# The Geopolitics of Sociotechnical Systems: America's Digital Colonialism and China's Isolated Internet

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science, School of Engineering

**Anthony Tiancheng Sun**

Spring 2022

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

Advisor

Sean M. Ferguson, Department of Engineering and Society

**The Geopolitics of Sociotechnical Systems: America's Digital Colonialism and China's Isolated Internet**

Modern human society has become increasingly reliant on information technologies to function. Many aspects of an average person's life have now moved towards the digital realm. Accessing financial statements and managing international transactions now only requires an internet connection instead of a visit to the bank, while most people's intake of news and social connections happen exclusively on digital websites rather than in-person forums. Like their citizens, the governments of nation-states have also become further reliant on information technologies. Infrastructure like pipeline and transportation apparatuses are controlled through an electronic network, while militaries are beginning to develop autonomous weapons and advanced electronic warfare platforms that are reliant on network connections to function.

While the environment modern countries exist in have changed dramatically, their geopolitical interests have continued to remain constant. Powerful nations still strive to maintain spheres of influence and exert their will on other countries in order to safeguard their interests. With the advent of a digitized society and the rising importance of information technologies around the globe, geopolitical power can now be manifested through control over these technologies. With this in mind, this paper wishes to investigate the ways in which control over information technologies augments a country's geopolitical influence. This paper will do so by examining the ways in which the United States government's dominance over information technology has allowed it to exert influence globally through the use of Michael Kwet's digital colonialism framework. This paper will also study the current state of the Chinese internet and how its isolated nature allows it to retain national control over its digital system. Such an investigation would provide insight into how sociotechnical systems created to benefit the

average citizen can also be used to serve broader geopolitical interests while also contextualizing why certain countries have chosen to develop their digital apparatuses in specific ways.

## The Digital Colonialism Framework

Digital Colonialism is a theoretical framework outlined by Michael Kwet following his observation of the U.S.'s international primacy in digital technologies. Digital colonialism is defined through five features of domination over a foreign country: economic domination, imperial control of architecture, global surveillance capitalism, imperial state surveillance, and a tech hegemony. Using the nation of South Africa as a case study, Kwet posits that the monopoly U.S. multinational corporations possess over the global digital ecosystem is analogous to imperial control and fulfills all five features of domination.

Under digital colonialism, economic domination is said to be brought through foreign corporations that seize the resources of colonized countries by creating technological dependencies through the monopoly of digital technology. Kwet identifies how U.S. multinationals dominate many functions of the digital ecosystem including search engines (Google); desktop operating systems (Microsoft Windows); social networking platforms (Facebook, Twitter); video streaming (Youtube, Netflix); and transportation apps (Uber, Lyft). This dominance comes at the detriment of the local population. Taking Uber as an example, the e-taxi application has begun outcompeting local South African taxis in Johannesburg, and with Uber taking a 25% commission for each trip, the situation has resulted in an outflow of revenue from the local economy into foreign companies (Kwet, 2019, pp 4).

Imperial control of architecture is defined by Kwet as the colonial conquest and ownership of critical infrastructure in the colonized nation. In a digital sense, this critical

infrastructure is identified as the software which runs the technologies used to digitize society. According to Kwet, the U.S. has monopolized this software code through the use of non-free licensing which prevents the software from going open-source and ensures that control over the code is held squarely by the multinational corporations that created it. This control allows these U.S. corporations to usurp sovereignty in foreign countries by preventing the citizens of these countries from making modifications to the software. "In the case of Microsoft Windows, for example, the public must pay for the program in order to use it… [and] they cannot change its behavior by changing the code… By design, non-free software provides the owner power over the user experience. It is authoritarian software" (Kwet, 2019, pp. 6).

In the case of surveillance, Kwet identifies two different types of information dominance created under digital colonialism: global capitalist and imperial state surveillance. Global capitalist surveillance is intelligence gathering for the purpose of furthering an economic agenda. With the development of data science and machine learning, corporations have found value in the collection of user metric and behavior data to power their backend prediction algorithms and inform on market trends and business decisions. Because the most popular social media websites used to collect this user data are owned by U.S. corporations (Facebook, Google), Kwet posits that the U.S. empire has monopolized the collection of this user data, further preventing global south firms from competing with Silicon Valley 'Big N' companies (Kwet, 2019, pp. 9-10)

In contrast, imperial state surveillance is defined by Kwet as the more conventional mass and targeted surveillance programs instituted by the U.S. intelligence community and their allies. He outlines how the dominance of U.S. based technology firms in global south nations has allowed the U.S. National Security Agency (NSA) unprecedented access to foreign populations. Having the tech corporations be U.S. based allows the NSA to easily partner directly with them

in order to access private information from social network platforms, and monitor phone calls and emails using surveillance technology. In comparison, "when the SA [South African] government wants information about a person of interest, it must apply through the Mutual Legal Assistance Treaty to access private information" (Kwet, 2019, pp. 11). This discrepancy in surveillance ability from the U.S. and global south countries like South Africa represents another facet of dominance defined by digital colonialism.

The final aspect of digital colonialism defined by Kwet is the idea of U.S. digital hegemony. Drawing upon all the previous dominations, the U.S. monopoly over the tech sector has created what Kwet calls "a new Manifest Destiny for the digital age" (Kwet, 2019, pp. 14). Since much of the world's information technology innovations are controlled by the U.S., it has allowed them to steer the narrative around how technology should expand, and by proxy define the economic ramifications of such an expansion. Kwet emphasizes how such a view of technological innovation is rooted in authoritarianism and serves as a scathing reminder of how "technology is part and parcel of power relations, and who controls technology matters to both elites and the popular classes" (Kwet, 2019, pp. 15).

## The West's Control over SWIFT

With the widespread adoption of the internet and mobile technologies, global economic activity has now become defined by the speed and wide-reaching connectivity facilitated by these technologies, creating what some term the 'digital economy'. The idea of the digital economy is defined as "…the economic activity that results from billions of everyday online connections among people, businesses, devices, data, and processes. The backbone of the digital economy is hyperconnectivity which means growing interconnectedness of people,

organizations, and machines that results from the internet, mobile technology and the internet of things (IoT)" (Deloitte Malta). The digital economy has resulted in not only an explosion of economic activity, but also a growing globalization of the economy as cross-border telecommunications networks increases the ease of performing international transactions.

One organization which arose to support the higher load of cross-border transactions thanks to the digital economy is the Belgium-based Society for Worldwide Interbank Financial Telecommunication (SWIFT). SWIFT is a cooperative society which provides telecommunication services for various financial institutions across the world, offering a fast and secure means for payment instructions to be transmitted between institutions. SWIFT has become ubiquitous in this field; its networks have been utilized for around 50% of the world's high-value cross-border payments and its messaging formatting has become the industry standard for financial syntax (Scott & Zachariadis, 2013).

Due to the importance of its networks in facilitating international transactions, access to SWIFT can be withheld as a means of pressuring countries against actions contradictory to Western interests. Cutting financial institutions off from SWIFT effectively prevents them from servicing international clients because of SWIFT's ubiquity in the global economy, which paired with the increase in globalization due to the digital economy, results in a marked downturn of revenue. Because of this, the countries that hold more influence over SWIFT's operations, namely the United States and the European Union, are able to wield SWIFT like a club, revoking access to nations that defy their control as a means to enforce their geopolitical dominance.

Evidence of the use of SWIFT as a tool of economic influence can be found in February of 2012, when SWIFT agreed to cut ties to Iranian banks in order to support the wider sanctions

levied by the E.U and U.S. against Iran following their government's attempts to develop nuclear weapons (Blenkinsop & Younglai, 2012). Similarly, on February 26, 2022, the governments of the E.U., United Kingdom, Canada, and the U.S. issued a joint statement condemning Russia's invasion of Ukraine, and announced that they would be removing select Russian banks from the SWIFT messaging system in order to "…hold Russia to account and collectively ensure that this war is a strategic failure" (Commission Spokesperson's Service, 2022).

The West's use of SWIFT as a tool to punitively damage the economies of foreign countries is an example of economic domination within the framework of digital colonialism. SWIFT's ubiquity in providing global financial telecommunications services has formed a de facto monopoly in facilitating transnational digital trade, and thus has created a technological dependency on the SWIFT network within the weaker countries of the world that wish to become a part of the global economy. With SWIFT being based in Belgium alongside their strong track record of supporting Western political goals, to the detriment of non-Western countries, it is safe to say that SWIFT represents an arm of Western digital imperialism.

## U.S. Information Control Through Social Media

The advent of digitized society has allowed for information to spread at breakneck speeds, fundamentally changing the way societies become informed on current events. Information reporting is now no longer monopolized by mainstream media corporations and government broadcasting services and has instead been distributed across the populace. The wide reach of social media websites like Twitter and Youtube have allowed anyone to platform themselves and spread their ideas on a global forum, one that has now become more popular than contemporary media. U.S. owned tech companies Google and Facebook have been reported to

reach more citizens in the U.K. than the state sponsored BBC media corporation (Swabey & Harracá, 2021).

The rise of this global forum with the use of social media platforms like Twitter has made it far easier for countries to disseminate information and misinformation within foreign populations. Social media algorithms are designed to push ideas that get more traction and impressions, while burying less popular ideas as a result (Oremus, 2017). This allows for countries to utilize large amounts of sock puppet accounts and bots to artificially inflate the popularity of conversations they wish to promote, making it easier to push propaganda into the forefront of the global conversation.

The U.S. has been suspected of using social media bots to influence political events abroad. During the 2021 Cuban protests, the hashtag #SOSCuba used to represent the protests was thought to be artificially popularized with U.S. social media bots by both Cuban officials and outside observers. Spanish social media expert Julian Macias Tovar described the unnatural numbers behind the hashtag, stating that "between July 5, when the #SOSCuba hashtag was first used, and the eighth, there were just 5,000 tweets… it then exploded exponentially… with two million on the twelfth" (Abiven, 2021). Around this time many accounts were seen posting a 'copypasta' of the same exact message which read "we Cubans don't want the end of the embargo if that means the regime and dictatorship stays, we want them gone, not more communism" and was thought to be another U.S. bot campaign aimed at manufacturing consent to the U.S.'s long standing policy of economic embargo against Cuba (Ryan, 2021).

U.S. Federal agencies have also been known to monitor social media accounts of international citizens. Agencies such as the Department of Homeland Security (DHS), Federal

Bureau of Investigation (FBI), and the Department of State use American-owned social media platforms for information collection. For foreign individuals, American surveillance of social media is used to screen travelers and monitor terrorist threats. The U.S. government even maintains agreements which allow them to share social media data on visa applicants with repressive foreign governments that may retaliate against critics. Such activities have started a chilling effect where people begin to self-censor as they believe they are being monitored by the U.S. government. According to the Brennan Center, the U.S. State Department and DHS's data collection led to international filmmakers censoring their own political speech on these social media platforms (Levinson-Waldman, 2022).

The U.S.'s control and surveillance over the flow of information on the world's most popular social media platforms constitutes an example of imperial state surveillance as defined by Kwet. The use of American social media platforms as a vector for false narratives and close surveillance of a foreign people serve to push the geopolitical interests of the United States, to the detriment of the foreign nation's sovereignty. Such a naturally hostile and inherently unequal relationship serves to enforce the imperialist power dynamic between the two parties within a digital context.

## China's Isolated Internet – A Case Study

The numerous ways in which control over the technologies powering a digitized society can be used to coerce and exploit weaker nations has led to countries becoming concerned with maintaining their digital sovereignty, the foremost of which is the People's Republic of China. China's government was concerned with the implications of the introduction of internet technology within its borders. It wished to exploit the technology's economic capabilities but did

not wish for the technology to allow for Western ideologies to spread throughout China unchecked. In order to both exploit the economic advantages of internet technology and mitigate its ability to spread divergent ideologies, China's Ministry of Public Security launched the Golden Shield Project in 2000 which tasked itself with content-filtering at the end-user level to allow the government to control the flow of information within their internet (Punyakumpol, 2011). This project eventually led to the current state of the Chinese internet, one which serves as a prime example of a society intentionally cutting themselves off from technologies controlled by adversaries.

Telecommunications services in China are dominated by state-owned companies, namely China Mobile, China Unicom, and China Telecom (Weissberger, 2019). It wasn't until 2019 that a foreign telecommunications company, BT, would be allowed to provide internet services in China (Global Services, 2019), illustrating the importance of domestic control over infrastructure in China's digital ecosystem. In addition to mobile telecommunications, China has its own financial telecommunications system based in Shanghai called the Cross-Border Interbank Payment System (CIPS) which handles international RMB trade and has been used across 103 countries. With its Western equivalent SWIFT having been used to further geopolitical agendas, Chinese security analysts hope to see CIPS used as an alternative to SWIFT, stating that "it is necessary to reduce reliance on Swift to ensure financial security" (Tang, 2022).

In addition to telecommunications services, China's gateways to the global internet are completely controlled by the Chinese government, which gives them the authority to restrict connections to content hosted on foreign servers (Chen, 2020). This has allowed China to ban domestic access to thousands of Western sites, including news sites such as CNN and the BBC, as well as social media platforms such as Facebook and Twitter (French, 2021). Instead of

allowing their citizens to use Western owned websites, Chinese companies have developed alternative platforms instead, giving the Chinese government greater control over their citizenry's social media activities. Sina Weibo is the Chinese counterpart to Twitter, the Baidu search engine is used rather than Google, and Youku Tudou is China's principle video sharing website instead of Youtube (Kong, 2019).

While like the U.S., China enjoys dominant domestic control over its internet, the Chinese internet differs in the sense that it hasn't seemed to be exported across the wider world. Out of 1.2 billion monthly active WeChat users, only 150 million are considered international users (Iqbal, 2022). 97.3% of Baidu users are from China, with the largest international user base being the United States at only 0.8% (Thomala, 2022). The majority of the content on Weibo is in Simplified Chinese, with even prominent international figures like former Australian Prime Minister Kevin Rudd posting in Simplified Chinese on the platform instead of English (Rudd, n.d.), indicating a lack of a strong international presence on the website. Even China's most successful exported social media platform, TikTok, is distributed as a separate platform in China, Douyin, with content on one app being unable to be viewed on the other (Citizen Lab, 2021). In essence, Chinese social media platforms and the Chinese internet in general seem to be for the Chinese only. Due to their lack of international reach, the Chinese internet cannot be considered imperialist under Kwet's definition of digital colonialism since that framework strictly concerns itself with exploitation on a global scale, not a domestic one.

## Discussion

While the advent of digital technologies has done wonders in promoting a globalizing world, it has also opened up new avenues for powerful countries to use to coerce and exploit weaker ones. In the case of the United States, its use of SWIFT as a punitive measure to hamper

foreign economies and its surveillance of social media scaring international political activists into silence represents the old goals of imperialism being accomplished through new technologies. While digital colonialism may not be as overt and immediately effective as more classic methods of imperialism, such as direct military intervention, they still represent attacks on the autonomy of nations with smaller tech sectors.

China's reaction to American digital supremacy at least indicates that digital colonialism is dangerous enough to be perceived as a legitimate threat to a nation's sovereignty. Its decision to cut its own internet from the global network was born out of a desire to preserve their own technological independence. They banned Western sites and filled the void with their own domestically designed counterparts, and they created a firewall which kept foreign users out of their own internet ecosystem. However, in doing so they strayed from the original purpose of digital technology; they used a tool meant to connect people as a way to further isolate themselves.

This situation is indicative of the choice historically exploited nations have when it comes to utilizing information technologies, they must either submit themselves to the wills of those that control the technology, or they must detach themselves from the global system and rely on domestically produced services. Either way, so long as those in control of these technologies continue to pursue exploitative endeavors, the weaker members of the international community will remain unable to fully enjoy the benefits of a digitized society.

## References


Abiven, K. (2021, July 15). *Cuban government blames Twitter for unrest*. Yahoo! News. Retrieved March 16, 2022, from https://news.yahoo.com/cuban-government-blames-twitter-unrest-014155225.html

Blenkinsop, P, & Younglai, R. (2012, February 17). *UPDATE 3-Banking's SWIFT says ready to block Iran transactions.* Reuters. Retrieved March 16, 2022, from https://www.reuters.com/article/iran-sanctions-swift-idUSL5E8DH31020120217

Chen. Q. (2020, June). *Inkstone Explains: How China engineers an alternative internet for its people.* Inknstone News. Retrieved April 26, 2022, from https://www.inkstonenews.com/tech/inkstone-explains-how-china-engineers-alternative-internet-its-people/article/3088426

Citizen Lab. (2021, March 22). *TikTok and Douyin Explained*. Retrieved April 26, 2022, from https://citizenlab.ca/2021/03/tiktok-and-douyin-explained/

Commission Spokesperson's Service. (2022, February 26). *Joint Statement on further restrictive economic measures.* European Commission. Retrieved March 16, 2022, from https://ec.europa.eu/commission/presscorner/detail/en/statement_22_1423

Deloitte Malta. *What is digital economy?* Deloitte. Retrieved March 16, 2022, from https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html

French, D. (2021, November 26). *Which websites and online services are banned in China?* Retrieved April 26, 2022, from https://www.techradar.com/vpn/which-websites-and-online-services-are-banned-in-china

Global Services. (2019, January 24). *First global telco to receive domestic telecoms licences in China*. BT. Retrieved April 26, 2022, from https://www.globalservices.bt.com/en/aboutus/news-press/bt-first-global-telco-to-receive-domestic-telecoms-licences-in-china

Iqbal, M. (2022, January 11). *WeChat Revenue and Usage Statistics (2022).* Business of Apps. Retrieved April 26, 2022, from https://www.businessofapps.com/data/wechat-statistics/#menu-item-32437:~:text=Some%20estimates%20peg%20international%20WeChat%20user%20numbers%20at%20between%20100%20and%20200%20million.

Kong, C. (2019, May 20). *Top 10 Chinese Social Media and Western Equivalents*. New Digital Noise. Retrieved April 26, 2022, from https://newdigitalnoise.com/top-10-chinese-social-media-and-western-equivalents

Kwet, M. (2019, January 14). *Digital colonialism: US empire and the new imperialism in the Global South*. Yale University. Retrieved March 16, 2022, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3232297

Levinson-Waldman, R et al. (2022, January 7). *Social Media Surveillance by the U.S. Government.* Brennan Center. Retrieved April 26, 2022, from https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government

Oremus, W. (2017, March). *Twitter's New Order*. Slate. Retrieved March 16, 2022, from http://www.slate.com/articles/technology/cover_story/2017/03/twitter_s_timeline_algorithm_and_its_effect_on_us_explained.html

Punyakumpol, P. (2011, June). *The Great Firewall of China: Background*. Stanford. Retrieved April 26, 2022, from https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html

Rudd, K. [@陆克文先生]. (n.d.). *Posts* [Weibo Profile]. Retrieved April 26, 2022, from https://weibo.com/u/2726223703

Ryan, C. (2021, July 29). *Cuba is resilient, the US is unrelenting: An analysis of US activities in Cuba and the current protest movement*. Hampton Think. Retrieved March 16, 2022, from https://www.hamptonthink.org/read/cuba-is-resilient-the-us-is-unrelenting-an-analysis-of-us-activities-in-cuba-and-the-current-protest-movement

Scott, S.V., & Zachariadis, M. (2013, October 18). *The Society for Worldwide Interbank Financial Telecommunication (SWIFT)*. Routledge. Retrieved March 16, 2022.

Swabey, P., & Harracá, M. (2021, February 16). *Power of Tech Companies: How Big Tech Draws its Influence*. Tech Monitor. Retrieved March 16, 2022, from https://techmonitor.ai/boardroom/power-of-tech-companies

Tang, F. (2022, February 28). *What is China's Swift equivalent and could it help Beijing reduce reliance on the US dollar?* SCMP. Retrieved April 26, 2022, from https://www.scmp.com/economy/china-economy/article/3168684/what-chinas-swift-equivalent-and-could-it-help-beijing-reduce

Thomala, L.L. (2022, February 17). *Distribution of global visitors to baidu.com as of February 2022, by top country.* Statista. Retrieved April 26, 2022 from https://www.statista.com/statistics/257592/share-of-baidu-users-by-country/

Weissberger, A. (2019, October 7). *China's big 3 mobile operators have 9 Million 5G subscribers in advance of the service; Barron's: China to lead in 5G deployments*. Techblog. Retrieved April 26, 2022, from https://techblog.comsoc.org/2019/10/07/chinas-big-3-mobile-operators-have-9-million-5g-subscribers-in-advance-of-the-service-barrons-china-to-lead-in-5g-deployments/