, A.C. (2017, June 1). China's Great Firewall: Business Implications. *China Briefing*. www.china-briefing.com/news/chinas-great-firewall-implications-businesses.

Koty, A.C. (2018, June 21). Why HR Should Care about VPN Use in China. *China Briefing*. www.china-briefing.com/news/vpn-china-hr-due-diligence.

Lam, O. (2019, Jan. 20). Chinese authorities go after citizens for using VPNs to skirt online censorship. *Hong Kong Free Press*. www.hongkongfp.com/2019/01/20/chinese-authorities-go-citizens-using-vpns-skirt-online-censorship.

Li, J. (2019, Nov. 14). Alibaba reminds investors China's censorship regime is a business risk. *Quartz*. qz.com/1748450/alibaba-hong-kong-filing-cites-chinas-censorship-as-business-risk.

Lu, J., Zhao, Y. (2018, Jan.). Implicit and Explicit Control: Modeling the Effect of Internet Censorship on Political Protest in China. *International Journal of Communication.* ijoc.org/index.php/ijoc/article/view/8532/2427.

MacKinnon, R. (2012, Jan. 29). Inside China's censorship machine. *National Post.* nationalpost.com/opinion/rebecca-mackinnon-inside-chinas-censorship-machine.

Mai, J. (2017, Dec. 3). Xi Jinping renews 'cyber sovereignty' call at China's top meeting of internet minds. *South China Morning Post*. www.scmp.com/news/china/policies-politics/article/2122683/xi-jinping-renews-cyber-sovereignty-call-chinas-top.

Marczak, B., Weaver, N., Dalek, J., Ensafi, R., Fifield, D., McKune, S., Rey, A., Scott-Railton, J., Deibert, R., Paxson, V. (2015). China's Great Cannon. *The Citizen Lab*. citizenlab.ca/2015/04/chinas-great-cannon.

Markuson, D. (2019, Aug. 25). *What is the best VPN for China?* nordvpn.com/blog/vpn-for-china.

McCarthy, N. (2018, Aug. 23). China Now Boasts More Than 800 Million Internet Users and 98% of Them Are Mobile. *Forbes.* www.forbes.com/sites/niallmccarthy/2018/08/23/china-now-boasts-more-than-800-million-internet-users-and-98-of-them-are-mobile-infographic/#63c0b8607092.

Normile, D. (2017, Aug. 13). Science suffers as China's internet censors plug holes in Great Firewall. www.sciencemag.org/news/2017/08/science-suffers-china-s-internet-censors-plug-holes-great-firewall.

Rabkin, A. (2015, April 6). Cyberattack Shows That China Isn't Content to Censor Its Own Internet. *Slate*. slate.com/technology/2015/04/github-ddos-attack-shows-china-isn-t-content-to-censor-its-own-internet.html.

Sharma, Y. (2017, July 13). Research could suffer as internet controls tightened. *University World News*. www.universityworldnews.com/post.php?story=20170713140950894.

Shepherd, C. (2017, May 2). China tightens rules on online news, network providers. *Reuters*. www.reuters.com/article/us-china-internet-censorship-security/china-tightens-rules-on-online-news-network-providers-idUSKBN17Y0Y6.

Shih, J. (2019, Jan. 4). Chinese censors go old school to clamp down on Twitter: A knock on the door. *Washington Post.* www.washingtonpost.com.

Silbert, S. (2014, Nov. 26). Routing around the Great Firewall of China. *Los Angeles Times*. www.latimes.com/business/technology/la-fi-tn-great-firewall-china-censorship-20141126-story.html

Wong, M., & Kwong, Y. (2019). Academic Censorship in China: The Case of The China Quarterly. PS: Political Science & Politics, 52(2), 287-292. doi:10.1017/S1049096518002093.

Yang, K. (2017). The door is closed, but not locked: China's VPN policy (Order No. 10273805). *ProQuest Dissertations & Theses Global*. (1897546080).

Yuan, L. (2018, Sep. 5). Young People in China Don't Know The Internet We Do – And They Like It That Way. *The Independent*. www.independent.co.uk/life-style/gadgets-and-tech/features/china-internet-social-media-great-firewall-of-china-censorship-apps-a8510036.html.

Yuan, L. (2019, Jan. 2). Learning China's Forbidden History, So They Can Censor It. *New York Times.* www.nytimes.com/2019/01/02/business/china-internet-censor.html.

Zheng, S. (2017, July 23). VPN crackdown an "unthinkable" trial by firewall for China's research world. *South China Morning Post*. www.scmp.com/news/china/policies-politics/article/2103793/vpn-crackdown-unthinkable-trial-firewall-chinas.