Sigma: Journal of Political and International Studies

Volume 39 Article 4

2022

Censorship Sensing: The Capabilities and Implications of China’s Great Firewall Under Xi Jinping

Emily Quan

Censorship Sensing: The Capabilities and Implications of China’s Great Firewall Under Xi Jinping

Emily Quan

Totaling over 989 million users at the end of 2020, Chinese Internet users interact with unprecedent amounts of data, communication, and media (Xu 2020). It is a far cry from 1987, when the first email was sent from China to the Karlsruhe Institute of Technology. The message in the email, later popularized on QQ desktops, was this: “Across the Great Wall, we can reach every corner of the world” (越过长城，走向世界, *Yuèguò Chángchéng, Zǒuxiàng Shìjiè*) (Internet Archive 2013).

This prophecy has certainly come true as China approaches a billion domestic Internet users. However, it also speaks to a certain irony that stems from the Chinese government’s extensive censorship across its networks: even as the Internet continues to function as a tool to connect individuals across the globe, how Chinese Internet access is partitioned off is creating an increasingly insular community within the country. This paper will begin with a brief history of the Internet in China and the corresponding evolution of Chinese technological censorship efforts. It will then discuss our current understanding of Chinese censorship systems as understood by outside network and censorship researchers and will explore the capabilities of its current implementation. It will then pivot to analyze what the implications of the censorship system’s understood abilities mean for understanding Xi Jinping’s leadership and examine economic and diplomatic consequences of Chinese censorship under Xi.

Although this paper necessarily focuses on the technical aspects of these networking systems in some areas, a computer networking or technical background is not necessary to understand the implications of the described capabilities. Focus on the technical implementation will only be described to outline basic abilities and limitations. Definitions will be provided to make important technical terms accessible to readers who do not stem from a technical background.

China's Internet and Censorship History

China's relationship with technology is all the more incredible when we consider its meteoritic rise over the past few decades. Although China has boasted significant scientific advances throughout history, it arrived relatively late to the game of modern science and technology. Its lack of modern military warfare in the 1800s directly contributed to the Century of Humiliation, during which foreign powers that took advantage of its resources and wealth (Joseph 2019, 52). Although the Republic of China began the advent of modern science in China as key Chinese figures received their education abroad and founded schools and universities in China, many of these institutions moved to Taiwan after the Communist Party gained power in 1949. Under Mao's rule, nuclear and satellite technology were the only regions that experienced significant scientific advancement (Joseph 2019, 91). The disastrous policies that resulted in the Great Leap Forward and the Cultural Revolution meant that China's populace was too consumed with fulfilling the Party quotas and dealing domestic shortages to make much progress in scientific advancements.

But if China has arrived relatively late in using technology to cement gains in international power, it has also excelled in catching up. Once it was ready to position itself for greater growth and economic development, it seized the opportunity to leverage science and technology as a vehicle for ascendancy. Science and technology were a pillar of the Four Modernizations announced by Deng Xiaoping for economic development in 1975, and in the period since then, it has positioned itself as one of the world's leading STEM leaders (Joseph 2019, 128). One measure that illustrates this is that, by some counts, China is the largest producer of scientific articles (Tollefson 2018).

China's relationship with the Internet has followed similar trends. Because the Internet began as an American government-related project, China did not play a significant part in the formation of key Internet infrastructure entities and services. However, in the ensuing years, China has seized the opportunity to both capitalize on providing services and amassing soft power. These efforts have included heavy investment in telecommunications infrastructure both domestically and in at least 16 countries as part of its Digital Silk Road (DSR) initiative, an extension of Beijing's Belt and Road Initiative strategy (Kurlantzick 2021). Its efforts to place Chinese needs and users at the center of Internet operations have also resulted in the development of its censorship model.

Although the first email from China was sent in 1987, the Internet did not arrive in China until 1994 under the leadership of Jiang Zemin. In parallel with the Internet's release, the Ministry of Public Security (MPS) in China worked on a project known as the Golden Shield, which was released in 2000 during a trade show in Beijing (Torfox 2011). The project aim was to act as a comprehensive surveillance system that would link all citizens' records at various levels. However, as the technology continued to advance at a rapid pace, the system shifted from linking information to filtering specific content for individuals in an expansive surveillance system.

The Golden Shield project is colloquially referred to as the Great Firewall of China (GFW). Co-located within the GFW is a project known as the Great Cannon, which is an offensive Internet attack tool that has been used to launch distributed denial-of-service attacks against websites that cause severe political problems for China (Marczak et al. 2015). An example of this is when the Great Cannon was used to attack GitHub, a popular web-based code hosting service, in 2015, perhaps due to the fact that GitHub hosts resources that detail how to circumvent censorship (Marczak et al. 2015). The Great Cannon has not been deployed extensively and has generally been used in response to what it considers "foreign hostile actors."

Under current President Xi Jinping's leadership, censorship efforts have continued with the proliferation of the Internet. In 2013, his first year in office, it was reported that over two million people were used as "public opinion analysts" to manually censor posts and observe user activity (Hunt and Xu 2013). Other individuals were hired to make patriotic posts and comments, introducing a barrage of CCP-positive material into Chinese cyberspace. Continued Chinese propaganda and censorship efforts make use of both human operators and algorithms to promote Party lines and censor sensitive topics.

Under President Xi Jinping's leadership, China has seen an increase in censorship across all forms of media. One example is that Chinese internet companies are required to sign a document entitled "Public Pledge on Self-Regulation and Professional Ethics for the China Internet Industry" (Albert and Xu 2017). Previous workarounds for bypassing censorship technologies, such as the use of virtual private networks (VPNs), have been blocked. In February 2016, Xi also announced increased restrictions for state media to better adhere to Party doctrine. As China's censorship efforts continue to develop and expand, the government's central purpose is to safeguard the Chinese Communist Party's (CCP) will, authority, and unity (Zhou 2020).

Research Objectives and Limitations

Although significant research on the technical capabilities and weaknesses of the GFW has taken place over recent years, much of this research has only been examined through a technical or computer networking basis. The purpose of this paper is to present a holistic picture of the extent to which the GFW filters information on a regional, platform-specific, and time-sensitive basis, and to contextualize it within past and current Chinese political events.

This section begins with a necessary disclaimer for understanding the limitations of research performed to understand the GFW. Researchers experience limitations regarding the GFW due to several reasons. Much of the research surrounding the GFW relies on testing its keyword filtering capabilities, which means that researchers test specific words within Chinese networks and record which entries experience censorship. The consequence of this method is that it primarily relies on guess-and-check. New discoveries in this area are generally made using suggestions from knowledgeable Chinese citizens or political scientists who study these areas or rely on accidental discoveries based on sample search queries. For example, Rambert et al. discovered that including the English version of the word “search” in an HTTP query (the data sent to a server when a user navigates to different webpages) resulted in the query being subjected to an expanded blocklist of words (Rambert et al. 2021). However, this discovery was only made through empirical methods.

Another limitation is that many researchers lack the ability to establish network infrastructure in China to directly test queries and other statistics from Chinese Internet infrastructure. As research from Rambert et al. has also shown, routing locations do make a difference in the types of queries that are censored (Rambert et al. 2021). Additionally, queries that researchers use do not always mirror natural banter or entries that most users might enter, meaning that researchers’ data results may ultimately be subject to more or less censorship than the average Chinese netizen. Although serious researchers in this area tend to use Chinese infrastructure to test their queries, there is not a definitive way to ensure that these servers are not experiencing disproportionately more or less censorship than the average Chinese Internet user (Christin 2021).

Timing also plays a factor into researchers’ results; many of the censorship implementations used for the Great Firewall vary week to week and have been shown to have tighter or varied controls during significant Party events or sensitive breaking news topics, such as the disappearance of famed Chinese tennis player, Peng Shuai (Mozur, Xiao, Kao, and Beltran 2021). Based on this, some studies may be skewed in their results based on global occurrences that may result in greater censored material during certain points of time. It is also possible that research machines and/or IP addresses may experience disproportionate censorship due to the number of controversial topics they periodically send. However, this is generally addressed in research findings, and researchers have not reported inconsistencies that would suggest such directed interference (Rambert et al. 2021).

Great Firewall Implementation

Contrary to the monolithic approach that its name suggests, the GFW does not actually constitute a single firewall. Rather, Chinese censorship utilizes a wide variety of techniques and is implemented at different stages of data transfer. The techniques that the GFW uses include, but are not limited to: IP range bans, URL filtering, DNS tampering, deep packet filtering, man-in-the-middle attacks, and TCP reset attacks (Asim 2021). This section will focus on several key techniques used as part of deterrence implementations.

An important feature of Chinese Internet censorship relies on DNS (Domain Name Service) poisoning, which is used to unconditionally block websites listed on a blacklist. DNS poisoning, which is also referred to as DNS tampering, is carried out by storing incorrect or fake information in the storage of a server, causing users to be redirected to the wrong website. In the case of Chinese censorship, a DNS-poisoned website will appear to be blocked or seem as if it has difficulty loading.

The top three categories of blocked domains are "business," "pornography," and "information technology" (Hoang et al. 2021, 3385). Approximately 311k domains are blocked daily within China, although it is worth noting that only around 1.3% of these domains rank among the top 100k most popular websites. Within the sub-domain of "information technology" are many popular global websites such as Google, Facebook, YouTube, and Twitter, which have been effectively replaced in Chinese cyberspace with Chinese copycat equivalents, such as WeChat, Sina Weibo, and Tencent QQ.

The blacklist of domains is dynamic, which is supported by the fact that COVID-19 related domains have also been censored (Rambert et al. 2021). Changes to the list also rely on manual and automated additions. This is supported by the fact that several higher education domains were also included in the block list that are targeted specifically without justification. Although the inclusion of many of these institutions' domains make sense based on their research on Chinese censorship and the Chinese government, other very specific entries, such as the sub-domain cs.colorado.edu (which is not currently in use), point to the fact that the list relies on manual and automated additions.

Several studies have reported the use of a penalty box in Internet transactions that contain filtered keywords (Xu, Mao, and Halderman 2011). This is an effective deterrence mechanism: if a user submits a request that includes a filtered keyword, then there is a 50–75% chance that requests submitted in the next 90 seconds afterwards will also be blocked, even if the subsequent requests don't contain filtered keywords (Rambert et al. 2021). The GFW further strengthens its Web censorship via HTTP/HTTPS filtering by deploying two separate censorship systems (Bock, Naval, Reese, and Levin 2021). The second system has been deployed since at least September 2019, and functions as a "backup censorship" system that runs in parallel to the main system and often blocks Web traffic that remained undetected by the first.

In addition to Internet filtering and blocking, chat clients in popular applications and games are also subject to censorship. A key difference for censorship performed for chat clients and games is that the words and material blocked is often company dependent. An analysis of top-downloaded mobile games in China showed that there was no single list of filtered keywords; the three statistically significant factors between censored lists were approval date, publisher, and developer (Knockel, Ruan, and Crete-Nishihata 2017). This points to a more decentralized model of the GFW than generally imagined, though at the same time points to evidence that regulation of censorship for games is still enforced via centralized regulations (due to the correlation with publisher date).

The Nature of Censored Material

Researchers have generally relied on compiled word lists and websites that include entries that have been blocked in the past to conduct future network observation studies. Categories of observed blocked Wikipedia entries include: the topic of censorship; censorship circumvention; sensitive events, such as Chinese protests; the Falun Gong (a religious movement that is regularly persecuted by the Chinese government), sensitive terms involving the government, such as the term "Princeling," which refers to the children of high-level government officials; various magazines, media, newspapers, and organizations; dissidents; certain political officials; regional issues that involve Hong Kong, Taiwan, Xinjiang, or Tibet; and Tiananmen ("Complete GFW Rulebook" 2021). Studies examining filtered keywords generally rely on word lists such as the Wikipedia 2014 and 2020 lists of censored words, which have similar categories with similarly sensitive people, organizations, or events that the Chinese government hopes to avoid.

There are various instances where users are subject to different filtered keyword lists. One is that users that submit search results inside of China are subject to different filtering restrictions than users outside of China. For example, foreign users have the terms "Coronavirus," "Remdesivir," and "Epidemic" filtered, whereas users located inside of China do not; this points to different objectives for filtering different audiences (Rambert et al. 2021).

Another instance is that users that have the English word "search" in HTTP requests are subject to an expanded keyword filtering list. For example, "法轮" (Falun Gong, a Chinese religious movement) is blocked when the English word "search" is included, but is not when the word is not present. Other variations of the word search, including words for "search" in Chinese, did not trigger the expanded blocklist (Rambert et al. 2021). Individuals who include the English word for "search" likely have more exposure to foreign information or influences, and also likely have enough fluency in English to understand articles stored on English webpages. Therefore, this discrepancy is likely indicative of the Chinese government's desire to detect and deter individuals from specific backgrounds from learning about sensitive topics.

Although the discussion of filtering up to this point has been focused on keyword filtering (blocking websites, requests, or content based on specific words or phrases), an analysis of filtering based on a user's location, profile, and/or other media used, such as pictures, has also been performed. Based on this analysis, the strongest predictor of censored posts on Weibo, a popular Chinese social media platform, was negative sentiment (Arefi 2020, 13).

Proactive and Reactive Filtering

GFW filtering has also been shown to be dynamic based on global and domestic events. Changes to filtered keywords, for example, are reflected in significant weekly changes that take into account recent events that censors hope to block. An interesting aspect of this is that keywords are also regularly removed from lists when they become irrelevant – showing that the government recognizes a need to provide Chinese netizens with a degree of Internet independence. The number of words that are changed on a regular basis are substantial: from a blocklist of about 1,400 words, some regions experienced hundreds of these words were removed or added based on the week and the region of the country (Rambert et al. 2021). This indicates that some regions may be subject to more robust oversight on censorship filtering than others, which also points to either sensitivity in regional control or a decentralization of censorship oversight. For example, Guangzhou experienced only one or two keyword changes to a list of over 1000 blocked words over a week, whereas Shanghai had 600 changes to this list during the same week (Rambert et al. 2021).

The time-sensitive filtering aspects of the GFW are most on display during two types of events: significant government events, which involve proactive filtering, and global or domestic events that spark outrage or dissent, which involve reactive filtering. An analysis of censored WeChat messages during China's 19th National Communist Party Congress in 2017 showed that even potentially neutral and positive messages that pertained to sensitive topics, such as Xi Jinping and the military, were blocked in the days leading up to and following the event. The top categories of blocked phrases and words were: Xi Jinping, references to a power transition, leadership, and Party policies and ideologies. Phrases blocked that revolved around Xi specifically included references to his desire to stay in power, critiques of his leadership, and his family (Ruan et al. 2020, 513). However, although many of the critical phrases remained blocked, around 50% of the tested phrases were unblocked a year after the Congress, which shows that censors recognize the importance of a certain degree of information flow is necessary to placate users.

Reactive censorship is more difficult to measure because such events occur without warning and the dynamics of netizen actions during/following an event are similarly volatile. However, events such as controversy over the recent disappearance of famous Chinese tennis star, Peng Shuai, show reactive censorship at work. After Peng's initial controversial post was deleted from Weibo, China's version of Twitter, censors quickly deleted other posts referring to her claims and banned a large scope of adjacent topics, including the topic of "tennis." Xiao Qiang, a researcher from UC Berkeley, noted that several hundred keywords were banned in relation to the incident (Mozur et al., n.d.). The aftermath of this event and the subsequent relaxation of censorship around Peng Shuai will remain to be seen, and will likely depend on future international engagement and events.

Focusing on Narrative Control

The government has realized that in its pursuit of a unified China, control over the narratives perpetuated over Chinese networks takes precedence over granular control of information. After the establishment of the People's Republic in China in 1949, information that entered and exited China was tightly controlled. It was not until the Reforms and Opening-up period under former President Deng Xiaoping that China became open to foreign exchanges, and even then, foreign nationals were still viewed with suspicion in context of the prior humiliations that China had endured at the hands of foreign powers (Sina News 2003). However, with the scope of the Internet, the Chinese government recognizes that even if it is able to deploy advanced censorship mechanisms to monitor and scrub certain pieces of unwanted information, it is no longer able to vet every source of new information that enters its borders. It has therefore also opted for control over how information is perceived to accompany its technological censorship efforts.

If the government can control the narrative, then it can shape the lens through which people filter information, and which will determine how much information will spread. Both concepts work hand in hand. If the government narrative is repeated and rigorously taught from a young enough age, then the populace will not be interested in researching additional information, even if it is possible to obtain. On the other hand, if the information flow into China can be shaped in such a way that almost all data supports or does not heavily discount the official narrative, then it strengthens the official narrative because alternate viewpoints are not easily obtained. This point is supported by the alternative keyword list when the English word “search” is included in search requests (Rambert et al. 2021). This forms a key principle of success behind the Chinese Firewall: information does not have to be blocked absolutely. Making information harder to obtain or access can act as a sufficient deterrent for most people. This principle is clear when we consider the “penalty box” mentioned earlier, which blocks traffic after a user searches for a blocked keyword (Xu et al. 2011).

The reach with which the Chinese government has implemented censorship through the GFW is extensive for filtering traffic coming outside of China but is surprisingly dynamic within China. The difference in block lists for international vs. domestic traffic shows that China has different objectives in its censorship. Censorship of outside traffic controls China’s image to the outside world, whereas domestic censorship is used to prevent undesirable information leaks.

Many of the studies that focused on variations in filtered keywords also found significant variations between the lists companies and service providers used. This suggests that censorship is generally decentralized between various entities. This decentralization extends to regional variations as well, as evidenced by the earlier example that shows censorship differences between Guangzhou and Shanghai. Although general guidance on what to block is likely issued from a centralized CCP authority, it has been noted that it is likely that much of the granular control of specific words being censored or not is most likely up to individual network administrators (Christin 2021). This explains the variability of some of the censorship observed throughout the research.

The implication of traffic through Internet Service Providers (ISPs) for major cities such as Beijing and Shanghai experiencing significantly less censorship is that the Chinese government understands that censorship within its intranet is more sensitive, and that it must be wary of allowing “maximal” search/message freedom to its citizens (so long as the data originates from a relatively safe source within the country, as opposed to traffic coming from abroad). Little to no censorship was observed for traffic between Hong Kong and international entities, which supports the idea that the government minimizes its use of censorship to placate its citizens.

This finding is especially interesting when we consider that the primary challenge of information control for the Chinese government may come from within its borders. Many Westerners incorrectly assume that the primary challenge of information control comes from the outside and assume that Chinese who are unaware of some of the more sensitive points of their country's history would immediately turn against their government if exposed to information about events such as Tiananmen. This is not necessarily the case. One author noted informal evidence against this in 2014 with students from prestigious Beijing universities such as Tsinghua and Peking University. When the author asked the students about their knowledge about the Tiananmen incident, many of the students were unaware of what had happened; in other cases, students defended the government's stance, even if they saw it as rather extreme. The reality is that "the propaganda apparatus has laid the groundwork so well that most students simply have no interest in questioning the government's version of events" (Lim 2015, 88).

The larger existential threat for the Chinese government may be that it is a victim of its own success. The exponential rise in standards of living across the board has set up high expectations for the future. At the turn of the century, China's roadways were dominated by bicycles; today, automobiles dominate the highways. Real weekly wages have increased 8-fold between 2000 and 2016, from 100 to 800 yuan (Zhang and Wu 2016). China's per capita GDP has more than doubled from 2010 to 2020, from $4,600 to $10,500 (Goldkorn 2021). President Xi has promised to eliminate inequality and continue China's prosperity, but many factors that remain out of his control may stand in the way of his delivery.

Against this backdrop, Chinese social media boards and blogposts are effective amplifiers for citizens to express discontent. The sheer amount of Internet users can be encapsulated in the popular term 人肉搜索 (*Rénròu Sōusuǒ*), which describes the powerful research capabilities Web bloggers and users to uncover and investigate information. Although the government is masterful at censoring data at will, it is also aware that heavy-handedness in censorship efforts decreases trust in citizen platforms, which it uses to measure public opinion. It understands that there is a delicate balance between deciding when to censor information and when to allow the public to blow off steam; too much, and leadership may lose control and credibility in the narrative.

Because the government walks a thin line between control and consent, Chinese netizens are able to successfully use the Web to advocate for issues that are important to them, such as environmental concerns and corruption. Outcry over unpopular decisions by local officials also results in greater scrutiny, allowing citizens to effectively hold many lower-level officials accountable even as top leadership remains taboo (Downey 2010). At the same time, the Chinese government is able to effectively channel the public outrage into channels that are not sensitive to the CCP's positions. For example, during the Diaoyu protests in 2012, the Chinese government said nothing while citizens gathered to protest against Japanese businesses (BBC

2012). As protestors united behind Chinese nationalism and railed against Japan in a cause that the Party supported, the government allowed the protests to continue.

Future Implications

As President Xi seeks to shape a "unified and resurgent China," he will continue to leverage technology to promote this narrative within the country (Economy 2022). Censorship is a crucial tool for ensuring that the conformity of opinion works towards, not against, the country's goals. As China continues to assume regional power over information access and dissemination, it is also hoping to shift the traditional way in which the Internet is regulated: as China's computer networks grow more insular, it is establishing its own form of Internet governance within its borders that trumps international norms.

Despite the fact that netizens are given some independence in the range of topics they can discuss, the extensive number of banned words and phrases that involve President Xi Jinping are in line with his current rise in power and authority. With the rise of Xi's cult of personality, which has been compared to a similar craze around Mao, the outsized sensitivity in censorship around his policies and power reflects either a fragility in his grip on power or a consolidation of authority—and it is possible that the answer is a mixture of both.

In parallel with how Mao effectively "Sinicized" Marxist-Leninist principles for application for China, Xi has also declared a similar vision for China's cyber future. The Cyberspace Administration of China (CAC), the country's regulator and censor, announced the government's intentions to ideologically censor and verify that algorithms adhere to Xi Jinping Thought on Socialism with Chinese Characteristics, specifically regarding "internet information service algorithms at consumer-facing internet companies" (Goldkorn 2021). Through this announcement, Chinese leadership is signaling its intentions to further ensure that the Internet serves to further the CCP's purposes—not the other way around.

As Xi continues to promote domestic businesses as part of China's rise, Chinese censorship of the Internet has provided a significant opportunity for Chinese companies to fill in a vast consumer niche in technological services. The fact that many popular Western websites are blocked is not a loss that is largely felt within the country because there are thriving Chinese equivalents for users. This may serve as a successful precedent for Chinese companies to capture markets in other sectors. Many Western companies that once operated in China have recently withdrawn from the market, citing difficulties imposed by the government. If the Chinese government recognizes that Chinese companies are able to replace other markets successfully, then they may continue to push for regulation that favors Chinese leadership and corporations. A smaller-scale example of this is Manner Coffee, a coffee shop brand that could be positioned to rival and eventually replace Starbucks as the provider in the market. As Xi Jinping continues to advance his Common Prosperity policies and favors domestic consumption, the success of Internet companies in satisfying their markets may serve as an encouraging precedent for his strategy (Che 2021).

The implications of Xi's vision extend well beyond China. In its dealings with other countries regarding the Digital Silk Road, a technological branch of China's Belt and Road Initiative, Beijing has provided training on how to censor Internet efforts (Kurlantzick 2021). This points to the larger issue of how China is exporting digital authoritarianism, and how its censorship efforts may not remain isolated to its own citizens. Additionally, as China becomes more confident as a leader on the world stage, it may have less reservations about displays of offensive cyber capabilities. The Great Cannon, an attack system co-located with the GFW, may be viewed as an increasingly attractive option for Chinese leaders wishing to push back on corporations or governments who fail to cooperate.

China may not be content to showcase its might through soft power as it takes an expanded leadership role on the global stage. It may see fit to make use of its offensive Great Cannon capabilities as those whom it deems "hostile foreign powers" continue to threaten China's harmonizing model. For example, increasing tensions over Taiwan between China and America and its allies may result in unprecedented cyber campaigns as a prelude to other military escalations. Such a possibility is not remote: Taiwan is already reporting around five million cyberattacks and probes daily, the overwhelming majority of which originate from the mainland (AFP 2021). As China seeks reunification, it could see the use of the Great Cannon against the Taiwanese government as an excellent symbolic move to neutralize some of its Internet capabilities. The last significant usage of the Great Cannon against GitHub was a significant message to the world: by targeting one of the world's largest codebases, China directly signaled to the West that any of its technology that stands in the way of the CCP is fair game.

The continued decoupling of Chinese Internet users from the rest of the world through censorship exacerbates a significant rift between China and its counterparts. Complete control comes at a cost for China: the more that Chinese censorship is actively deployed, the more it advertises its insecurities to the outside world and risks stoking the outrage of its own netizens. However, it is a cost that it is increasingly eager to pay. Subsequently, outsiders will need to pay careful attention to changes in Chinese censorship models as its model is successfully exported to other authoritarian regimes to silence dissent and perform surveillance. As the CCP grows more insular in its dealings with the outside world, understanding the topics that are important to them through empirical observation will become critical to understanding its domestic and international aims—seeing both the image it wishes to present and the image it seeks to hide.

WORKS CITED

Albert, Eleanor, and Beina Xu. *Media Censorship in China*. February 17, 2017. https://www.cfr.org/backgrounder/media-censorship-china#chapter-title-0-4 (accessed December 18, 2021).

Arefi, Meisam Navaki. *Data Mining of Chinese Social Networks: Factors That Indicate Post Deletion*. PhD Thesis, Albuquerque: University of Mexico, 2020.

Asim, Uneeb. *The Great Firewall of China: Everything You Need to Know*. August 15, 2021. https://www.thetechlounge.com/great-firewall-of-china/ (accessed December 18, 2021).

BBC. *Anti-Japan protests across China over island dispute*. August 19, 2012. https://www.bbc.com/news/world-asia-19312226 (accessed December 18, 2021).

Bock, Kevin, Gabriel Naval, Kyle Reese, and Dave Levin. "Even Censors Have a Backup: Examining China's Double HTTPS Censorship Middleboxes." *FOCI '21*. ACM, 2021.

Che, Chang. *The rise of Manner Coffee: SupChina.* November 5, 2021. (accessed November 16, 2021).

Christin, Nicolas, interview by author. *CMU Q&A* (November 22, 2021).

Complete GFW Rulebook. n.d. docs.google.com/spreadsheets/d/11GBNGwMP0XOVKCR5AG1PJ1U2dJCNQG7U3L-Sx8zz1cw/edit#gid=1 (accessed December 18, 2021).

Downey, Tom. *China's Cyberposse: New York Times*. March 3, 2010. (accessed November 16, 2021).

Economy, Elizabeth. *Foreign Affairs*. January 2022. foreignaffairs.com/articles/china/2021-12-09/xi-jinpings-new-world-order (accessed March 15, 2022).

Goldkorn, Jeremy. *Government announces three-year plan to tame China's algorithms: SupChina*. September 29, 2021. (accessed November 16, 2021).

—. *Xi Jinping's greatest hits, so far*. November 10, 2021. supchina.com/2021/11/10/xi-jinpings-greatest-hits-so-far/ (accessed December 18, 2021).

Hoang, Nguyen Phong, et al. "How Great is the Great Firewall? Measuring China's DNS Censorship." *Proceedings of the 30th USENIX Security Symposium*. USENIX, 2021. 3381-3398.

Hunt, Katie, and CY Xu. *China 'employs 2 million people to police internet*'. October 7, 2013. cnn.com/2013/10/07/world/asia/china-internet-monitors/index.html (accessed December 18, 2021).

Joseph, William. *Politics in China: An Introduction*. Oxford University Press, 2019.

Knockel, Jeffrey, Lotus Ruan, and Masashi Crete-Nishihata. "Measuring Decentralization of Chinese Keyword Censorship via Mobile Games." *7th USENIX Workshop on Free and Open Communications in the Internet*. Vancouver: USENIX Association, 2017.

Kurlantzick, Joshua. *Assessing China's Digital Silk Road Initiative*. January 1, 2021. cfr.org/china-digital-silk-road/ (accessed December 18, 2021).

Mail Administration for China. "China First Email." *Internet Archive*. September 14, 1987. archive.org/details/ChinaFirstEmail (accessed December 19, 2021).

Marczak, Bill, et al. *China's Great Cannon*. April 10, 2015. citizenlab.ca/2015/04/chinas-great-cannon/ (accessed December 18, 2021).

Mozur, Paul, Muyi Xiao, Jeff Kao, and Gray Beltran. "Beijing Silenced Peng Shuai in 20 Minutes, Then Spent Weeks on Damage Control." *New York Times*, December 8, 2021.

Rambert, Raymond, Zachary Weinberg, Diogo Barradas, and Nicolas Christin. "Chinese Wall or Swiss Cheese? Keyword filtering in the Great Firewall of China." *Proceedings of the Web Conference 2021*. New York: ACM, 2021.

Ruan, Lotus, Masashi Crete-Nishihata, Jeffrey Knockel, Ruohan Xiong, and Jakub Dalek. "The Intermingling of State and Private Companies: Analysing Censorship of the 19th National Communist Party Congress on WeChat." *The China Quarterly*, 2020: 497–526.

Sina News. July 8, 2003. news.sina.com.cn/c/2003-07-08/0611337601s.shtml (accessed March 14, 2022).

Tollefson, Jeff. *China declared world's largest producer of scientific articles*. January 18, 2018. nature.com/articles/d41586-018-00927-4 (accessed March 14, 2022).

Torfox: A Stanford Project. *The Great Firewall of China: Background*. June 1, 2011. cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/author/pingp/index.html (accessed December 18, 2021).

Xu, Nadeem. *Asia Times*. February 4, 2021. asiatimes.com/2021/02/chinas-internet-users-hit-989-million-in-2020/ (accessed December 18, 2021).

Xu, Xueyang, Z. Morley Mao, and J. Alex Halderman. "Internet Censorship in China: Where Does the Filtering Go?" In *Lecture Notes in Computer Science*. Springer, 2011.

Zhang, Junsen, and Jia Wu. *The Chinese labor market, 2000–2016*. 2016. (accessed November 16, 2021).

Zhou, Qijia. *Building the (Fire) Wall: Internet Censorship in the United States and China*. December 28, 2020. hir.harvard.edu/building-the-fire-wall/ (accessed December 18, 2021).