Comment September/October 2018 Issue China Science & Technology

When China Rules the Web

Technology in Service of the State

By Adam Segal

For almost five decades, the United States has guided the growth of the Internet. From its origins as a small Pentagon program to its status as a global platform that connects more than half of the world's population and tens of billions of devices, the Internet has long been an American project. Yet today, the United States has ceded leadership in cyberspace to China. Chinese President Xi Jinping has outlined his plans to turn China into a "cyber-superpower." Already, more people in China have access to the Internet than in any other country, but Xi has grander plans. Through domestic regulations, technological innovation, and foreign policy, China aims to build an "impregnable" cyberdefense system, give itself a greater voice in Internet governance, foster more world-class companies, and lead the globe in advanced technologies.

China's continued rise as a cyber-superpower is not guaranteed. Top-down, state-led efforts at innovation in artificial intelligence, quantum computing, robotics, and other ambitious technologies may well fail. Chinese technology companies will face economic and political pressures as they globalize. Chinese citizens, although they appear to have little expectation of privacy from their government, may demand more from private firms. The United States may reenergize its own digital diplomacy, and the U.S. economy may rediscover the dynamism that allowed it create so much of the modern world's technology.

But given China's size and technological sophistication, Beijing has a good chance of succeeding—thereby remaking cyberspace in its own image. If this happens, the Internet will be less global and less open. A major part of it will run Chinese applications over Chinese-made hardware. And Beijing will reap the economic, diplomatic, national security, and intelligence benefits that once flowed to Washington.

XI'S VISION

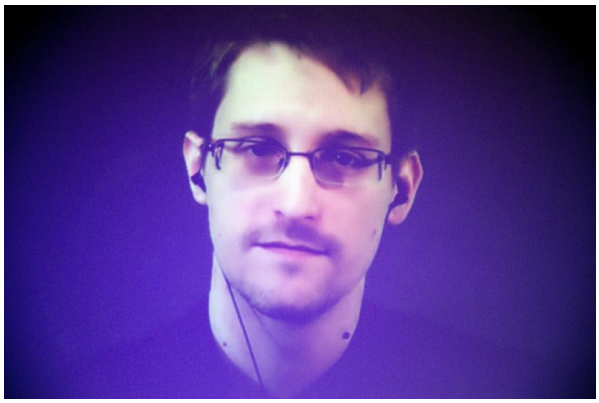
Almost from the moment he took power in 2012, Xi made it clear just how big a role the Internet played in his vision for China. After years of inertia, during which cyber-policy was fragmented among a wide array of government departments, Xi announced that he would chair a so-called central leading group on Internet security and informatization and drive policy from the top. He established a new agency, the Cyberspace Administration of China, and gave it responsibility for controlling online content, bolstering cybersecurity, and developing the digital economy.

Cyberpower sits at the intersection of four Chinese national priorities. First, Chinese leaders want to ensure a harmonious Internet. That means one that guides public opinion, supports good governance, and fosters economic growth but also is tightly controlled so as to stymie political mobilization and prevent the flow of information that could undermine the regime.

Second, China wants to reduce its dependence on foreign suppliers of digital and communications equipment. It hopes to eventually lead the world in advanced technologies such as artificial intelligence, quantum computing, and robotics. As Xi warned in May, "Initiatives of innovation and development must be securely kept in our own hands."

Almost from the moment he took power, Xi made it clear just how big a role the Internet played in his vision for China.

Third, Chinese policymakers, like their counterparts around the world, are increasingly wary of the risk of cyberattacks on governmental and private networks that could disrupt critical services, hurt economic growth, and even cause physical destruction. Accordingly, the People's Liberation Army has announced plans to speed up the development of its cyber-forces and beef up China's network defenses. This focus on cybersecurity overlaps with China's techno-nationalism: Chinese policymakers believe they have to reduce China's dependence on U.S. technology companies to ensure its national security, a belief that was strengthened in 2013, when Edward Snowden, a former contractor with the U.S. National Security Agency, revealed that U.S. intelligence services had accessed the data of millions of people that was held and transmitted by U.S. companies.



Charles Platiau / REUTERS

Edward Snowden speaks at a conference in Paris via video link from Moscow, December 2014.

Finally, China has promoted "cyber-sovereignty" as an organizing principle of Internet governance, in direct opposition to U.S. support for a global, open Internet. In Xi's words, cyber-sovereignty represents "the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing." China envisions a world of national Internets, with government control justified by the sovereign rights of states. It also wants to weaken the bottom-up, private-sector-led model of Internet governance championed by the United States and its allies, a model Beijing sees as dominated by Western technology companies and civil society organizations. Chinese policymakers believe they would have a larger say in regulating information technology and defining the global rules for cyberspace if the UN played a larger role in Internet governance. All four of Beijing's priorities require China to act aggressively to shape cyberspace at home and on the global stage.

THE END OF THE OPEN INTERNET

The Xi era will be remembered for putting an end to the West's naive optimism about the liberalizing potential of the Internet. Over the last five years, Beijing has significantly tightened controls on websites and social media. In March 2017, for example, the government told Tencent, the second largest of China's digital giants, and other Chinese technology companies to shut down websites they hosted that included discussions on history, international affairs, and the military. A few months later, Tencent, the search company Baidu, and the microblogging site Weibo were fined for hosting banned content in the run-up to the 19th Party Congress. Officials ordered telecommunications companies to block virtual private networks (VPNs), which are widely used by Chinese businesses, entrepreneurs, and academics to circumvent government censors. Even Western companies complied: Apple removed VPNs from the Chinese version of its App Store. Beijing also announced new regulations further limiting online anonymity and making the organizers of online forums personally accountable for the contributions of their members.

Chinese censors are now skilled at controlling conversations on social media. In 2017, as the dissident and Nobel Peace Prize laureate Liu Xiaobo became increasingly ill, censors revealed that they could delete his image from chats. In an even more Orwellian move, authorities have rolled out a sophisticated surveillance system based on a vast array of cameras and sensors, aided by facial and voice recognition software and artificial intelligence. The tool has been deployed most extensively in Xinjiang Province, in an effort to track the Muslim Uighur population there, but the government is working to scale it up nationwide.

In addition to employing censorship and surveillance, China has also created an interlocking framework of laws, regulations, and standards to increase cybersecurity and safeguard data in governmental and private systems. The government has enacted measures to protect important Internet infrastructure, it has mandated security reviews for network products and services, and it has required companies to store data within China, where the government will face few obstacles to accessing it. Beijing has also introduced new regulations concerning how government agencies respond to cybersecurity incidents, how and when the government discloses software vulnerabilities to the private sector, and how ministries and private companies share information about threats.

Different agencies and local governments could interpret and implement these policies in different ways, but at the least, the regulations will raise the cost and complexity of doing business in China for both domestic and foreign technology companies. Draft regulations published in July 2017 were particularly broad, defining "critical information infrastructure" to cover not only traditional categories such as communications, financial, and energy networks but also the news media, health-care companies, and cloud-computing providers. Baidu, Tencent, and Weibo have already been fined for violating the new cybersecurity laws. Foreign companies worry that an expansive interpretation of the requirements for inspections of equipment and storing data within China will raise costs and could allow the Chinese government to steal their intellectual property.

MADE IN CHINA

Chinese policymakers believe that to be truly secure, China must achieve technological self-sufficiency. Small wonder, then, that support for science and technology is front and center in the country's most recent five-year plan, which began in 2016. China's investment in research and development has grown by an average of 20 percent a year since 1999. It now stands at approximately $233 billion, or 20 percent of total world R & D spending. More students graduate with science and engineering degrees in China than anywhere else in the world, and in 2018, China overtook the United States in terms of the total number of

scientific publications. Western scientists have long ignored Chinese research, but they are now citing a growing number of Chinese publications.

Three technologies will matter most for China's ability to shape the future of cyberspace: semiconductors, quantum computing, and artificial intelligence. For years, Beijing has tried and failed to build an indigenous industry producing semiconductors, that is, the integrated circuits (or microchips) found in nearly every technological device. In 2016, China imported $228 billion worth of integrated circuits—more than it spent on imported oil—accounting for over 90 percent of its consumption, according to the consultancy McKinsey. The risk of relying on U.S. suppliers was brought home this April, when the Trump administration sanctioned ZTE, the world's fourth-largest maker of telecommunications gear. ZTE relies on U.S.-made components, including microchips to power its wireless stations. When the sanctions cut the company off from its supplies, it ceased major operations. In June, Trump reversed course on the sanctions, but the move did little to assuage Chinese concerns about dependence on foreign suppliers. Soon after the sanctions were announced, Xi called on a gathering of the country's top scientists to make breakthroughs on core technologies.

China is striving to define international standards for the next wave of innovation

In 2015, China issued guidelines that aim to get Chinese firms to produce 70 percent of the microchips used by Chinese industry by 2025. Since then, the government has subsidized domestic and foreign companies that move their operations to China and encouraged domestic consumers to buy from only Chinese suppliers. The government has committed $150 billion over the next decade to improve China's ability to design and manufacture advanced microprocessors. China has also acquired technologies abroad. According to the Rhodium Group, a research firm, from 2013 to 2016, Chinese companies made 27 attempted bids for U.S. semiconductor companies worth more than $37 billion in total, compared with six deals worth $214 million from 2000 to 2013. Yet these attempts have run into problems: many of the high-profile bids, including a $1.3 billion offer for Lattice Semiconductor and a $2.4 billion deal for Fairchild Semiconductor, were blocked by the U.S. government on national security grounds.

Then there is quantum computing, which uses the laws of quantum mechanics—essentially the ability of quantum bits, or "qubits," to perform several calculations at the same time—to solve certain problems that ordinary computers cannot. Advances in this area could allow Chinese intelligence services to create highly secure encrypted communications channels and break most conventional encryption. High-speed quantum computers could also have major economic benefits, remaking manufacturing, data analytics, and the

process of developing drugs. In 2016, China launched the world's first satellite that can communicate using channels secured by quantum cryptography and constructed the world's longest quantum communications cable, connecting Beijing and Shanghai. It's not clear how much China spends on quantum computing, but the sums are certainly substantial. It is spending $1 billion alone on one quantum computing laboratory.

More than its investments in semiconductor research and quantum computing, it is China's ambitious plans in artificial intelligence that have caused the most unease in the West. At an artificial intelligence summit last year, Eric Schmidt, the former chair of Google, said of the Chinese, "By 2020, they will have caught up. By 2025, they will be better than us. And by 2030, they will dominate the industries of AI." China is racing to harness artificial intelligence for military uses, including autonomous drone swarms, software that can defend itself against cyberattacks, and programs that mine social media to predict political movements.

In 2017, the Chinese government outlined its road map for turning itself into the "world's primary AI innovation center" by 2030. The plan is more a wish list than a concrete strategy, but it does provide direction to central ministries and local governments on how to invest to achieve breakthroughs by highlighting specific fields for research and development. The government has singled out Baidu, Tencent, the e-commerce giant Alibaba, and the voice recognition software company iFLYTEK as national champions in AI, identifying these companies as the first group to develop systems that can drive autonomous cars, diagnose diseases, act as intelligent voice assistants, and manage smart cities, that is, urban spaces that use a wide variety of sensors to collect data on how people live and then analyze that data to reduce cities' environmental impact, spur economic development, and improve people's quality of life.

China is also striving to define international standards for the next wave of innovation, especially in fifth-generation mobile network technology, or 5G, which will offer much faster Internet speeds to mobile users and enable new uses for Internet-connected devices. To many Chinese leaders, China's current place in the global division of labor looks like a trap: foreign firms reap high profits from the intellectual property they own, and Chinese companies survive on the thin margins they make by manufacturing and assembling physical products. If China can control technology standards, it will ensure that its firms receive royalties and licensing profits as others develop products that plug into Chinese-owned platforms.

Over the last decade, Beijing has increased the skill, sophistication, and size of the delegations it sends to standards organizations. China was essentially absent for the discussions about third- and fourth-generation mobile network technologies, but things have changed. In 2016, Huawei, China's largest

telecommunications company, sent twice as many representatives as any other company to the meeting in Vienna that defined the specifications for the coming fifth generation of mobile networks.

Aly Song / REUTERS

Xi at the World Internet Conference, Wuzhen, December 2015.

GOVERNING THE INTERNET

Under Xi, China has also tried to shape the international institutions and norms that govern cyberspace. For much of the last decade, Chinese hackers de facto set those norms by engaging in massive cyber-espionage campaigns designed to steal military, political, and, worst of all in the eyes of the United States, industrial secrets. The Obama administration pressed Beijing on the subject, publicly attributing attacks on U.S. companies to state-backed hackers and threatening to sanction senior officials. In 2015, the two sides agreed that neither would support digital theft for commercial advantage. China went on to sign similar agreements with Australia, Canada, Germany, and the United Kingdom. There was a marked downturn in activity in the wake of these agreements, but the decline seems to have been as much a result of a reorganization within the Chinese military as of U.S. diplomatic efforts. Now that the People's Liberation Army has consolidated control over its cyber-forces, industrial espionage has shifted to more sophisticated hackers in China's intelligence agencies.

China's more visible efforts at writing the rules of the road for cyberspace have centered on the UN. Washington and its allies have promoted a distributed model of Internet governance that involves technical bodies, the private sector, civil society, and governments, whereas Beijing prefers a state-centric vision. In 2017, for example, China called for "a multilateral approach to governing cyberspace, with the United Nations taking a leading role in building international consensus on rules." Beijing believes a multilateral approach

located at the UN has two immediate benefits. It would prioritize the interests of governments over those of technology companies and civil society groups. And it would allow China to mobilize the votes of developing countries, many of which would also like to control the Internet and the free flow of information.

Beijing has resisted U.S. efforts to apply international law, especially the laws of armed conflict, to cyberspace. A forum at the UN known as the Group of Governmental Experts has identified some rules of behavior for states in a series of meetings and reports from 2004 to 2017. Although in the 2013 report, Chinese diplomats accepted that international law and the UN Charter apply to cyberspace, and in 2015, they agreed to four norms of state behavior, they dragged their feet on discussions of exactly how neutrality, proportionality, the right of self-defense, and other concepts from international law might be applied to conflict in cyberspace. They argued instead that discussing international law would lead to the militarization of cyberspace. Chinese diplomats, along with their Russian counterparts, stressed the need for the peaceful settlement of disputes.In 2017, the participating countries in the Group of Governmental Experts failed to issue a follow-on report in part because China and Russia opposed language endorsing the right of self-defense.

In addition to working through the UN, Chinese policymakers have created their own venue to showcase their vision for the Internet and strengthen their voice in its governance: the World Internet Conference, held annually in Wuzhen. In 2017, Tim Cook and Sundar Pichai, the chief executives of Apple and Google, respectively, attended for the first time. Cook, a vocal defender of privacy and free speech at home, stated that Apple shared China's vision for "developing a digital economy for openness and shared benefits." By echoing Chinese officials' language on openness despite the tight controls on the Internet in China, Cook was signaling Apple's willingness to play by Beijing's rules.

Beijing is likely to have its biggest impact on global Internet governance through its trade and investment policies, especially as part of the Belt and Road Initiative, a massive effort to build infrastructure connecting China to the Indian Ocean, the Persian Gulf, and Europe. Along with the more than $50 billion that has flowed into railways, roads, pipelines, ports, mines, and utilities along the route, officials have stressed the need for Chinese companies to build a "digital Silk Road": fiber-optic cables, mobile networks, satellite relay stations, data centers, and smart cities.

Much of the activity along the nascent digital Silk Road has come from technology companies and industry alliances, not the Chinese government. Alibaba has framed its expansion into Southeast Asia as part of the Belt and Road Initiative. It has acquired the Pakistani e-commerce company Daraz and launched a digital free-trade zone with the support of the Malaysian and Thai governments, which will ease customs checks, provide logistical support for

companies, and promote exports from small and medium-sized companies in Malaysia and Thailand to China. ZTE now operates in over 50 of the 64 countries on the route of the Belt and Road Initiative. As well as laying fiber-optic cables and setting up mobile networks, the company has been providing surveillance, mapping, cloud storage, and data analysis services to cities in Ethiopia, Nigeria, Laos, Sri Lanka, Sudan, and Turkey.

The Chinese government hopes that these enterprises will give it political influence throughout the region. But private firms are focused on profit, and Beijing has not always succeeded in converting business relationships into political heft, even when the projects have involved state-run enterprises, since these firms also often pursue commercial interests that conflict with diplomatic goals. In the short term, however, the presence of Chinese engineers, managers, and diplomats will reinforce a tendency among developing countries, especially those with authoritarian governments, to embrace China's closed conception of the Internet.

THE FUTURE IS CHINESE

Beijing's vision of the Internet is ascendant. According to the think tank Freedom House, Internet freedom—how easily people can access the Internet and use it to speak their minds—has declined for the last seven years. More countries are pushing companies to store data on their citizens within their borders (which companies resist because doing so raises costs and reduces their ability to protect the privacy of their users) and to allow the government to carry out security reviews of their network equipment. Each country pursues these policies in support of its own ends, but they all can turn to China for material, technical, and political support.

The United States' position at the center of the global Internet brought it major economic, military, and intelligence benefits. U.S. companies developed the routers and servers that carry the world's data, the phones and personal computers that people use to communicate, and the software that serves as a gateway to the Internet. In a similar way, the Chinese Communist Party sees technology companies as a source of economic dynamism and soft power. And so it is increasing its political control over Chinese technology giants. As those companies come to supply more of the world's digital infrastructure, China's spy services will be tempted to collect data from them.

Chinese technology companies have several advantages: access to a lot of data with few restrictions on how they can use it, talented workers, and government support. But the country's legacy of central planning may lead companies to overinvest, build redundant operations, and stifle their employees' creativity. And Chinese technology firms have become the targets of political pressure in Australia, the United States, and Europe. The Australian government is considering banning Huawei from supplying equipment for Australia's fifth-

generation mobile networks. Washington is working to limit Chinese investment in U.S. technology companies and has made it more difficult for Chinese telecommunications firms to do business in the United States: it has blocked China Mobile's application to provide telecommunications services in the United States, banned the sale of Huawei and ZTE smartphones on U.S. military bases, and sought to prohibit U.S. telecommunications companies from spending critical infrastructure funds on equipment and services from China.

Yet none of these challenges is likely to deal a fatal blow to China's digital ambitions. The country is too large, too powerful, and too sophisticated. To prepare for greater Chinese control over the Internet, the United States should work with its allies and trading partners to pressure Beijing to open up the Chinese market to foreign companies, curb its preferential treatment of Chinese firms, and better protect foreign companies' intellectual property. U.S. policymakers should shift from simply defending the bottom-up, private-sector-led model of Internet governance to offering a positive vision that provides developing countries with realistic alternatives to working solely through the UN. Washington should talk to Beijing directly about norms of state behavior in cyberspace. The two countries should work together on setting global standards for government purchases of technology, determining how companies should secure their supply chains against cyberattacks, and planning government inspections of critical communications equipment. Yet these efforts will only shape trends, not reverse them. Whatever Washington does, the future of cyberspace will be much less American and much more Chinese.