China is reshaping the technologies, governance, and international understanding of cyberspace. In part this is an almost unavoidable result of demographics and market size. But it is also the outcome of Chinese domestic and foreign policies motivated by two tightly linked ideas: a conception of the Internet as a “double edged sword” and the drive for “information sovereignty,” the idea that cyberspace has been and always should be under national sovereignty.

The future of the Internet is in the developing world and in Asia in particular. At present, the Asian region comprises 42 percent of the world’s Internet population (most by region), but ranks only sixth in penetration rates (21.4 percent). In China, there were approximately 618 million users in 2013, with approximately another 700 million to come online. In addition, these users are young; 56 percent of Chinese users are under the age of 30, and their views on privacy, security, and the appropriate uses of cyberspace can be expected to diverge from those of their counterparts in the United States and Western Europe.

China is also actively shaping the software and hardware that undergird cyberspace. This is happening commercially as Chinese companies leave the safety of the domestic market and expand abroad. Huawei and ZTE have a strong presence in Europe and emerging markets, and the smartphone messaging application Weixin has tens of millions of users in Southeast Asia. This influence is also felt through Chinese participation in technical standards setting bodies such as the International Organization for Standardization and the growing research output of Chinese scientists and engineers.

From the moment Chinese users first went online, policy makers and analysts conceived of the Internet as a double-edged sword, essential to economic growth and good governance, but also the source of threats to domestic stability and regime legitimacy. Economic development has been the priority; the first Internet White Paper described the Internet's “irreplaceable role in accelerating the development of the national economy.” Authorities have also stressed the importance of the web’s role in “supervision”, the exposure on the Internet of official corruption and malfeasance by Chinese users, and in “public opinion guidance” through the orderly spread of information.
While the White Paper declares Chinese citizens enjoy full freedom of speech on the Internet, it states that the exercise of those rights must not “jeopardize state security, the public interest or the legitimate rights and interests of other people.” To prevent these threats, the CCP has built an Internet management system that has an external and domestic face. Offending material from outside of China is filtered and blocked by a number of technologies colloquially known as the Great Firewall. News articles on the wealth amassed by the families of Wen Jiabao and Xi Jinping, for example, have resulted in the blocking of the New York Times and Bloomberg websites.

Within China, black lists block certain phrases or words; in extreme cases, whole regions can be removed from the Internet as happened for ten months after riots in Xinjiang in 2009. Real name registration makes anonymity for most users difficult, and intermediary liability requires Chinese companies to employ huge departments of employees to monitor and censor their customers. A recent study by Gary King suggests that it is not simply online criticism of the CCP or government authorities that results in censorship, but rather calls for physical mobilization and collective action. In May 2013, the State Internet Information Office announced a campaign against “online rumors”, and Big Vs, influential users of the microblogging website Weibo, were warned that they faced up to three years of jail time if “defamatory” comments were forwarded more than 500 times or viewed more than 5000 times. These technical, legal, political, and psychological measures create uncertainty about where the red line is and as a result many users are inclined to self censor.

Domestic stability concerns are at the forefront of Chinese discussions of network security. While U.S. policy makers and analysts use the term cybersecurity, which refers to the defense of routers, computers, networks, and the integrity of data, their Chinese counterparts prefer information security, which includes content and the flow of information. Chinese officials do not ignore the vulnerability of domestic networks, arguing that in fact China is the “world’s biggest victim” of cyber attacks, with the majority of attacks conducted via Internet Protocol (IP) addresses in Japan, the United States and South Korea. The International Code of Conduct for Information Security, submitted to the UN by China and Russia along with Tajikistan and Uzbekistan, is, however, expansive, allowing countries room to interpret the spread of rumors, gossip, and other malicious information through the use of communication technologies as a security threat.

Chinese officials frame network security as a global problem that requires international cooperation, but while the United States, United Kingdom and other liberal democracies prefer a multistakeholder model of Internet governance, China supports a more state-centric approach anchored in the United Nations and the International Telecommunications Union. In a 2013 speech, Lu Wei of the State Internet Information Office argued that information services could cross borders, “but cyberspace cannot live without sovereignty.” States should proceed from the principles of the UN Charter, and Lu suggested that China would work with others to develop a multilateral framework for the governance of the Internet under the UN.
On questions of international law and cybersecurity, the United States and the United Kingdom have consistently argued that cyberspace should not be considered an entirely new domain and that the laws of armed conflict (proportionality and neutrality, for example) apply. Chinese analysts by contrast have stated that international law has not kept up with technological changes, that it is too narrow, and that it should be supplemented with new treaties, including perhaps arms control treaties for cyber weapons. In June of 2013, China, along with fourteen other countries, signed off on a report by UN Group of Government Experts (GGE) that argued “international law, and in particular, the United Nations Charter” applies to cyberspace and that there was a norm of state responsibility—states must meet their international obligations regarding internationally wrongful acts attributable to them. Since the report’s publication, the State Department has tended to stress the perceived consensus around international law and state responsibility. In contrast, the public statements by Chinese officials have centered on the norms of state sovereignty.

For many Chinese analysts, the overall security trends are negative. New technologies mean new threats, and the impact of cyber events is growing. The United States, Australia, UK, India, and Canada have used security concerns to block the import of Chinese products. Western countries, and the United States in particular, are increasing their “Internet containment of China” through diplomatic efforts such as cyber defense consultations with Japan, South Korea, and Australia. Spending on cyber offense by the Pentagon is increasing, and the Snowden revelations have reinforced the sense that the United States occupies the preeminent position in cyberspace.

These challenges give a sense of Chinese policy priorities over the next five years. The development of domestic technology and indigenous innovation will remain critical. Within China, the institutional, legal, and policy frameworks for cybersecurity must be developed. Some analysts have also called for the public development of active defense and offensive capabilities. There is also a sense that China needs to step up its international efforts to promote the concept of national sovereignty in cyberspace within the UN framework. In short, many in China are likely to see the country engaged in intense competition with the liberal democracies. Or as Major General Wu Jiangxing, the president of the PLA Information Engineering University, put it in an interview: “Cyberspace has become a field of intense struggle, and the state, government, and army must take extraordinary measures to enhance its security.”

---


