PACNET

CYBERSECURITY: THE CHINA PROBLEM

BY ROBERT POTTER

Robert Potter (robert@withyouwithme.com.au) is a Pacific Forum young leader, cyber security fellow at the Centre for Rule-Making Strategies in Tokyo, the general manager of WYWM Cyber, and a PhD candidate at the University of Queensland.

As China rolls out its 2016 cyber security law, its drive to develop national cyberspace sovereignty continues. China's law outlines a rules-based view of privacy and emphasizes critical infrastructure and domestic collection of citizen data. With the second largest economy in the world and the largest number of internet users, China has a tough task attempting to establish a national framework for cyber security while fostering an innovative technology sector. China is now a rule maker in cyberspace and home to a number of very large and highly capable technology companies. However, China's lofty goals in cyberspace and innovation are undercut by its behavior in other countries.

The difference in views between the United States and China on cyber security are both broad and deep, often diverging at the ideological level. For the US and other like-minded countries, the internet should be an open, secure platform. China seeks to control narratives that relate to itself. While the US and China have signed agreements on cyber security, their normative preferences diverge sharply. Beijing continues to define cyber security through a lens of national sovereignty and in a manner that is at odds with the notion of an open and accessible internet.

China's efforts to define its cyber security in terms of cyber sovereignty has provoked a significant response from countries like the United States and Australia. The latter, in particular, has made its position clear through the Australian International Cyber Engagement Strategy. China's official position is that "Cyber-sovereignty dictates that no surveillance or hacking against any sovereign nation should be tolerated in cyberspace." Two trends are undermining China's efforts to push forward its normative preferences and both relate to how it behaves in other states.

First, China's cyber security preferences are impacted by its own National Intelligence Laws. These national laws require that: "All organizations and citizens shall, in accordance with the law, support, cooperate with, and collaborate in national intelligence work, and guard the secrecy of national intelligence work they are aware of. The state will protect individuals and organizations that support, cooperate with, and collaborate in national intelligence work."

All Chinese companies must comply with the national intelligence laws. Companies operating within China operate in alignment with both national intelligence laws and the cyber security laws (which require domestic storage of data), which enables the projection of power into other states.

While espionage and intelligence activities have been seen as traditionally outside arguments relating to sovereignty, China's definition of cyber security also relates to normative preferences about narrative. This creates a problem for other states. On the one hand, respecting China as a sovereign internet environment entails accepting censorship of platforms. While states might describe platforms such as Weibo and WeChat as being 'Chinese' they are not used that way. Rather, they are Chinese language platforms and are increasingly popular outside China. Censorship and surveillance of those platforms are not geographically limited to the borders of China. From the perspective of international norms, a China-based platform emerging outside the borders of China renders discussion of a sovereign internet difficult to reconcile. The reality is that China's ambitions are more directly correlated to controlled networks, companies, and platforms than to its own borders.

When platform security moves past the application layer and into critical infrastructure, the potential level of vulnerability increases. Under its National

Intelligence Law, China expects companies to ensure that their critical infrastructure products comport with its national law, regardless of where they are used. For states other than China, technology companies like Huawei and ZTE deploy technologies that are vital to daily business but often housed beyond user control.

The second trend that undermines discussion of a sovereign internet relates to the reality of information operations beyond China's borders. Censorship engines such as Weibo or WeChat work to censor regardless of border. This, in turn, allows China's influence operations to further its 'sharp power' abroad. Just as it curbs criticism of the Communist Party internally, China's has also made efforts to influence each of the "five eyes" (UK, France, US, Australia, New Zealand) countries.

The platforms being developed by China are often full spectrum communications environments covering services from messaging to micropayments. They are very powerful within China to further state control and project state force. Combined with traditional media operations directed by the UFWD, China has constructed a powerful mechanism to enable its sharp power.

These two trends have undermined two aspects of China's policy. First, by expanding efforts beyond the borders of China, the norm of internet sovereignty that Beijing has endeavored to build is likely to erode. Second, Huawei, ZTE, Tencent, and other technology behemoths face strong headwinds as they expand into other countries. ZTE, in particular, is facing a potential shutdown and Huawei is being blocked from major infrastructure projects. The core business of many Chinese technology companies requires strong integration with global partners, leaving them with highly volatile supply chains. This places these very large companies in a highly vulnerable position. China's efforts to enable and cultivate surveillance and influence operations abroad could have a major impact on the ability of those companies to deploy innovative products on a global scale.

China is therefore stuck within a competing set of priorities. Other countries have an interest in accessing Chinese technology. Huawei, for example, is significantly more affordable than many alternatives. Weibo is larger than Twitter and WeChat is one of the most innovative payment platforms developed. Decision makers wanting to engage with this highly innovative technology sector face strong disincentives to do so if using Huawei's technology means deploying an authoritarian state's surveillance technology at the same time.

This challenge can be countered by reasonable policy decisions. First, states need to outline investment screening tools in an approachable and forthright manner. Some of these tools should make reference to cyber security and the need to protect critical infrastructure and democratic institutions. As this policy is developed, we must maintain the international norm of an open internet while holding China accountable to its own narrative (particularly concerning intellectual property and respect for sovereignty). Implemented correctly, a policy aimed at resisting influence operations through investment screening and management can impose direct and material costs.

A second policy response should focus on ensuring that consumers of technology understand the privacy implications of their use. Building awareness of the impacts of influence operations should aim at developing a common understanding of cyber security at the point where technology is engaged with by the general public. For a country like Estonia, influence operations are a fact of life and the government there has endeavored to inoculate civilians through awareness. But, conversations about influence operations should not degenerate into a campaign targeting Chinese citizens.

China's goal of developing a synergy between its technology sector and the party-state apparatus involves significant tradeoffs. Efforts to preserve and cultivate a sovereign cyber security apparatus within China, which enables the party's surveillance ambitions, has saddled technology companies with baggage that companies operating within liberal democracies do not have. Efforts by China to leverage this capacity into the projection of sharp power abroad is directly impacting the ability of those companies to operate as 'normal' participants in the global economy. States seeking to leverage Chinese technology need to implement a realistic risk-oriented approach to assess their level of comfort with Beijing ambitions. This is likely to result both in increased awareness and scrutiny of Beijing's activities as well as increasing resistance to open market access to Chinese technology companies.

PacNet *commentaries and responses represent the views of the respective authors. Alternative viewpoints are always welcomed and encouraged. Click here to request a* PacNet *subscription.*