A RISING "CYBER CHINA"

As Xi Jinping prepares to secure an unprecedented third term as party leader, observers will find that the PRC has become increasingly assertive in its regulation of the internet and its infrastructure. The techniques honed in the treatment of China's domestic cybersphere are increasing in presence in international cyberspace, as domestic propaganda effectively suppresses dissenting voices and nurtures cyber nationalism. The CPC's promotion of "cyber sovereignty" and "self-reliance" in technological innovation and manufacturing further demonstrate a concerted effort to carve out a "Chinese cyberspace" different from the current free and open model. Understanding both domestic and international aspects of China's internet is the key to addressing a more proactive and confident "Cyber China."

Jonathan Sullivan[*], Sarah Jeu[**]
& Weixiang Wang[***]

TPQ
Fall 2021

[*] Dr Jonathan Sullivan is director of China programmes at the University of Nottingham Asia Research Institute.
[**] Sarah Jeu is a PhD student in the School of Politics and IR at the University of Nottingham.
[***] Weixiang Wang is a PhD student in the School of Politics and IR at the University of Nottingham

While western democracies belatedly confront the havoc that social media have wrought on the cohesion of their societies, the Chinese Party-state has again demonstrated its mastery of the digital information environment. The regime's ever-evolving toolkit is full of sophisticated precision instruments, but sometimes a sledgehammer will suffice. That was the case this month when Peng Shuai, a Grand Slam tennis champion and one of China's most celebrated athletes, used her account on Chinese social media Weibo to level serious allegations of sexual assault against one of China's most powerful politicians, former Vice Premier Zhang Gaoli. The post was taken down within the hour, but in that time it circulated widely. In a political culture where the elite political leadership is protected from public comment, this was the kind of explosive intervention that, in colloquial western parlance, could be expected to 'break the internet.' It might also have reinvigorated China's embattled #MeToo movement. But this is Chinese social media in 2021, not 2011, when Weibo routinely broke government scandals and mobilized so many angry netizens it had the potential to spill over into physical world contention.[1] All references to Peng's post, even oblique ones (and the word 'tennis'), were blocked and rendered unsearchable. Peng's account remains up but immobilized, and she has effectively been scrubbed from the Chinese internet. The political elite and Chinese media responded with deafening silence. Peng herself disappeared from sight, sparking an international campaign led by Naomi Osaka, Serena Williams and the WTA to establish her whereabouts and wellbeing. Emerging just before the Sixth Plenum, a highly consequential meeting of Communist Party elites that paved the way for Xi Jinping to continue his leadership into a third term next year, Peng's revelation was quickly consigned to the Chinese internet's blackhole. The meeting progressed without a hitch, as China's e-commerce giants celebrated the world's most lucrative retail event, Single's Day. And when the Plenum's "historical resolution" was publicly released, the machinery of a vast outward-facing propaganda apparatus incorporating Chinese state organs, media outlets, 'wolf warriors,' paid commentators, cybernationalists and bots, flooded the free cyberspaces outside of China with positive commentary and pushback against criticism. This weeklong snapshot hints at the extent to which the Chinese Party-state exerts domination over the domestic information environment, while harnessing the affordances of the internet economy and exploiting the openness of the 'free internet' for propaganda purposes. Nevertheless, this is neither the extent nor the endpoint for the Party-state's ambitions for establishing hegemony over digital spaces, both domestic and international.

Taming Dissent in Domestic Cyberspace

The Party-state has always perceived potential for the internet to facilitate economic

[1] Yongshun Cai, *Collective Resistance in China* (Stanford University Press, 2010); Jonathan Sullivan, "China's Weibo: is Faster Different?" *New Media & Society*, Vol. 16, No. 1 (2014), p. 24-37.

"Dominance of cyberspace begins with the underlying technologies and physical in frastructure, which the state controls. It has the capacity to cut off internet access entirely (as it did following ethnic conflict in Xinjiang in 2009 and protests in Inner Mongolia in 2011)."

development and tentatively welcomed the benefits of wider and accelerated information flows. In the early days, it also attached feelings of 'aspirational modernity' to the development of the internet, the pursuit of which continues to be a national preoccupation. But the Party-state has never been willing to concede ideological hegemony over online spaces, nor countenance threats to regime or social stability emanating from digital mobilizations. Through the evolution of internet technologies and cultures, it has sought to strike a balance between allowing and controlling information flows. In a polity without meaningful elections, online public opinion is a useful informational input in a system of evolving deliberative or consultative authoritarianism.[2] However, the freewheeling nature of social media was a threat, and since 2012, these platforms have been progressively neutered. Implementation of legal and technological frameworks, combined with increasingly pervasive surveillance and increasingly precise censorship[3], have transformed the Chinese internet into a safer space for the regime. Public discussions, including expressions of discontent and criticism, have moved to the quasi-private spaces of the now hegemonic Weixin (known as WeChat outside China). Liberal and critical opinion leaders have been silenced, some arrested, others merely cowed. The small number of big internet platforms has been thoroughly co-opted, forming a symbiotic relationship with the regime. Online spaces have been colonized by Party-state organs and pro-regime and nationalist voices have been emboldened. The diversity of opinion and volume of dissent that were once a sign of the vitality of online public opinion are pale imitations of their former selves.

A crucial difference between the approach to online public opinion now and in previous periods, is that instead of vacillating between mobilization (of pro-regime voices) and control (of critical or alternative ones), both are implemented simultaneously. Whereas degrees of freedom used to wax and wane, the trajectory under Xi has become monotonic. Online public opinion has been contained and corralled

[2] Steve Tsang, "Consultative Leninism: China's new Political Framework," *Journal of Contemporary China*, Vol. 18, No. 62 (2009), p. 865-880.

[3] Rogier Creemers, "Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century," *Journal of Contemporary China*, Vol. 26, No. 103 (2017), p.85-100.

in the service of producing, reproducing and even coproducing pro-regime propaganda and nationalistic sentiment.[4] The ideal scenario is a majority of PRC netizens who subscribe to official discursive cues voluntarily, and disseminate and amplify such messaging. Predominant pro-regime actors would then exert their own form of "cancel culture" on dissenting or unorthodox voices, by turn inducing pervasive self-censorship. Chinese cyberspace would then enter a "post-censorship phase," where blunt force measures are no longer necessary. To reach such a state does not happen by accident. It has taken long years of experimentation and capacity building, and is founded on a dense techno-legal governance architecture.

Dominance of cyberspace begins with the underlying technologies and physical infrastructure, which the state controls. It has the capacity to cut off internet access entirely (as it did following ethnic conflict in Xinjiang in 2009 and protests in Inner Mongolia in 2011). And the power to grant access to the free internet to whom it deserves worthy (the campuses of foreign universities, for instance). It is followed in influence by the complex web of overlapping and nested institutions and techno-legal frameworks that incorporate adjacent sectors of economy, technology, ideology, propaganda, creative and cultural industries, media, national and international security. The well-known Cyberspace Administration of China is certainly a powerful organ, but it is just one part of the governance system. The next foundation is the pervasive system of digital surveillance and censorship mechanisms. Although major digital platforms are nominally run by private companies, they have no option but to serve the Party-state's interests. When a law was passed making platforms liable for user generated content on their sites, they had to comply, adding a further level of information control. Next, Chinese social media have been flooded with Party, state and other official accounts.[5] From the smallest police department to national organizations like the Communist Youth League, tens of thousands of official organs contribute floods of "positive energy" and political correctness (in the Chinese sense) to the digital information environment. Media organizations like the Communist Party's *People's Daily* and nationalist tabloid *Global Times* have tailored their digital offerings to the preferences of contemporary netizens, generating enormous audiences and dominant positions at the centre of the social media ecosystem. Next come the pro-regime opinion leaders in journalism, academia and even the co-opted celebrities of the entertainment industry, many of whom have social media audiences in the tens of millions. In sum, the regime has established dominion over the "public opinion high ground." Yet it is the way that the discourse is reproduced at the lowest level of discussion boards and social media comment

[4] Rongbin Han, "Defending the Authoritarian Regime Online: China's 'Voluntary Fifty-Cent Army'," *The China Quarterly*, Vol. 224 (2015), p. 1006-1025.

[5] Shaohua Guo, "'Occupying' the Internet: State Media and the Reinvention of Official Culture Online," *Communication and the Public*, Vol. 3, No. 1 (2018), p. 19-33.

sections that is so remarkable. The cowing and silencing of diverse opinions created a vacuum that has been occupied by domineering cybernationalists and pro-regime proponents. Dissenting voices still exist in Chinese cyberspace, and necessity being the mother of creation, negotiating constrained conditions has forced them to adopt oblique and ingenious modes of expression.

> *"The PRC is pushing an alternative internet governance framework that opposes the free and open model supported by the U.S. and other liberal democracies."*

Increasingly, China is not content to limit its ambition to the domestic cyberspaces as it begins to manifest its ideological understanding of the internet and the techniques it has honed at home in the international arena. We look now at two aspects: externally facing digital propaganda and the concept of internet sovereignty as well as the technological aspects associated with it.

Fighting for International Discourse

Accompanying the robust foreign policy posture encouraged by Xi Jinping[6] is a sharpening of China's outward-facing information and propaganda activities, including various manifestations of cyber competition and cyberwarfare. In the discursive arena, it embodies the new "assertiveness" of China's "confident rise," following the dictates of 'telling Chinese stories well" and "daring to fight." These orientations reflect a paradigm shift in the guiding principle of PRC diplomacy, from the Dengist "Hide and bide" to Xi's "Great Power diplomacy". In China's quest for "major power status," building up this "discursive power" is intended to complement hard power.

If the internet at-large is a discursive field where different actors struggle to advance competing claims, it has unsurprisingly become a significant battlefield for the PRC, especially when it comes to vaguely defined and ever-expanding "core interests." Over time the PRC has become increasingly sophisticated in its foreign propaganda, leveraging the freedom of expression on western social media platforms. The most easily distinguished manifestation of this is the "wolf-warrior" giving loud and acerbic voice to pro-Chinese perspectives within these venues.[7] Alongside them is a

[6] Peter Martin, *China's Civilian Army: The Making of Wolf Warrior Diplomacy* (Oxford: Oxford University Press, 2021).

[7] Yaoyao Dai and Luwei Luqiu, *China's Wolf Warrior Diplomacy and Xi Jinping's Grand Diplomatic Strategy*, Working Paper (2021). https://www.researchgate.net/publication/350677590

dense network of state organs, bots and paid and organic cybernationalists flooding cyberspaces with mis- and disinformation.[8] Although Chinese internet users are, in theory, barred from accessing foreign sites, the Great Fire Wall (GFW) is more porous than its name suggests, and the routine and "expeditionary" presence of pro-PRC netizens in western social media is commonplace. Voluntary, fragmented or coalescing in substantial groups, PRC users compete for "narrative control" on free internet sites from Wikipedia to Twitter and YouTube, and are hyper-alert and ready to mobilize against any entity judged to have "insulted China" or "interfered in China's internal affairs."

State actors have noticed and helped to promote such grassroots nationalism. Zhao Lijian, arguably the most famous "wolf warrior" known in the West, reposted works from Chinese netizens on Twitter and triggered an angry reaction from countries including Australia and Japan. Though condemned as disinformation and undiplomatic abroad, Zhao's moves have been widely celebrated at home as a success for the PRC's "fight for international discourse". There are numerous "grassroots" key opinion leaders like them tirelessly producing pro-regime messages in the PRC's cybersphere. And thanks to their efforts, propaganda in the PRC has taken on a new face, permeating into the popular culture and "reinventing" official discourses. The unofficial "collaborations" between Zhao Lijian and Fu Yu, a regular netizen producing nationalist digital artworks, are a signal manifestation of what Repnikova and Fang[9] describe as "authoritarian participatory persuasion 2.0." In addition, for commercialized media and internet operations, required to maximize profits while staying within the bounds of politically permissible parameters, nationalist content is both safe and profitable: In effect, it is a media ecology built for promoting nationalism.[10] However, media are only part of the story. Party and state actors have also leveraged technological affordances on a massive scale to shape and engage publics with new forms of messaging that complement and reaffirm the messaging that dominates the broader information environment. The Communist Youth League and various state and Party affiliated media are at the vanguard of nurturing participatory, interactive and collaborative digital operations, producing content that is consonant with digital cultural practices and resonates with digital native publics.

The PRC's assertiveness in the international cybersphere should not be considered separately from the intensifying propaganda drives at home. Many of the techniques

[8] Gary King, Jennifer Pan and Margaret Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review*, Vol. 111, No. 3 (2017), p. 484-501; Margaret Roberts, *Censored: Distraction and Diversion inside China's Great Firewall* (Princeton: Princeton University Press, 2018); Marcel Schliebs, Hannah Bailey, Jonathan Bright and Philip N. Howard, *China's Public Diplomacy Operations: Understanding Engagement and Inauthentic Amplifications of PRC Diplomats on Facebook and Twitter*, Dem Tech Working Paper.

[9] Maria Repnikova and Kecheng Fang, "Authoritarian Participatory Persuasion 2.0: Netizens as thought work collaborators in China," *Journal of Contemporary China*, Vol. 27, No. 113 (2018), p. 763-779.

[10] Florian Schneider, *China's Digital Nationalism* (Oxford: Oxford University Press, 2018).

it adopts in conducting foreign propaganda have been honed in the treatment of the domestic, and connections should be made between the two dynamics. There exists a "flow-back" and reproduction of its external assertiveness within the PRC's domestic cybersphere, which further breeds and encourages the grassroots nationalistic voices and suppresses those *dissenting views.*

Redefining the Internet

The PRC is pushing an alternative internet governance framework that opposes the free and open model supported by the U.S. and other liberal democracies. The concept of *cyber sovereignty* has widespread implications, as it relates to everything from domestic internet content in China to data localization regulations for foreign firms. Amid trade sanctions from the U.S. and a global semiconductor shortage, the Chinese state is investing heavily in domestic manufacturing and innovation for critical internet technologies. This move demonstrates the PRC's increasing focus on cultivating technological self-sufficiency and shaping future internet-related development through technology standards. the PRC views standards as a critical area of competitive advantage that could diminish some of the U.S.'s longstanding influence over key internet technologies. Other areas of focus include Artificial Intelligence, Big Data, cloud and quantum computing.

Introduced in the 2010 white paper 'The Internet in China,' the concept of 'internet sovereignty' has been a pivotal aspect of China's cyber governance strategy since the late 1990s.[11] While the central government has long focused on honing censorship techniques to manage domestic internet content, it has recently developed more comprehensive regulations for managing data and critical technology innovation and manufacturing. For the CCP, ensuring a sovereign Chinese internet is about maintaining material and ideational power, achieving development objectives, and preventing reliance on and intrusion from 'hostile foreign forces.' As a result, the Chinese government's broadened goals for achieving internet sovereignty have both domestic and international implications. Domestically, the tech sector in China has felt a significant shift in its operating abilities and relationship with the central government, which previously were relatively unrestricted and mutually beneficial. While China has long promoted cyber sovereignty in international fora like ICANN and the UN, rising global issues surrounding Big Tech, data security, and the spread of disinformation have renewed concerns among the U.S. and its allies about the appeal of a bounded cyberspace.

In 2017, the PRC implemented its Cybersecurity Law, which set out a broad legal framework for ensuring the security and sovereignty of Chinese cyberspace. Since

[11] Rogier Creemers, *China's approach to cyber sovereignty* (Berlin: Konrad-Adenauer-Stiftung, 2020).

then, newly published laws and regulations have helped clarify many of the undefined aspects of the basic law and have highlighted areas of importance for the Chinese government. Implemented in September and November of this year, the Data Security (DSL) and Personal Information Protection (PIPL) laws, respectively, have sweeping implications for how companies store, secure, process, and use the data of Chinese nationals, even when a company fully operates outside of the PRC. Pragmatically speaking, these laws reflect China's response to experiencing its own data leaks and cyberattacks, which are a natural cost of being a highly wired state. However, they can also be understood as China's answer to the E.U.'s General Data Protection Regulation and the U.S.'s CLOUD Act.[12] As the U.S. and its allies have targeted Chinese tech giants like Huawei as cybersecurity threats, the PIPL and DSL allow China to level similar arguments against those accusing it of malpractice.

This increased focus on data security goes hand in hand with China's recent crackdown on Big Tech, as the CCP attempts to level competition within the tech sector and reduce the monopoly of tech powerhouses like Alibaba and Tencent. As these companies experience an increase in regulatory oversight, they have also been pushed to embrace objectives that align with state development goals. While pursuing technological 'self-reliance' has been an ongoing process for the past few years, the concept was again highlighted in the central government's 14th Five-Year Plan, which was released earlier this year. This objective concerns China's reliance on foreign firms for imports and 'core technologies' like semiconductors, which are the brainpower behind everything from AI and quantum computing to self-driving cars and smartphones. The semiconductor industry experienced a massive shortage throughout the coronavirus pandemic, a situation that was exacerbated in China by U.S. sanctions on Chinese companies like Huawei and ZTE. To help China decrease its reliance on foreign-made semiconductors, China's largest chip manufacturer Semiconductor Manufacturing International Corporation (SMIC) plans to build new facilities in Beijing, Shanghai, and Shenzhen. On the design side, Alibaba, Baidu, and Tencent have also recently turned to semiconductors as a strategy to support state objectives and reassure investors after the tech crackdown.

The push for self-reliance also concerns strengthening China's leadership role in strategic technological areas. In 2020, the Chinese government published its China Standards 2035 plan, which encourages the indigenous creation of global standards in key areas like AI and 5G. While technical standards are not legally binding rules, their implication for global interoperability means that their normative power is substantial. As the West, and primarily the U.S., has long dominated in the standards arena, the Chinese government sees setting future standards as an opportunity

[12] Matt Haldane, "What China's New Data Laws are and their impact on Big Tech," *South China Morning Post*, 1 September 2021, https://www.scmp.com/tech/policy/article/3147040/what-chinas-new-data-laws-are-and-their-impact-big-tech

to increase its own influence and chip away at this hegemony, while also boosting technological competitiveness and securing its own systems against interference. Standards are also economically beneficial, as licensing fees generate significant revenue. China has long had to pay these fees to Western firms, and thus seeks to reverse these roles in emerging areas. Moreover, the Chinese government also plans to utilize its Belt and Road Initiative to export its technical standards across borders. As China aims to offer developing countries technologies using standards with lower licensing costs than Western counterparts do, it has the potential to wear away the dominance of interoperable systems like Microsoft and Apple.

The Authoritarian Internet

When Bill Clinton famously compared China's efforts to suppress free online discussion as "trying to nail Jell-O to the wall," he underestimated the CPC's determination to adopt an internet that both facilitates China's development and preserves the Party's governing power. With such an authoritarian model in place coupled with pervasive online nationalism, it is unlikely that the CPC's hegemonic status within its domestic cybersphere will easily be challenged by external forces. In addressing foreign propaganda, social media platforms should be clear about how they want to sign-post state-affiliated actors, block fake and bot accounts, and flag controversial content. This is, of course, part of a global conversation surrounding the influence of dis- and misinformation on these platforms. When it comes to internet sovereignty, key technologies, and technology standards, states will find that China is not the only one strongly considering the advantages of more consolidated control over future developments. That being said, states need not worry about China becoming completely self-sufficient in the short-term, as it still lacks some of the core technologies needed to make this goal a reality.

Other major cyber powers such as the U.S., UK and EU, need to form a clear and coordinated strategy for addressing "Cyber China." States should be cautious in areas related to national security or with high sensitivity, but welcome cooperation when it is related to low-risk and low-sensitivity areas. A rising "Cyber China" should be of the world's legitimate concern, but neither wishful thinking, excessive worrying nor unconditional rejection will work. Critical engagements built on deeper understanding is much needed.