Cybersoverignty: Redefining Digital Citizenship in the Cyber Era

By: Sophie Laurence
AP Gov
May 20, 2019

Cyber: a combining form meaning "computer," "computer network," or "virtual reality," used in the formation of compound words (cybertalk; cyberart; cyberspace) and, by extension, meaning "expressing visions of the future."

Sovereignty: supreme power especially over a body politic; freedom from external control; autonomy.

A search in dictionary.com yields the following result: "No results found for cybersovereignty." Neither this word nor its variations (cyber-sovereignty, cyber sovereignty) appears in any English language dictionary. Yet, the rise of China as the world's dominant cyber-superpower amplifies the urgent need for international discourse on its meaning and implications. Even as the West is wondering if a change in the global paradigm is underway, China has already dramatically redefined what it means to be a digital citizen in the 21st century.

The working meaning of "cybersovereignty" is the full right and power of a governing body over the internet within its own borders, without any interference from outside entities. In the material world, national borders are physical boundaries protected by border guards, demarcated by country lines on maps, and governed by national laws. There is no equivalent universal system to regulate internet borders. Though utopianists routinely frame the internet as an open and free instrument of democracy, this is an ideological fiction; the reality is that the internet is a commodified entity owned by a privileged few and, in the case of China, state-controlled. Correspondingly, it has become a battleground in the struggle for international economic dominance and domestic political control.

Invoked by China for years, cybersovereignty has provoked growing international unease over the fuller implications of its actions. As the topic was being debated (with no resolution) at the United Nations, China simply moved its Golden Shield project forward (a.k.a. The Great Firewall of China). Coupled with domestic cybersecurity laws and the Cyberspace Administration of China to oversee new regulations, China now restricts international interactions and communications by way of internet censorship, controlled digital access, and surveillance.

China has defined cybersovereignty (網絡主權), its national digital border (數字邊邊界), Golden Shield (金盾), and domestic cyberlaws (網絡法). What implications does this have for digital citizenship (數字公民身份)?

+ + +

Digital: available in electronic form; readable and manipulable by computer.

Citizenship: **1**. the state of being vested with the rights, privileges, and duties of a citizen, **2**. the character of an individual viewed as a member of society.

According to dictionary.com, a digital citizen is "a person who develops the skills and knowledge to effectively use the Internet and other digital technology, especially in order to participate responsibly in social and civic activities." A certain number of ideological

assumptions inform that definition, including the understanding that the internet is free, uncensored, and relatively unfettered by government regulation.

In 2019, these assumptions largely still apply to American netizens. The growing digital divide notwithstanding, virtual reality has become like the weather, where a "cloud" is both of and not-of human making. Most Americans never question what the internet is, how it works, how they connect to it, or what happens with their data, because they've been led to believe they do not have to. There is profit in our passivity. From Apple to Zynga, Americans enjoy citizenship in multiple digital nations, roaming the internet with the technological equivalent of visa waiver arrangements.

This carefree condition stops when Americans try to visit the Chinese internet. Predicated on the primary definition of political citizenship ("the state of being vested with the rights, privileges, and duties of a citizen,") China's version of digital citizenry comes with government-imposed consequences for violating the rules. Second, China restricts foreign cloud providers, blocks cryptocurrencies, and actively censors content online.

> Even as the Chinese internet grows..., speech is controlled, dissent quashed, and any attempts to organize outside the official Communist Party are quickly stamped out. Some are able to bypass the wall using VPNs, but this creates further a further divide between an intellectual class and the population at large.[1]

In much the same way that national borders separate countries, firewalls block digital traffic. The state controls the flow of information, and blocks content it finds objectionable. Having already

---

[1] James Griffiths, *The Great Firewall of China,* 2019 https://press.uchicago.edu/ucp/books/book/distributed/G/bo38180868.html

enacted "the most sophisticated system of digital censorship in the world,"[2] the Chinese government's control of online information is so vast and pervasive that it's quickly reaching the point where its people will be unable to discern the workings of the state, and simply accept the censored version of virtual reality as a given, like the weather.

For many Chinese citizens, however, the real-life implications of a fully state-controlled internet are bleak. The Council on Foreign Relations reports that the Cyberspace Administration of China announced "new regulations limiting online anonymity, censoring photos in WeChat, and limiting WhatsApp."[3] Meanwhile, in the province of Xinjiang,

> Thousands of Uighurs...have disappeared into so-called political education centers, apparently for offenses from using Western social media apps to studying abroad in Muslim countries...it has become a window into the possible dystopian future of surveillance technology, wielded by states like China that have both the capital and the political will to monitor — and repress — minority groups. The situation in Xinjiang could be a harbinger for draconian surveillance measures rolled out in the rest of the country.[4]

This is digital citizenship in China, where technology enables repression as a mode of state control.

+ + +

---

[2] Ibid.

[3] Adam Segal, "Year in Review: Chinese Cyber Sovereignty in Action" *Council on Foreign Relations,* 8 January 2018 https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action

[4] Megha Rajagopalan, "This Is What A 21st-Century Police State Really Looks Like" *Buzzfeed News*, BuzzFeed, 17 October 2017 https://www.buzzfeednews.com/article/meghara/the-police-state-of-the-future-is-already-here#.gq7oaPGvJ

If we are to understand the challenges, we must be able to articulate them. To this end, we must have a working and shared vocabulary of applicable terms. China is rapidly forging ahead, with Russia not far behind. By contrast, Americans haven't even begun to formally define words just to be able to talk about what has already happened--and what is happening *to* them.

"One of China's most insidious exports is its censorship techniques," Griffiths notes, "and its Firewall is an inspiration for aspiring autocrats the world over." If you are a digital citizen in China, you are digitally surveilled and censored by the state. In the U.S., by contrast, it's chiefly corporations collecting your data for their profit. However, these corporations have begun selling your data to the state (i.e. Amazon, IBM, and Oracle bidding on a mysterious Pentagon contract known as JEDI; Peter Thiel's Palantir selling data to law enforcement, and so on.) If you are not among those controlling the internet, you are both product and prisoner, in the manner of the people of Xinjiang. Avoiding the internet merely turns you into an undocumented digital citizen. In countries where electronic currency is replacing cash, the inability to access the internet means more than being cut off from communications: it also means being cut off from the economic system.

In a cyber world where governments spy on other governments (even among allies), trade and business secrets are stolen, and elections are influenced, the case for China's Golden Shield becomes more convincing. At the same time, its drawbacks--on the level of human rights and civil liberties--are manifold and self-evident. If not cybersovereignty, then what are the alternatives? An unregulated, open internet is a naive and unworkable ideal. The reality of globalisation makes transparent technology trade politically messy, as the Huawei Incident is

unfortunately demonstrating. Meanwhile, cybernationality is quickly becoming defined by which firewall you are behind, having little to do with your actual country of citizenship. Americans traveling physically to China, for example, will also be digitally forced to exit Facebook Nation and Google-land. Upon arrival in China, and finding themself blocked from American interface and internet, travelers must use Chinese equivalents such as Baidu and WeChat. Travelers know they must abide by the laws of the land, observing Chinese traffic and drug laws, for example. But what about cyber laws? As soon as they go online in Chinese cyberspace, is their personal and business data subject to Chinese jurisdiction?

International cyberlaw for digital citizens is desperately needed, including in the areas of cybersecurity, cyberimmigration, and cyberhuman rights. In the meantime, everyone with (democratically) free internet must take action to protect online access in the name of human rights, including the right to privacy. On May 14, 2019, San Francisco became the first U.S. city to ban the use of video surveillance, arguing that "we can have security without being a security state. We can have good policing without being a police state."[5] Decoupling state from corporate power, the mayor's position also illustrates the impact of cybersovereignty on ordinary human lives. As the Cyber Era unfolds, we must each take an ever more active role as digital citizens in articulating, legislating, and protecting digital freedom.

---

[5] Trisha Thadani, "San Francisco Bans City Use of Facial Recognition Surveillance Technology." *San Francisco Chronicle*, 14 May 2019 https://www.sfchronicle.com/politics/article/San-Francisco-bans-city-use-of-facial-recognition-13845370.php

BIBLIOGRAPHY

Griffiths, James. (2019). *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. Chicago, IL: University of Chicago Press. https://press.uchicago.edu/ucp/books/book/distributed/G/bo38180868.html

Rajagopalan, Megha. "This Is What A 21st-Century Police State Really Looks Like." *Buzzfeed News*, BuzzFeed, 17 October 2017. https://www.buzzfeednews.com/article/meghara/the-police-state-of-the-future-is-already-here#.gq7oaPGvJ

Segal, Adam. "Year in Review: Chinese Cyber Sovereignty in Action." *Council on Foreign Relations,* 8 January 2018. https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action

Thadani, Trisha. "San Francisco Bans City Use of Facial Recognition Surveillance Technology." *San Francisco Chronicle*, 14 May 2019. https://www.sfchronicle.com/politics/article/San-Francisco-bans-city-use-of-facial-recognition-13845370.php

Adee, Sally. "The Global Internet is Disintegrating. What Comes Next?" *BBC Future Now,* 15 May 2019.

http://www.bbc.com/future/story/20190514-the-global-internet-is-disintegrating-what-comes-next?utm_source=pocket-newtab

Baron, Jessica. "Cyber-Sovereignty and China's Great Firewall: An Interview With James Griffiths." *Forbes* 8 April 2019. https://www.forbes.com/sites/jessicabaron/2019/04/08/cyber-sovereignty-and-chinas-great-firewall-an-interview-with-james-griffiths/#8fcab44747bc

"Cyber sovereignty." *Wikipedia.* 18 January 2019. Web. Accessed 6 May 2019. en.wikipedia.org/wiki/Cyber_sovereignty

"Global Surveillance Disclosures." *Wikipedia.* 22 April 2019. Accessed May 2019. en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)

Griffiths, James. (2019). *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. Chicago, IL: University of Chicago Press. https://press.uchicago.edu/ucp/books/book/distributed/G/bo38180868.html

Jensen, Eric Talbot. "Cyber Sovereignty: The Way Ahead." 50 Tex. Int'l L. J. 275 (2014).

Kuo, Kaiser. "What Makes China's Tech Tick?" 12th Annual Camden Conference. Camden, ME. 22-24 Feb. 2019. https://www.camdenconference.org/2019-camden-conference/

Leigh, Karen, Stepan Kravchenko, and Saritha Rai. "How 'Cybersovereignty' Splits the Once World Wide Web." *Bloomberg Businessweek*, Bloomberg, 9 May 2019. https://www.bloomberg.com/news/articles/2019-05-02/how-cybersovereignty-splits-the-once-world-wide-web-quicktake.

Morozov, Evgeny. "Reasserting cyber sovereignty: how states are taking back control." *The Guardian*, 7 October 2018. https://www.theguardian.com/technology/2018/oct/07/states-take-back-cyber-control-technological-sovereignty

Mossberger, Karen, Caroline J. Tolbert, and Ramona S. McNeal. (2007). *Digital Citizenship: The Internet, Society, and Participation.* Cambridge, MA: The MIT Press. https://mitpress.mit.edu/books/digital-citizenship

Rajagopalan, Megha, "This Is What A 21st-Century Police State Really Looks Like." *Buzzfeed News*, BuzzFeed, 17 October 2017. https://www.buzzfeednews.com/article/meghara/the-police-state-of-the-future-is-already-here#.gq7oaPGvJ

Segal, Adam. "Year in Review: Chinese Cyber Sovereignty in Action." *Council on Foreign Relations,* 8 January 2018. https://www.cfr.org/blog/year-review-chinese-cyber-sovereignty-action

Thadani, Trisha. "San Francisco bans city use of facial recognition surveillance technology." *San Francisco Chronicle*, Hearst Newspapers. 14 May 2019, https://www.sfchronicle.com/politics/article/San-Francisco-bans-city-use-of-facial-recognition-13845370.php

Walker, James. "China reasserts right to 'cyber sovereignty'." *Digital Journal,* 4 December 2017. http://www.digitaljournal.com/tech-and-science/technology/china-reasserts-right-to-cyber-sovereignty/article/509135

World Economic Forum, “Digital Borders: Enabling a Secure, Seamless and Personalized Journey.” *World Economic Forum White Paper*. World Economic Forum, 17 February 2017. https://www.weforum.org/whitepapers/digital-borders-enabling-a-secure-seamless-and-personalized-journey